Starterkit
Business Continuity Management

Colofon

SURFibo
Het SURF Informatie Beveiligers Overleg is ingesteld door het platform SURF ICT en Bedrijfsvoering met als doelen het actief stimuleren van en richting geven aan informatiebeveiliging binnen het hoger onderwijs (universiteiten, hogescholen en universitair medische centra).
Dat wordt bereikt door het bevorderen van de samenwerking tussen informatiebeveiligers en het leveren van praktisch bruikbare adviezen.
Meer informatie over SURFibo staat op www.surfibo.nl onder het thema informatiebeveiliging.

Voor meer informatie over deze Starterkit kan contact opgenomen worden met de secretaris van SURFibo, Anita Polderdijk (am.polderdijk@windesheim.nl of 038-4699076)

Inhoudsopgave

1. Inleiding

1.1 Aanleiding

In 2008 heeft een inventarisatie plaatsgevonden van de volwassenheid van instellingen in het Hoger Onderwijs en Onderzoek op de onderwerpen informatiebeveiliging, identity management en security incident management.
Hieruit bleek dat er verbeteringen mogelijk zijn door het delen van best practices en het 'normeren' van de te volgen aanpak. Dit heeft in 2009 geleid tot het opstellen van starterkits en leidraden.
Gebleken is dat ook het onderwerp bedrijfscontinuïteit (Business Continuity Management: BCM) voor verbetering vatbaar is. Om die reden is deze Starterkit BCM opgesteld.

1.2 Doelstelling

De starterkit is bedoeld om instellingen in het hoger onderwijs en onderzoek[1] een handleiding te bieden bij het inrichten van bedrijfscontinuïteit binnen hun instelling, op basis van een pragmatische aanpak.

1.3 Doelgroep

De doelgroep is divers omdat BCM een rol speelt door de hele organisatie. De primaire doelgroep bestaat in elk geval uit beveiligingsfunctionarissen.

1.4 Scope van het document

De in de starterkit onderscheiden stappen en de benoemde voorbeelddocumenten hebben betrekking op bedrijfscontinuïteit voor de gehele organisatie, zoals de inrichting van de calamiteitenorganisatie, het crisismanagement en escalatiemechanismen. In uitwerkingen die wat meer de diepte in gaan is de informatievoorziening / IT als voorbeeld genomen. Wel zal daarbij regelmatig de link naar de business gelegd worden, want die is leidend in het bepalen van de kritieke systemen.

1.5 Resultaat en timing

Het eindresultaat is een continu proces voor bedrijfscontinuïteit (met Plan-Do-Check-Act-cyclus), waarin de link naar crisismanagement is gelegd en het oefenen door de organisatie geborgd is.

De stappen van fase 1 kunnen worden gezet in 3 maanden tijd. Fase 2 beslaat 3 tot 12 maanden, afhankelijk van de concrete situatie bij een instelling. Vervolgens is de verfijning en optimalisering van het geheel (fase 3) een continu proces.

[1] Hoewel academische ziekenhuizen ook tot de directe doelgroep van SURFnet behoren, is deze starterkit niet specifiek op deze doelgroep gericht, gezien de specifieke continuïteitseisen die gesteld worden aan de patiëntprocessen.

2. Achtergrond BCM

2.1 Waarom BCM

Risico's die de continuïteit van een instelling 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 deze criminaliteit, fysiek en cyber terrorisme, bestuurlijke crisis, sabotage, diefstal of verlies van informatie en lekken binnen organisaties die breeduit in de media worden uitgemeten. Ongeacht de aard en oorzaak van de verstoring of crisis kunnen de gevolgen grote impact hebben en voor de organisatie desastreus van aard zijn. Het belang van Business Continuity Management is dan ook evident.

BCM is gericht op het waarborgen van de voortgang van bedrijfsprocessen. Bij de implementatie van BCM gaat het om drie aandachtspunten:

1. De mate waarin de gewenste procesvoortgang gegarandeerd is (beschikbaarheid - availability)
2. De mate waarin maatregelen getroffen zijn om het hoofd te bieden aan buitengewone omstandigheden (herstelvermogen - recuperative power)
3. Het bestaan van een beheerstructuur waarmee continuïteit gewaarborgd blijft (bedrijfszekerheid - dependability).

2.2 Afbakening BCM en BHV

BCM heeft betrekking op het veiligstellen van de continuïteit van bedrijfsprocessen en bedrijfsmiddelen (gebouwen, systemen en data). Het doel van bedrijfshulpverlening (BHV) is uitsluitend om de veiligheid van mensen (medewerkers, studenten en andere aanwezigen) te waarborgen.

2.3 Hoofdverantwoordelijkheden bij BCM

BCM verantwoordelijkheid vind je terug in de hele organisatie. Op bestuurlijk niveau zal een van de bestuursleden BCM in zijn portefeuille hebben. Deze heeft die portefeuille gedelegeerd naar de manager integrale veiligheid, en/of de facilitair manager en de CIO/CISO[2]
In de praktijk zal de invoering van BCM worden gecoördineerd door de Information Security Officer of de facilitair manager. Zij zijn verantwoordelijk voor de inrichting van een BCM-organisatie, waarin rollen en verantwoordelijkheden zijn benoemd en verdeeld.

Het is niet wenselijk om dit onderwerp te delegeren naar de ICT-manager, aangezien dan het gevaar bestaat dat alleen de ICT-continuïteit opgepakt wordt en niet de bedrijfscontinuïteit.

Voor BCM dient een onderscheid gemaakt te worden tussen de verantwoordelijkheden ten tijde van een calamiteit (het crisis- en calamiteitenteam) en de verantwoordelijkheden voor de inrichting en het onderhoud van de BCM-processen. Dit laatste staat centraal in de Starterkit, al worden in het Bijlagendocument ook sjablonen aangeboden met betrekking tot crisismanagement.

[2] Bij veel instellingen in het hoger onderwijs en onderzoek is (nog) geen manager integrale veiligheid aangesteld. De situatie is niet overal dezelfde; er zal per instelling gekeken moeten worden naar de juiste functiebenamingen. Hetzelfde geldt voor de BCM-coördinatie en beheer.

Voor het inrichten en onderhouden van de BCM-processen wordt aanbevolen een procescoördinator in te stellen. Grotere instellingen zullen per faculteit, school of locatie deze rol moeten beleggen (zie hoofdstuk 6).

2.4 De mens tijdens een calamiteit

Mensen reageren heel verschillend op een crisissituatie. Daarbij maakt het uit wat voor soort crisis er optreedt. Wanneer daarbij gewonden zijn gevallen, is de reactie van mensen doorgaans veel heviger dan bij een crisissituatie zonder gewonden.

Vaak stellen mensen in een crisissituatie heel verschillende prioriteiten. De een wil direct een brand blussen, terwijl de ander eerst de gewonden in veiligheid wil brengen en verzorgen.

Het is dan ook aan te bevelen om een leidraad te hebben over wat eerst gedaan moet worden en wat later kan. In bijlage 11 (zie Bijlagendocument) wordt een voorbeeld gegeven van een dergelijke leidraad. In de aanbevolen aanpak wordt over calamiteiten vooraf met elkaar van gedachten gewisseld teneinde goed voorbereid te zijn op een crisis.

3. Draagvlak en scoping

Het eerste wat binnen een onderwijsinstelling moet gebeuren als het om de invulling van het proces van bedrijfscontinuïteit gaat, is draagvlak creëren en de scope bepalen.

Net als voor informatiebeveiliging moet er voor bedrijfscontinuïteitmanagement commitment bestaan. Ook hier is het argument dat aandacht voor bedrijfscontinuïteit bijdraagt aan de realisering van de overall doelstellingen van de instelling. De afwegingen omtrent de mate waarin de bedrijfscontinuïteit gewaarborgd moet worden, wordt mede bepaald door de risk appetite van de instelling: welke risico's is het bestuur bereid te nemen. Die bereidheid wordt in belangrijke mate bepaald door het risicoprofiel van de instelling: wordt er gewerkt met proefdieren, zijn er meerdere locaties, of hoe multicultureel is de omgeving?

Onderdeel van het overleg met het bestuur is ook in welke mate er ruimte gegeven kan worden voor de specifieke situatie bij faculteiten en/of scholen. Die discussie heeft doorgaans als uitkomst dat er een instellingsbreed basispakket voor bedrijfscontinuïteit moet komen, waar bovenop afdelingsspecifieke toevoegingen gedaan kunnen (moeten) worden.

Verder is het ondoenlijk om alle deelonderwerpen (calamiteiten) in één keer te behandelen. Er wordt aanbevolen hierin een fasering aan te brengen, door bijvoorbeeld eerst de fysieke infrastructuur (bedreigingen zoals brand, explosie, aanslag, e.d.) te bezien. Met de daar opgedane ervaringen kan vervolgens gekeken worden naar de ICT-infrastructuur. Hierdoor wordt de organisatie gelijkmatiger belast met de invulling van het proces van bedrijfscontinuïteit en kunnen de vervolgfases nuttig gebruik maken van de 'lessons learned' uit de eerdere fases.

Ook is de vraag aan de orde 'welk deel van de organisatie is waar aan toe?' Het verkrijgen van draagvlak bij onderdelen van de instelling is er bij gebaat dat doelen realistisch gesteld worden.

Het is noodzakelijk om in elk geval de primaire processen onderwijs en onderzoek mee te nemen en daarnaast de belangrijkste ondersteunende processen, zoals ICT en facilitair management & vastgoed.

Een en ander moet leiden tot een Plan van Aanpak. Het instellingsbrede basispakket aan maatregelen komt modulair tot stand en het maatwerk daar bovenop per deelorganisatie eveneens. De verantwoordelijkheden voor het basispakket liggen centraal binnen de instelling, die voor het maatwerk per organisatieonderdeel decentraal.

4. De BCM-aanpak op hoofdlijnen

4.1 Inleiding

Op het gebied van BCM bestaan een aantal internationale standaarden, methodieken en codes of practice (zie literatuuroverzicht in bijlage 1).
De schrijvers van deze documenten zijn het aardig eens met elkaar. Na lezing van bijvoorbeeld de BS 25999 wordt weinig nieuws aangetroffen in de overige documenten. De stappen om te komen tot BCM in een instelling zijn vrijwel identiek:

- opstellen project- of programmaplan;
- processen op een rijtje zetten;
- uitvoeren Business Impact Analyse;
- uitvoeren dreigingen-analyse;
- vaststellen continuïteitstrategie;
- opstellen bedrijfscontinuïteitsplan;
- uitvoeren maatregelen;
- inrichten beheerorganisatie (BCM-organisatie);
- testen, oefenen en evalueren.

In de praktijk worden nogal wat nadelen ervaren bij het uitvoeren van een BCM-aanpak volgens de bekende standaarden:

- De analyses (business impact analyse en dreigingsanalyse) worden vaak 'kwalitatief' uitgevoerd en leiden tot uitspraken als 'hoog', 'laag', 'midden' als het gaat om de impact van een calamiteit, of 'nooit', 'vrijwel nooit', 'wel eens' of 'vaak' als gaat om de kans dat een dreiging kan voorkomen
- De eerste resultaten laten te lang op zich wachten. Het duurt soms maanden voordat de analyses zijn uitgevoerd en de gekozen BCM-strategie ook daadwerkelijk geïmplementeerd is. In de tussentijd is de organisatie niet beschermd tegen calamiteiten. Bovendien is de spanningsboog van zo'n BCM-traject te lang, waardoor het draagvlak snel afneemt.

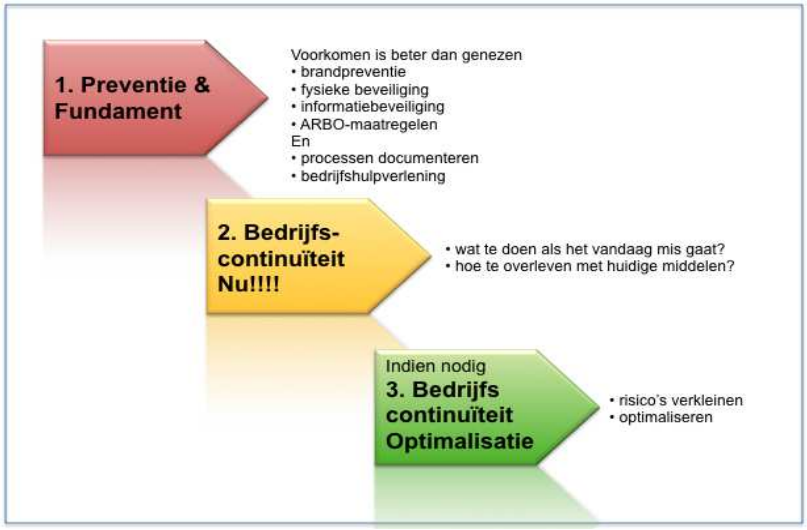
Om deze redenen is, in het kader van de MSIT-opleiding (Master of Security in Information Technology), door Jan Ploeg een alternatieve aanpak ontwikkeld die bovengenoemde knelpunten voorkomt. In de paragrafen 4.2 t/m 4.4 is een korte beschrijving van deze methodiek opgenomen. De volledige thesis 'Kleine stappen en toch snel(ler) thuis' is te vinden op www.janploeg.eu/?page_id=222.

Bij het ontwikkelen van deze nieuwe BCM-aanpak hebben de volgende vragen een rol gespeeld:

- Hoe kan voorkomen worden dat het BCM-traject te lang duurt?
- 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'[3] die te kort zijn?

[3] Recovery Time Objective (RTO) - the acceptable amount of time to restore the function: Ofwel: Hoe lang mag het duren voor de instelling weer over een operationele functie kan beschikken?

De antwoorden op eerder genoemde vragen hebben geleid tot een oplossing waarbij BCM in twee of drie stappen tot stand wordt gebracht.



Afbeelding 1: De BCM-aanpak op hoofdlijnen

4.2 Preventie en Fundament

De basis van onze pragmatische benadering bestaat uit preventie. De term preventie impliceert zowel het wegnemen van de bedreigingen, als het beperken van de impact ervan. Inventariseer eerst welke maatregelen ter bevordering van de veerkracht al zijn genomen:

- Zijn voldoende maatregelen tegen brand en bliksemschade getroffen?
- Zijn voldoende maatregelen genomen in het kader van Informatiebeveiliging?
- Zijn de maatregelen rondom de fysieke toegangsbeveiliging van de panden op orde?
- Is het personeel in het dagelijkse werk wel voldoende beschermd via afdoende arbomaatregelen?

Als het antwoord op deze vragen ontkennend is, start dan nog niet met BCM. Het is effectiever om eerst deze preventieve maatregelen op te pakken. De preventieve maatregelen vormen een onmisbaar onderdeel van het fundament onder het BCM-gebouw dat later opgezet wordt.

Een ander onderdeel van het fundament wordt gevormd door een goede inrichting van bedrijfshulpverlening (BHV, overigens wettelijk verplicht) en een beschrijving van de relevante bedrijfsprocessen op hoofdlijnen en de verantwoordelijkheden binnen en rondom die processen.

Is dit fundament niet voldoende: start dan nog niet met BCM. De (schaarse) middelen kunnen effectiever ingezet worden om de veerkracht van de organisatie te verhogen.

4.3 Bedrijfscontinuïteit nu!!!

Stel je voor dat er vandaag brand uitbreekt. Of een helikopter vernielt vandaag in de buurt een hoogspanningsleiding. Wat zou je dan doen?

Als er nog geen business-impact-analyse is uitgevoerd, geen strategie bepaald is en geen bedrijfscontinuïteitsplan voorhanden is, benoem dan de maatregelen om deze calamiteiten het hoofd te bieden. Het noteren van deze maatregelen is een goede oefening. Immers, de uitkomsten ervan zijn een eerste stap op weg naar een 'Bedrijfscontinuïteitsplan'.

En wie neemt tijdens de calamiteit vandaag de leiding? Wie neemt besluiten? Wie voert deze besluiten uit en hoe communiceren we met elkaar? En wie moeten we waarschuwen dat het primaire proces stil ligt? De antwoorden op deze vragen leg je vast in een 'Crisismanagementplan'.

Als vervolgens ook afgesproken wordt wie deze documenten beheert en wie regelt dat de bedachte scenario's worden getest en geoefend, dan is er weer een stap gezet: de instelling beschikt over een eerste opzet van het proces en de 'BCM-organisatie'.

Als het complete beeld dan voorhanden is en de scenario's zijn getest[4] , is het tijd om de uitkomsten (bijv. hoe snel zijn we weer in de lucht met onze kritieke processen?) te beoordelen. Passen de uitkomsten bij het risicoprofiel van de instelling of niet?
Feitelijk heeft de instelling hiermee een omgekeerde business-impact-analyse uitgevoerd.

Levert de evaluatie op dat de gerealiseerde hersteltijden (Recovery Time Realisation!) acceptabel zijn? Waarom zou de instelling dan verder een uitgebreid BCM-traject ingaan? Als nu de tests en oefeningen periodiek herhaald worden en de uitkomsten iedere keer weer geëvalueerd, dan heeft de instelling z'n BCM feitelijk op orde.

Is de uitkomst van de evaluatie dat de gerealiseerde hersteltijden nog niet goed genoeg zijn maar dat met kleine en snel uit te voeren maatregelen verbetering mogelijk is:

- Voer die maatregelen dan door.
- Pas de documenten (crisismanagementplan en/of bedrijfscontinuïteitsplan) aan.
- Voer tests en oefeningen uit.
- Evalueer op dezelfde manier als hierboven beschreven.

Ook dan heeft de instelling z'n BCM redelijk snel op orde.

Blijkt uit de eerste of volgende evaluaties dat de gerealiseerde hersteltijden te veel risico opleveren voor het voortbestaan van de instelling c.q. dat er teveel schade wordt geleden, dan kan de laatste stap uit de aanpak ter hand worden genomen.

[4] Op welke wijze het testen aangepakt kan worden wordt uiteengezet in paragraaf 5.2, stap 13.

4.4 Bedrijfscontinuïteit: optimaliseren

Na fase 2 (paragraaf 4.3) is het BCM-proces op orde. Maar in delen van de instelling zal dit nog niet het gewenste continuïteitsniveau opleveren. Waar nodig wordt in fase 3 op onderdelen naar een hoger plan toegewerkt.

In dat geval start je een BCM-traject waarbij je een aantal aanvullende stappen zet. Overigens kan in deze fase gekozen worden uit alle beschikbare standaarden, methodes en codes of practice. Zo kan bijvoorbeeld een BS 25999-traject worden ingezet of de werkwijze in de BSI 100-4 worden gekozen.

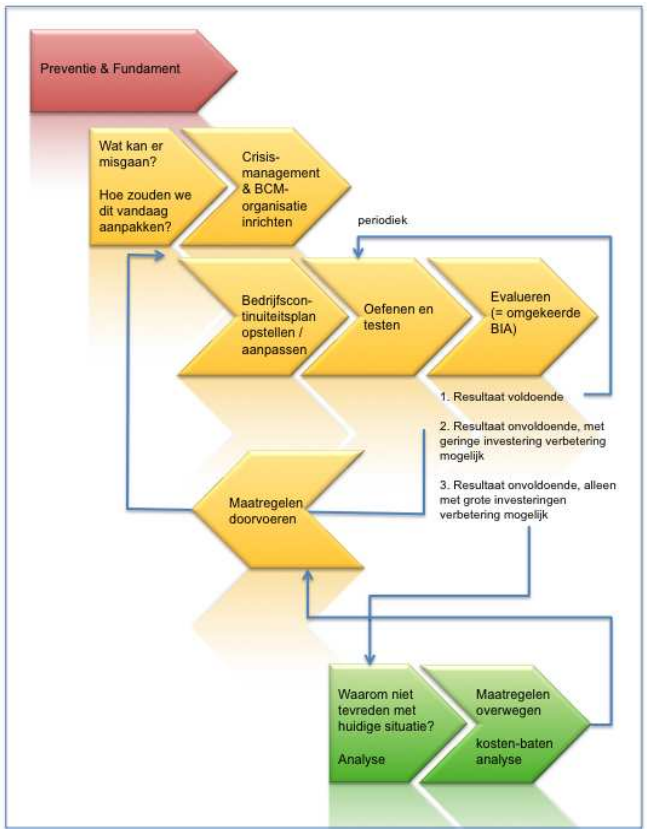
In deze fase wordt o.a. een business-impact-analyse uitgevoerd en worden betere scenario's (BCM-reactie) en een strategie opgesteld. Voordeel hierbij is dat in de voorliggende fase al ervaring is opgedaan en input is verzameld. Bijkomend voordeel is dat het senior management van de instelling al een tijdje met het onderwerp bezig is en zodoende de "mind-set" en de "sense of urgency" op niveau is.
Daarmee kan deze derde fase relatief snel en efficiënt uitgevoerd worden. Ook is er reeds een BCM-organisatie ingericht waardoor het beheer van de documenten is ingeregeld.

Nadat de nieuwe strategie is vastgesteld:

- Worden de maatregelen uitgevoerd.
- Worden vervolgens (in die volgorde dus) de documenten (bijv. crisismanagementplan en bedrijfscontinuïteitsplan) aangepast. En dat kan vlot, immers de BCM-organisatie is al tot stand gekomen in de vorige fase.
- Worden tests en oefeningen uitgevoerd.
- Wordt een evaluatie uitgevoerd.
- Eventueel aanpassingen gedaan, wederom getest/geoefend: kortom een proces van continue verbetering wordt op gang gebracht.

Het grote voordeel ten opzichte van de gebruikelijke aanpakken is dat in de tussentijd (immers fase 1 en fase 2 van de aanpak zijn doorlopen) altijd een bedrijfscontinuïteitsplan ligt dat uitgevoerd kan worden. Hiermee kan in ieder geval op elk moment zo optimaal mogelijk worden gereageerd op een calamiteit.

In de volgende figuur zijn de drie fases van onze BCM-aanpak ondergebracht.



Afbeelding 2: Bedrijfscontinuïteit: kleine stappen en toch sneller thuis

4.5 Projectmatige opzet

In hoofdstuk 5 worden de hierboven gepresenteerde fasen verder uitgewerkt en de uit te voeren activiteiten per fase beschreven. Voor een efficiënte en snelle uitvoering van deze BCM-aanpak is het noodzakelijk om de uitvoering projectmatig op te pakken.

Een projectleider en opdrachtgever moeten aangewezen worden. Goed denkbaar is, dat dit de toekomstige BCM-coördinator respectievelijk de BCM-eigenaar zijn. De activiteiten van de BCM-aanpak dienen te worden ondergebracht in een projectplan. De vaststelling van dit projectplan door het bestuur dient dan als officiële start van het BCM-traject.

Belangrijk is om in dit projectplan ook aan te geven welke middelen (zowel geld als inzet van mensuren) nodig zijn om het project uit te voeren. Omdat het op dit punt nog niet duidelijk is hoe veerkrachtig de instelling nu al is, zal de inschatting van de middelen voor fase 2 en eventueel ook fase 3 uiteraard nog globaal zijn.

Vanaf het moment dat de situatie is bereikt dat:
- de instelling beschikt over een BCM-organisatie, én
- uit een evaluatie is gebleken dat de hersteltijden acceptabel zijn, kan het project worden afgerond en treedt de beheerfase van BCM in de instelling in werking.

5. Stappenplan

5.1 Fase 1: Preventie en Fundament

N.B.: het oordeel of maatregelen 'voldoende en passend' zijn, wordt uiteindelijk bepaald door de risk appetite van de instelling: welke risico's is het bestuur bereid te nemen (zie ook hoofdstuk 3). Uiteraard kunnen zij zich bij hun oordeelsvorming laten bijstaan door deskundigen.
Uitgangspunt: het onderwijs mag niet langer dan één week stilliggen. Dus alles wat dat in de weg staat moet aangepakt worden.

1. Toon samen met de verantwoordelijke manager voor facilitair of gebouwzaken aan dat er voldoende en passende maatregelen zijn genomen tegen brand en bliksemschade.

Vanwege het belang van de preventieve maatregelen tegen brand en bliksemschade, dient bij twijfel over de toereikendheid ervan een externe en onafhankelijke adviseur ingeschakeld te worden om een review/second opinion uit te voeren naar de maatregelen tegen brand en bliksemschade.

Denk aan voorzieningen zoals:
- Aardingssystemen
- Bliksembeveiliging
- Brand- of rookdetectie
- Policy voor opslag gevaarlijke stoffen
- Ontruimingsplannen
- Blusmiddelen
- Overspanningsbeveiliging
- Potentiaalvereffening

Speciale aandacht dient hierbij uit te gaan naar ruimtes die van bijzonder belang zijn voor het functioneren van de instelling, bijvoorbeeld de server/computerruimtes, laboratoria, de bibliotheek en/of ruimtes met technische voorzieningen (verwarming, koeling etc.).

Mocht blijken dat de maatregelen die de instelling reeds genomen heeft, niet toereikend zijn, geef dan prioriteit aan het nemen van deze maatregelen boven het uitvoeren van een BCM-traject.

2. Stel samen met de verantwoordelijke manager voor facilitaire- of gebouwzaken vast dat er voldoende en passende maatregelen zijn genomen in het kader van toegangsbeveiliging.

Schakel bij twijfel een externe en onafhankelijke adviseur in om een review/second opinion uit te voeren naar de toereikendheid van de maatregelen.

Geef ook hier speciale aandacht aan ruimtes die van bijzonder belang zijn voor het functioneren van de instelling, bijvoorbeeld de serverruimte, (delen van) het magazijn of laboratoria.

De volgende zaken voor toegangsbeveiliging kunnen voor iedere instelling overwogen worden; waar noodzakelijk vanwege specifieke onderzoeksprocessen of andere omstandigheden kunnen verdergaande maatregelen genomen worden.

- Receptiepost in elke locatie, waar bezoekers de weg kunnen vragen.
- Passysteem voor speciale locaties, zoals de bibliotheek, een computerruimte of technische ruimtes.
- Medewerkerspas voor de kantoren en de kantine.
- Cameratoezicht bij de toegang tot de serverruimte en leveranciersingangen.
- Algemene inbraakbeveiligingsmaatregelen, hang- en sluitwerk, inbraakdetectie (alarminstallatie), bouwkundige maatregelen en hekken.

Bij verdergaande maatregelen kan gedacht worden aan:

- algehele toegangscontrole met pas of scanner;
- tijdregistratie / aanwezigheidsregistratie.

Mocht blijken dat de maatregelen die de instelling reeds genomen heeft niet toereikend zijn, geef dan prioriteit aan het nemen van deze maatregelen boven het uitvoeren van een BCM-traject.

3. Laat een review uitvoeren naar het niveau van informatiebeveiliging in de instelling.

Interne en externe reviews hebben zo hun eigen voor- en nadelen. Het voordeel van een externe review is dat deze strikt onafhankelijk wordt uitgevoerd en met de daarvoor geldende auditmethodieken; vaak wordt de prijs ervan als nadeel gekenmerkt. Als alternatief hiervoor kan gekozen worden voor een SURFaudit[5] of een interne review door de eigen audit-afdeling. Spreek bij een interne audit wel af dat er serieus werk van gemaakt moet worden en dat men collega's niet 'de hand boven het hoofd' mag houden; dat werkt contraproductief.

Overigens spelen preventieve maatregelen tegen brand, bliksem en fysieke toegangsbeveiliging bij een informatiebeveiligingsaudit ook een rol.
Betrek bij deze review ook de vraag of er een managementproces rondom informatiebeveiliging is ingericht en geïmplementeerd.

Mocht uit deze review blijken dat het niveau onvoldoende is, doorloop dan eerst de benodigde stappen om de informatiebeveiliging op orde te krijgen en te houden, alvorens te starten aan een BCM-traject.

Passende maatregelen voor informatiebeveiliging moeten in elk geval betrekking hebben op onderstaande zaken:

- **Vaststellen en implementeren van het beveiligingsbeleid**, gericht op een eenduidige wijze van omgang met beveiliging in de organisatie en bewustwording van het belang van beveiliging.
- **Incidentenmanagement**, gericht op de registratie, analyse, escaleren, oplossen en voorkomen van beveiligingsincidenten.
- **Logische toegangsbeveiliging**, gericht op het onderhouden van een set van regels voor het verlenen van toegang tot netwerk- en computersystemen.
- **Fysieke beveiliging**, gericht op het weren van onbevoegden.
- **Personele beveiliging**, gericht op het vaststellen van de betrouwbaarheid van het personeel bij het in dienst nemen van personeel, tijdens de uitvoering van het dienstverband en het einde dienstverband.

[5] SURFaudit geeft een snel overall-beeld van de informatiebeveiliging binnen de instelling, afgezet tegen een algemene normering voor het hoger onderwijs en onderzoek in Nederland.

- **Risicoanalyses,** gericht op het bepalen van een beveiligingsclassificatie voor een (business)applicatie en eisen voor specifieke application controls.
- **Onderhouden van een basisbeveiligingsniveau** voor de pc-werkstations, de netwerken en de applicatieservers.

Bij een gedegen review naar het niveau van informatiebeveiliging komt overigens vanzelf de vraag naar voren hoe het is gesteld met de continuïteit van de IT-dienstverlening, waarmee een natuurlijke brug ontstaat naar het vraagstuk van bedrijfscontinuïteit.

4. Verzeker je ervan dat de Bedrijfshulpverlening op orde is.

Van het allergrootste belang is dat de medewerkers, studenten en bezoekers van de instelling bij het optreden van een calamiteit, waarbij gevaar voor personen kan ontstaan, op een snelle en veilige manier het gebouw/het terrein kunnen verlaten en op een plek elders worden opgevangen. Een goed lopende en geoefende bedrijfshulpverlening is van levensbelang voor een instelling bij het overleven van een calamiteit.

Gelukkig is de bedrijfshulpverlening in ons land gebonden aan wet- en regelgeving. Er is een verplichting van kracht voor organisaties om de bedrijfshulpverlening goed op orde te hebben.

BHV wordt in de praktijk vaak bij de personeelsafdeling belegd. De te stellen vragen zijn:

- *Is er een BHV-organisatie in ieder gebouw?*
- *Zijn er ontruimingsplannen?*
- *Wanneer is voor het laatst geoefend?*

We hoeven hier niet te checken of de BHV aan de wettelijke voorschriften voldoet.

Neem het voorbeeld van de brand die het gebouw van de faculteit Bouwkunde van de TU Delft in 2008 in as legde. Tijdens die brand zijn geen grote persoonlijke ongelukken voorgekomen. Het personeel en de aanwezige studenten en bezoekers waren snel uit het pand.
Stel dat er één of meer slachtoffers waren gevallen doordat personeel of studenten niet op tijd het pand hadden kunnen verlaten. Dan krijgt zo'n calamiteit een extra dimensie. Ontstaan er slachtoffers, dan is de organisatie de eerste dagen na de calamiteit waarschijnlijk meer bezig met het verwerken van het verlies en het organiseren van herdenkingsbijeenkomsten dan met weer in de lucht krijgen van de bedrijfsprocessen.
In dit geval kon de faculteitsleiding al tijdens de brand starten met het werken aan de bedrijfscontinuïteit van de faculteit. Na 5 werkdagen kwam het onderwijsproces weer op gang.

5. Toon samen met de verantwoordelijke manager voor personeelszaken aan dat er voldoende en passende maatregelen zijn genomen in het kader van de arbeidsomstandighedenwet.

Beoordeel in ieder geval of in de organisatie periodiek risico-inventarisaties en -evaluaties worden uitgevoerd en controleer of de daaruit voortgekomen maatregelen zijn doorgevoerd.

Schakel bij twijfel een externe en onafhankelijke adviseur in om een review/second opinion uit te voeren naar de toereikendheid van de maatregelen.

6. Stel samen met de belangrijkste proceseigenaren een overzicht op van processen, verantwoordelijkheden en afhankelijkheden.

De redenen om hier aandacht aan te besteden zijn:
- het identificeren van afhankelijkheden in ketens;
- het identificeren van contactpersonen;
- de mogelijkheid om op basis van deze kennis prioriteiten te kunnen stellen.

Bij het identificeren van afhankelijkheden in ketens wordt een eenvoudige Afhankelijkheids- & Kwetsbaarheidsanalyse (A&K-analyse) uitgevoerd. Doorgaans is dat voldoende voor het beoogde doel. Wie verder wil gaan, kan gebruik maken van risicoanalyses die gebaseerd zijn op SPRINT van het Information Security Forum (ISF).

Hier kan een keuze gemaakt worden om eerste de belangrijkste primaire processen te inventariseren, bijvoorbeeld die m.b.t. het onderwijs en (contract)onderzoek.

Bij wijze van voorbeeld tonen we onderstaand het overzicht van vier kritische bedrijfsprocessen van het Erasmus MC, met daarbij (tussen haakjes) de noodzakelijk geachte hersteltijden:

Afbeelding 3: kritische bedrijfsprocessen en gewenste hersteltijden bij het Erasmus MC

Bij UMC's zijn de patiëntprocessen typisch 'minuut'-kritiek. Dit kan overigens ook voorkomen in een onderzoekomgeving, waar het bijvoorbeeld ook om mensenlevens gaat (een kernreactor), of om feitelijk onherstelbare schade aan een zeer kostbaar onderzoek (dus net als bij een mensenleven geen return to operations mogelijk).

Onder het kopje 'verantwoordelijkheden en afhankelijkheden' dient ook aandacht besteed te worden aan de afhankelijkheid van leveranciers. In een Service Level Agreement (SLA) wordt niet alleen opgenomen wat voor levertijden gelden voor bepaalde zaken, maar ook iets over hoe de leverancier omgaat met een calamiteit en hoe de levering dan gegarandeerd wordt. Het is aan te bevelen om tevens het recht op een audit bij de leverancier in de SLA op te nemen, zodat gecontroleerd kan worden of zijn BCM op orde is. En als je dan nog niet overtuigd bent en de betreffende afhankelijkheid is van kritisch belang, dan zou je kunnen vragen of de instelling opgenomen kan worden in het oefenplan van de leverancier.

De deliverable van fase 1 is het realiseren van de quick wins uit de stappen 1 t/m 5 en een beschrijving van kritieke bedrijfsprocessen (stap 6).

5.2 Fase 2: Continuïteit nu!!!

7. Stel een projectplan op op basis van de onderstaande stappen 8 t/m 15.

Maak hierbij gebruik van de projectmanagementmethodiek die binnen je organisatie gebruikelijk is. Paragraaf 4.5 geeft aan waarom het gebruik van een projectplan wordt aanbevolen. Zet dit niet te zwaar aan! Het gaat erom dat de stappen 8 t/m 15 realistisch in de tijd ingepland worden en dat de benodigde middelen beschikbaar gesteld worden. Neem in het projectplan activiteiten op om na de stappen 9 en 14 het projectplan te concretiseren (zie ook bijlage 18 Modelplanning (stap 7) in het Bijlagendocument).

8. Tref de voorbereidingen voor het houden van een calamiteitenscenario-sessie

De Calamiteitenscenario-sessie moet goed worden voorbereid. Degene die de sessie organiseert en begeleidt, dient een aantal activiteiten te verrichten alvorens de sessie kan worden gehouden. Om deze voorbereidingen te doen, zijn interviews noodzakelijk en moeten reeds beschikbare documenten (bijv. overzicht van processen en hun onderlinge relaties) bestudeerd worden.

Zie voor een uitgebreidere beschrijving het scriptiewerk 'Kleine stappen en toch snel(ler) thuis'.

9. Organiseer de calamiteitenscenario-sessie

Eén of meerdere bijeenkomsten worden georganiseerd met het bestuur van de instelling. Tijdens deze bijeenkomst(en) worden de volgende onderwerpen behandeld:

1. Welke uitwegen zijn in de huidige situatie mogelijk in geval van een calamiteit?
2. Hoe organiseren we het crisismanagement?
3. Welke BCM-rollen moeten worden toegewezen en aan wie?

Of er één of meerdere bijeenkomsten noodzakelijk zijn, is afhankelijk van de situatie. Beschikt de instelling al over een algemeen crisismanagementplan en wordt dit regelmatig geoefend? Hoe groot is het bestuur? Hoe snel kan men tot besluiten komen? Hoe lang mogen de sessies duren?
Het is wel aan te bevelen om in een bestuursvergadering, voorafgaande aan de eerste sessie, de procedure tijdens calamiteitenscenario-sessie in te leiden. Tevens kunnen dan de calamiteitenscenario's gepresenteerd worden, zodat het bestuur zich alvast kan voorbereiden.

In bijlage 2 worden een aantal mogelijke incidenten opgesomd die de continuïteit van een instelling in gevaar kunnen brengen. Uiteindelijk zijn de gevolgen van zulke incidenten terug te brengen tot vier calamiteitenscenario's, die grosso modo voor elke onderwijsinstelling gelden. Deze zijn:

- *Verlies van mensen: bijvoorbeeld door een voedselvergiftiging op een afdelingsfeestje. Meer dan 50% van de ICT-medewerkers is afwezig. Dit gaat naar verwachting een week duren. De afwezigheid is niet gelijk gespreid over de organisatie. Sommige helpdesks zijn volledig onbemand, de meest kritische expertisegroep is afwezig*
- *Verlies van gebouw(en): door een brand of andere calamiteit is een gebouw volledig verloren geraakt. Er zijn geen bruikbare spullen over; men heeft niets kunnen redden uit de 'boedel', dus ook geen backup tapes/schijven, e.d.*

- *Sabotage van data: op een maandagochtend komt men er achter dat zeer veel gegevens op de file servers verminkt zijn. Er is geen duidelijke oorzaak (virussen op PC's, een hack, een ontevreden medewerker?). Men moet ervan uitgaan dat alle fileservers getroffen zijn. Bij de eerste check blijkt dat de laatste backups ook verminkt zijn.*
- *Verlies van een datacenter: het oefenscenario moet realistisch zijn, dat wil zeggen dat het moet afgestemd zijn op de lokale situaties. Is er een DC of zijn er meer? Is een DC gevestigd in een multi-purpose gebouw of stand-alone?*

Tijdens een bijeenkomst met het bestuur van de instelling wordt een aantal calamiteitenscenario's doorgesproken. Het is de bedoeling dat als uitgangspunt wordt gehanteerd dat de calamiteit zich nu, op dit moment, voordoet. De opdracht aan het bestuur is om met elkaar een uitweg te vinden uit de calamiteit. Doel van de sessie is om een aantal uitwegscenario's te bedenken. Bewust wordt niet gekozen voor de term uitwijkscenario's omdat deze term te snel leidt tot het uitwijken van de productie, werkplekken en/of systemen naar een (hiervoor voorbereide) uitwijklocatie. Dat hoeft niet altijd het geval te zijn.

Scenario's dienen, door oefening, meerdere doelen:
- oefen de samenwerking binnen calamiteiten- en herstelteams onder druk;
- test de plannen;
- ga na of er voldoende veerkracht in de instelling zit. Met andere woorden zijn er voldoende preventieve maatregelen genomen om na een calamiteit weer te kunnen herstellen?

Zie voor een uitgebreidere beschrijving van de calamiteitenscenario-sessie het scriptiewerk 'Kleine stappen en toch snel(ler) thuis'.

10. Richt de crisismanagement-organisatie in of pas deze aan op basis van de uitkomsten van de calamiteitenscenario-sessie

Na de calamiteitenscenario-sessie(s) worden de besluiten van het bestuur rondom crisismanagement uitgewerkt door de BCM-coördinator of, als die er al is, samen met de beheerder van het crisismanagementplan. Het crisismanagementplan omvat de eerste stappen die gezet worden bij het daadwerkelijk optreden van een calamiteit (in bijlage 11 van het Bijlagendocument worden deze stappen nader toegelicht). In het crisismanagementteam worden tijdens een crisis de benodigde besluiten genomen en wordt de uitvoering van deze besluiten gevolgd.

11. Richt de BCM-organisatie in op basis van de uitkomsten van de calamiteitenscenario-sessie

Onder andere de onderstaande vragen moeten daarbij beantwoord worden:
- Wie is binnen de instelling eindverantwoordelijk voor het BCM-beheerproces (BCM-eigenaar)? In hoofdstuk 6 wordt apart aandacht besteed aan het beheerproces van BCM.
- Wie zorgt voor de operationele coördinatie van de BCM-werkzaamheden (BCM-coördinator)?
- Wie is eigenaar/beheerder van de BCM-documenten?
- Wie is inhoudelijk verantwoordelijk voor het up to date houden van de uitwegplannen?
- Wie zorgt dat er op gezette tijden wordt getest, geoefend en geëvalueerd (BCM-coördinator)?

12. Stel een bedrijfscontinuïteitsplan op op basis van de uitkomsten van de calamiteitenscenario-sessie

De calamiteitenscenario-sessie levert inzichten op rondom:

- uitwegscenario's, inclusief communicatie;
- crisismanagement;
- escalatiemechanisme;
- BCM-organisatie.

De uitkomsten van de sessie kunnen nu ondergebracht worden in een bedrijfscontinuïteitsplan. Dit plan bevat de volgende onderdelen:

1. het crisismanagementplan;
2. een escalatieplan;
3. een beschrijving van de BCM-organisatie (inclusief beheerplan voor de BCM-documenten;
4. de uitwegscenario's en de bijbehorende uitwegplannen;
5. een communicatieplan;
6. een test- en oefenplan;
7. een opleidingsplan (bijv. voor crisismanagement).

13. Oefenen, testen en doorrekenen

Als het bedrijfscontinuïteitsplan is vastgesteld door het bestuur van de instelling, is de volgende activiteit het testen en oefenen van het crisismanagement, de uitwegscenario's en de uitwegplannen.

Doel van het testen en oefenen is:

- Het testen van de uitwegscenario's op uitvoerbaarheid.
- Het oefenen van het crisismanagement en de uitwegscenario's zodat in geval van een calamiteit snel en correct gehandeld kan worden.
- Het vaststellen van de doorlooptijden van de uitwegscenario's.
- Het creëren van awareness over bedrijfscontinuïteit binnen de organisatie in het algemeen als ook awareness met betrekking tot de specifieke uitwegscenario's en uitwegplannen bij de betrokken medewerkers.

Sommige (delen van de) uitwegscenario's zijn wellicht in de praktijk niet te testen. Probeer in dat geval het scenario droog of op papier te testen en door te rekenen.

De uitkomsten van de tests en oefeningen vormen vervolgens de input voor de uit te voeren evaluatie.

14. Evalueren

Op basis van de resultaten van de tests en oefeningen wordt een overzicht opgesteld van de bevindingen.

Kenmerk van deze evaluatie is dat, aan de hand van de resultaten van de tests en oefeningen, het bestuur vaststelt of de uitwegscenario's acceptabele hersteltijden opleveren. Daarmee wordt eigenlijk met deze evaluatie een omgekeerde business impact analyse uitgevoerd:

- Welke resultaten zijn met de huidige middelen haalbaar?
- Zijn die resultaten acceptabel (incl. financiële consequenties)?

Zie voor een uitgebreidere beschrijving van de evaluatie het scriptiewerk 'Kleine stappen en toch snel(ler) thuis'.

Op basis van de bovenstaande vragen en antwoorden dient een conclusie getrokken worden. Zijn de uitwegscenario's afdoende? Kan de instelling op dit moment een calamiteit overleven? Zijn er nog verbeteringen mogelijk? Wat kosten die en hoeveel leveren ze op?

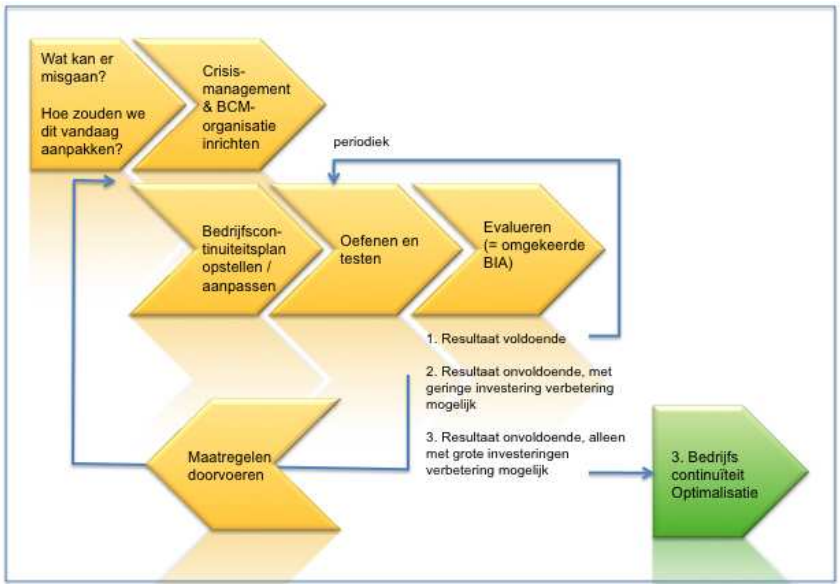
Uiteindelijk kunnen de volgende hoofdconclusies getrokken worden:

1. De resultaten die behaald zijn met de beschreven uitwegscenario's zijn voldoende.
2. De resultaten die behaald zijn met de beschreven uitwegscenario's zijn nog niet voldoende. Echter, met een aantal aanpassingen en geringe investeringen kunnen de resultaten voldoende verbeterd worden.
3. De resultaten die behaald zijn met de beschreven uitwegscenario's zijn niet voldoende en er zijn waarschijnlijk grote investeringen en aanpassingen nodig om de resultaten naar een acceptabel niveau te brengen.

ad 1.
Het bestuur van de instelling heeft naar aanleiding van de test- en oefenresultaten geconstateerd dat de hersteltijden acceptabel zijn en de performance na het herstel van de betrokken processen voldoende is.

Met deze uitkomst van de evaluatie is het voldoende om de BCM-organisatie zijn werk te laten doen. Uit de tests en oefeningen zijn vast nog een aantal verbeterpunten naar voren gekomen. Deze kunnen in de uitwegscenario's en het crisismanagement- en escalatieplan worden doorgevoerd.

Door periodiek de oefeningen en tests te herhalen en vervolgens de evaluatiemethode te herhalen, blijft de instelling steeds 'in control' met betrekking tot bedrijfscontinuïteit. Het herhalen van de tests, oefeningen en evaluatie zorgt ervoor dat in geval van gewijzigde situaties (andere facilitaire voorzieningen, nieuwe organisatieonderdelen, andere wet- en regelgeving, nieuwe contractvoorwaarden etc.) iedere keer vastgesteld wordt of de uitwegscenario's en het crisismanagement nog steeds acceptabel zijn. In paragraaf 6.5 wordt nader ingegaan op frequentie en inhoud van deze periodieke activiteiten.



Afbeelding 4: Evaluatie: wat te doen met de uitkomsten?

ad 2.
Indien wordt geconcludeerd dat de behaalde resultaten nog niet acceptabel zijn (de restrisico's zijn nog te groot), maar met een aantal aanpassingen en kleine investeringen de gewenste verbetering haalbaar is, kan besloten worden deze aanpassingen uit te voeren.

Nadat deze aanpassingen zijn gedaan, kunnen de uitwegscenario's in het bedrijfscontinuïteitsplan aangepast worden en kunnen de tests en oefeningen opnieuw doorlopen worden. Uit een herhaalde evaluatie blijkt dan of de aanpassingen hebben geleid tot de gewenste verbetering.

ad 3.
Blijkt uit de evaluatie dat de resultaten niet voldoende zijn en dat acceptabele hersteltijden slechts bereikbaar zijn na grote investeringen en veel aanpassingen, dient besloten te worden om alsnog een systematischer benadering te kiezen alvorens over te gaan tot deze investeringen.
Het gaat in dat geval om grote investeringen en dan is het verstandig een goede afweging te kunnen maken. Een dergelijke afweging wordt gemaakt in fase 3 Optimalisatie.

15. Verbetermaatregelen doorvoeren
De evaluatie (omgekeerde BIA) is uitgevoerd. Indien het bestuur heeft besloten dat het resultaat weliswaar nog onvoldoende is, maar met een aantal aanpassingen en geringe investeringen alsnog verbeteringen behaald kunnen worden, worden deze aanpassingen doorgevoerd.

Nadat deze aanpassingen zijn gedaan, dienen de uitwegscenario's te worden aangepast. Daarna wordt er weer getest en geoefend. De resultaten worden op de wijze zoals beschreven in stap 14 geëvalueerd.

5.3 Fase 3: Optimalisatie

Fase 1 en 2 zijn uitgevoerd. De instelling heeft inmiddels de eerste stappen op het gebied van bedrijfscontinuïteit gezet:

- preventieve maatregelen zijn voldoende;
- de BHV-organisatie is op orde;
- processen en verantwoordelijkheden zijn beschreven;
- uitwegscenario's en uitwegplannen zijn bedacht en beschreven;
- crisismanagement- en BCM-organisatie zijn ingericht;
- tests en oefeningen zijn uitgevoerd;
- eén of meerder evaluatierondes zijn uitgevoerd.

Blijkbaar heeft de instelling op basis van de uitkomsten van de evaluatie besloten dat de gerealiseerde hersteltijden niet goed genoeg zijn. Er zijn nogal wat aanpassingen nodig om wel het gewenste niveau te bereiken en hiermee zijn grote investeringen gemoeid.

16. Vaststellen gewenste hersteltijden

Uitwegscenario's als door de uitgevoerde evaluatie (de omgekeerde business impact analyse):

- We weten welke producten/diensten en daarbij horende processen kritiek zijn en prioriteit moeten hebben.

- We kennen de afhankelijkheden tussen de processen (uitwegscenario's, testen, oefenen, evalueren).
- We weten voor welke processen we tevreden zijn met de in fase 2 gerealiseerde hersteltijden.
- We weten voor welke processen we niet tevreden zijn met de in fase 2 gerealiseerde hersteltijden.
- Impliciet weten we daarmee ook de gewenste hersteltijden voor de laatst genoemde processen.

Het is daarom in deze fase mogelijk om snel een overzicht te maken van de processen en de daarbij behorende hersteltijden.

17. Huidige situatie goed in kaart brengen

Voor de processen waarvoor in fase 2 nog geen acceptabele hersteltijden zijn behaald, wordt bekeken welke aspecten (bijv. middelen) binnen en rondom het proces ervoor zorgen dat de gewenste hersteltijden niet worden gehaald.

Daarbij moeten de volgende aspecten in ogenschouw worden genomen:

- Afhankelijkheid van andere processen en de volgorde waarin de processen na een calamiteit weer in de lucht komen (uitwegscenario's).
- Personele middelen die nodig zijn voor het proces.
- Benodigde productieruimte/huisvesting voor het proces.
- Benodigde technische middelen voor het proces.
- Benodigde informatie en communicatie voor het proces.
- Benodigde materialen voor het proces.
- Betrokken stakeholders bij het proces (bijv. leveranciers, onderhoudspartners, klanten).

18. Inventariseren mogelijke maatregelen

Nagegaan moet worden welke maatregelen genomen kunnen worden om ofwel de hersteltijden op het gewenste niveau te krijgen dan wel of er zodanige preventieve maatregelen genomen kunnen worden dat het proces door de calamiteit niet getroffen wordt, c.q. de kans hierop zo klein is dat het restrisico geaccepteerd kan worden.

19. Uitvoeren kosten-batenanalyse

Van belang is om een juiste kosten-batenanalyse te maken. Hoeveel middelen moeten worden ingezet om de mogelijke maatregelen te nemen? Wat is de afname van de hersteltijd c.q. hoeveel kleiner wordt de kans dat het proces door de mogelijke calamiteiten wordt getroffen.

20. Besluit nemen voor aanvullende maatregelen

Aan het senior management van de instelling is het vervolgens om te kiezen uit de mogelijke maatregelen, dan wel ervoor te kiezen om – vanwege het niet in balans zijn van de kosten en de baten – alsnog tevreden te zijn met de in fase 1 en 2 gerealiseerde hersteltijden.

21. Uitvoeren maatregelen, aanpassen bedrijfscontinuïteitsplan, testen, oefenen en evalueren

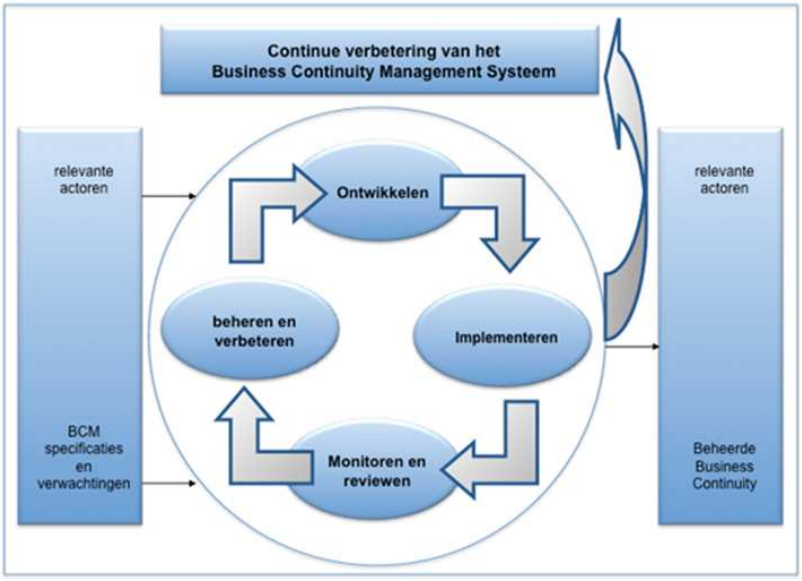
Nadat het bestuur heeft besloten welke maatregelen noodzakelijk zijn, worden deze maatregelen doorgevoerd.

Nadat de maatregelen zijn uitgevoerd, dienen de uitwegscenario's en de uitwegscenario's te worden aangepast. Daarna wordt er weer getest en geoefend. De resultaten worden op de wijze zoals beschreven in stap 14 geëvalueerd.

6. Het Beheerproces

6.1 Het Beheerproces

Ook indien er geen crisis of calamiteit is, moet aandacht besteed worden aan BCM. Hiervoor is het BCM-beheerproces ingericht. Dit hoofdstuk beschrijft de wijze van inrichting, het doel, de taken, activiteiten en verantwoordelijkheden van het BCM-beheerproces. In afbeelding 5 is het gehele beheerproces schematisch weergegeven.



Afbeelding 5: het BCM-beheerproces

6.2 Doel

Het doel van het proces BCM-beheer is om de BCM-plannen (documentatie) en BCM-organisatie (vaardigheden) actueel te houden.

6.3 Resultaat

Het BCM-beheerproces wordt ergens ondergebracht, bijvoorbeeld bij het Shared Service Centrum – ICT, de afdeling integrale veiligheid of de afdeling informatie management. Deze beheert de volgende BCM-documenten:

- het Crisismanagementplan
- de Bedrijfscontinuïteitsplannen
- (opstellen en doen uitvoeren) jaarlijkse oefenkalender
- algemeen oefeningendraaiboek
- jaarverslag

Onderdeel van het Crisismanagementplan en de Bedrijfscontinuïteitsplannen zijn ook de alarmeringslijsten, waarin de namen en telefoonnummers van de leden van de rampenbestrijdingsorganisatie zijn opgenomen, evenals andere telefoonnummers die van belang kunnen zijn bij de bestrijding van rampen en zware ongevallen.

6.4 Afbakening

De activiteiten die ten tijde van een crisis nodig zijn om de bedrijfscontinuïteit te borgen, vallen buiten het BCM-beheerproces. Het BCM-beheerproces beperkt zich tot de BCM-plannen. Onderliggende technische documentatie en plannen vallen buiten de scope en zijn een verantwoordelijkheid van de betrokken technische beheerafdelingen.

6.5 Procesonderdelen

Onderdelen van het BCM-beheerproces zijn:

- Beheer van de documentatie van het Crisismanagementplan, de Bedrijfscontinuïteitsplannen en het oefeningendraaiboek. Tenminste één maal per kwartaal worden het Crisismanagementplan en de Bedrijfscontinuïteitsplannen gecontroleerd op actualiteit en aangepast voor eventuele personele mutaties. Na iedere oefening worden de resultaten van de evaluatie van de oefening verwerkt in de plannen.
- Opstellen oefenkalender: jaarlijks wordt een jaar-oefenkalender opgesteld in overleg met de directeur van de afdeling waar het beheer van de BCM-documenten is belegd. Jaarlijks worden tenminste drie oefeningen gehouden, een mix van gepland en onverwacht, papier en fysiek en een mix van calamiteitenscenario's. De mix wordt in overleg met de directeur van de afdeling waar het beheer van de BCM-documenten is belegd vastgesteld.
- Organiseren oefeningen: de uitvoering van de oefenkalender.
- Evalueren oefeningen.
- Evalueren Bedrijfscontinuïteitsplan en BCM-proces bij een calamiteit.

6.6 Organisatie

Het procesbeheer voor het BCM-beheerproces kan bijvoorbeeld worden belegd bij de facilitair manager en de CIO/CISO en/of de manager integrale veiligheid. Proceseigenaar is de directeur ICT of directeur integrale veiligheid (zie ook par. 2.3). Een deel van de uitvoering is belegd bij het secretariaat van de betreffende directie. Bij grote instellingen zijn op meerdere plekken een procescoördinator en operationele coördinatoren aanwezig.

6.7 Kosten

Het beheerproces kan worden begroot op een aantal interne uren per jaar (zeg 80 uur). Daarnaast kan bij het opstellen van de jaarkalender of naar aanleiding van een evaluatie van een oefening besloten worden externe ondersteuning in te zetten, bijvoorbeeld voor training, onafhankelijke observatie tijdens oefeningen of voor het leiden van een oefening. Hiervoor kan als onderdeel van de begroting van het security management een budget van enkele adviesdagen worden opgenomen (zeg € 6.000).

7. Erkenning

Bij de totstandkoming van deze Starterkit is dankbaar gebruik gemaakt van de inbreng van een werkgroep, bestaande uit de volgende personen.

José Eerens	academisch ziekenhuis Maastricht
Bart van den Heuvel	Universiteit Maastricht
Peter Oost	Erasmus Universiteit
Menno Nonhebel	KNAW
Martin Romijn	Hogeschool Utrecht
Alf Moens	TU Delft

Daarnaast heeft Jan Ploeg (ministerie van VROM) teksten aangeleverd, die zijn gebaseerd op de door hem geschreven thesis 'Kleine stappen en toch snel(ler) thuis', waarvoor SURFibo hem veel dank verschuldigd is.

Bij de totstandkoming van deze Starterkit is Mark Hoevers van IGI Group ingeschakeld als ghostwriter.

8. Bijlagen

Bijlage 1. Literatuuroverzicht

- British Standard 25999-1: 2006 Business Continuity Management – Part 1: Code of Practice, ICS 03.100.01, ISBN 0 580 49601 5
- British Standard 25999-2: 2007 Business Continuity Management – Part 2: Specification, ICS 03.100.01, ISBN 0 580 59913 2
- Nederlandse norm NEN-ISO/IEC 27002 Informatietechnologie – Beveiligingstechnieken – Code voor Informatiebeveiliging, ICS 35.040, ISBN 0 580 59913 2
- BSI-Standard 100-4, 2008 Bundesamt für Sicherheit in der Informationstechnik (BSI)
- NIST 800-34, Contingency Planning for Information Technology Systems June 2002
- NFPA 1600, Standard on Disaster/Emergency Management and Business Continuity Programs, 2007 Edition
- OAS 77: 2006, IT Service Continuity Management, Code of Practice, ICS 35.020, ISBN 0 580 49047 5
- ENISA, Business and IT Continuity: Overview and Implementation Principles, version 1.1, February 2008
- Business Continuity Management – weg van de gebaande paden; Jacques Cazemier, Dick Leegwater en Jan Ploeg, ISBN 9789012582292

Bijlage 2. Typen incidenten

- Brand met escalatiemodel van kleine naar grote brand
- Bommelding / bomalarm
- Poststukken met mogelijk gevaarlijke stoffen, als Antrax
- Storing bedrijfsvoering, waaronder:
    - Staking
    - Demonstratie
    - Blokkades
    - Bezetting
    - Sabotage
    - Vernieling / vandalisme
    - Grootschalige ziekte
- Incidenten met geweld, waaronder:
    - Gebruik van (vuur)wapens
    - Bedreiging / afpersing
    - Gijzeling
- Technisch falen:
    - Uitstroom gevaarlijke stoffen binnen de instelling
    - Uitstroom gevaarlijke stoffen buiten de instelling
    - Ongelukken met liften
    - Nutsonderbrekingen
    - Uitval ICT voorziening
    - Ongevallen
- Weerinvloeden:
    - Extreme warmte
    - Extreme koude
    - Extreme wind-, sneeuw- of wateroverlast
- Interne verstoring:
    - Besmetting met bacteriën (legionella / salmonella)
    - Besmetting drinkwater
    - Systeemstoringen die gezondheidsproblemen kunnen veroorzaken
    - Zelfdoding
- Deel- en totale ontruiming / evacuatie
- Financiële calamiteiten:
    - Diefstal
    - Fraude
    - Non-beschikbaarheid tegoeden

Bijlage 3. Index voor bijlagendocument

1. Inhoudsopgave BCM-beleid en -strategie
2. Inhoudsopgave Crisismanagementplan
3. Inhoudsopgave Crisiscommunicatieplan
4. Inhoudsopgave Bedrijfscontinuïteitsplan
5. Inhoudsopgave Beheerplan Bedrijfscontinuïteit
6. Voorbeeld oefenkalender
7. Inhoudsopgave Calamiteitenplan
8. Inhoudsopgave Crisis- en calamiteitenorganisatie
9. Beschrijving van kritieke processen
10. Voorbeeld logboek met besluitenlijsten
11. Checklist hoofdstappen tijdens crisis en daarna
12. Info card met noodzakelijke gegevens
13. Alarmeringslijst / oproeplijst
14. Inhoud calamiteitenkast en calamiteitenkoffer
15. Profiel escalatie- / crisismanager
16. Overdracht van werkzaamheden na een calamiteit
17. Praktische zaken die vaak vergeten worden
18. Modelplanning (stap 7)