



Bent u  
voorbereid op  
uitval van  
elektriciteit  
of ICT?

Handleiding  
**continuïteitsmanagement  
voor organisaties met een vitale  
maatschappelijke functie**

## Voorwoord

Vóór u ligt de handleiding continuïteitsmanagement 'Bent u voorbereid op uitval van elektriciteit en ICT?'. Ik bedank de deelnemers uit de vitale sectoren die in werksessies hebben bijgedragen aan deze handleiding en de doelgroepspecifieke documenten. De ervaringen van enkele bedrijven, gemeenten, provincies, ministeries, waterschappen en politie- en veiligheidsregio's vormen de basis voor deze producten. Producten die ons allemaal helpen om het continuïteitsmanagement in onze eigen organisatie verder vorm te geven.

De moderne mens is steeds meer afhankelijk van elektriciteit of ICT. Een uitval of verstoring heeft grote gevolgen voor ons dagelijks leven. Daarom is het belangrijk dat organisaties met een maatschappelijke taak, de vitale sectoren, zich voorbereiden op deze situaties. Niet alleen omdat het voor het eigen werk belangrijk is dat ze altijd doordraaien, maar ook omdat hun werk voor het functioneren van de samenleving zo ontzettend belangrijk is. Door ons grondig voor te bereiden, kunnen we voorkomen dat zaken escaleren. We moeten "het dak repareren als het droog is."

U doet dit niet voor niets. In 2009 hebt u zich als vitale sector al voorbereid op een mogelijke griepvloed naar aanleiding van de uitkomsten van de Nationale risicobeoordeling. Bij deze dreiging is continuïteitsmanagement grootschalig en bewust ingezet als instrument. Dit heeft geleid tot het concrete resultaat dat tachtig procent van de vitale organisaties eind 2009 een continuïteitsplan voor griep had. Velen van u hebben toen ervaren hoe belangrijk het is om terug te kunnen vallen op een continuïteitsplan tijdens de griep AH1N1.

Aantasting van de cybersecurity is nu één van de grootste dreigingen, daar willen we op voorbereid zijn. Samen met u zullen we er daarom zorg voor dragen dat de organisaties binnen de sectoren Openbare Orde en Veiligheid en Openbaar Bestuur eind 2011 een continuïteitsplan hebben gericht op de verstoring van ICT en elektriciteit.

Ik roep u dan ook op om een continuïteitsplan te maken, zodat we voorbereid zijn en we de kans op maatschappelijke ontwrichting verkleinen. Ik heb er vertrouwen in dat deze handleiding u hierbij zal helpen.

Ik wens u veel succes bij uw voorbereidingen.

Dick Schoof  
*Directeur-Generaal Veiligheid*  
*Ministerie van Veiligheid en Justitie*

Den Haag, december 2010

## Inhoudsopgave

	Voorwoord — 2
	Inhoudsopgave — 3
	Inleiding — 5
<b>1</b>	<b>Uitval van elektriciteit en ICT: twee nauw verbonden risicotypen — 7</b>
	Inleiding — 7
1.1	ICT uitval — 7
1.1.1	Oorzaken — 7
1.1.2	Impact — 8
1.2	Elektriciteitsuitval — 10
1.2.1	Oorzaken — 10
1.2.2	Impact — 11
1.3	Grootte van de impact: situationele risicofactoren — 12
1.4	Uitval van elektriciteit en ICT: overzicht impact organisatie en samenleving — 14
1.4.1	De impact op organisaties — 14
1.4.2	De impact op de samenleving — 16
<b>2</b>	<b>De meerwaarde van continuïteitsmanagement voor organisaties met een vitale maatschappelijke functie — 18</b>
	Inleiding — 18
2.1	Waarom moet mijn organisatie zich voorbereiden op uitval van elektriciteit of ICT? — 18
2.2	Wat is continuïteitsmanagement? — 18
2.3	Wat is de meerwaarde van continuïteitsmanagement voor uw organisatie? — 19
2.4	Hoe verhoudt continuïteitsmanagement zich tot risicomanagement? — 20
2.5	Hoe verhoudt continuïteitsmanagement zich tot crisismanagement? — 20
<b>3</b>	<b>Starten met continuïteitsmanagement: zes essentiële stappen — 22</b>
	Inleiding — 22
Stap 1	Randvoorwaarden voor continuïteitsmanagement — 23
Stap 2	Organisatie-analyse: ken uw organisatie (...écht!) — 23
Stap 3	Impactanalyse: weet wat u te wachten staat — 25
Stap 4	Formuleer de continuïteitsstrategie van uw organisatie — 27
Stap 5	Ontwikkel het continuïteitsplan voor uw organisatie — 29
Stap 6	Test uw continuïteitsvoorzieningen, train uw organisatie — 30
Bijlage 1	Impactanalyse Toolkit: stel zelf de impact van uitval voor uw organisatie vast — 32
Bijlage 2	Model continuïteitsstrategie — 36
Bijlage 3	Model continuïteitsplan — 40

## Inleiding

Verstoring van de ICT en elektriciteit vormen actuele en voorname risico's voor organisatie en samenleving. De toenemende afhankelijkheid van ICT en elektriciteit schept enerzijds nieuwe en voorheen ongekende mogelijkheden. Anderzijds maken deze mogelijkheden ons ook in toenemende mate kwetsbaar. Dat geldt ook voor uw organisatie. De nationale en internationale voorbeelden van ICT en elektriciteitsuitval zijn rijk en nemen snel toe. Uitval is dan ook allesbehalve ondenkbaar.

Elektriciteit en ICT vervullen voor onze samenleving vitale functies. Beide infra-structuren zijn bovendien in toenemende mate met elkaar verweven. De wederzijdse afhankelijkheid tussen ICT en elektriciteit is groot en bovendien groeiende. Uitval van elektriciteit heeft onherroepelijk gevolgen voor ICT. Andersom functioneren elektriciteitsvoorzieningen ook in toenemende mate ICT-gedreven. Uitval van ICT kan daarom evengoed leiden tot uitval van elektriciteit.

De impact van uitval wordt vaak onderschat. Maar schetst u voor uw organisatie de scenario's die passen bij deze risico's, dan zult u concluderen dat de continuïteit van uw maatschappelijke dienstverlening al snel in het geding raakt. Daarbij komt dat het hervatten van de ICT- en elektriciteitsvoorzieningen veelal geen kwestie is van 'even een reparatie uitvoeren'. Het herstel neemt doorgaans geruime tijd in beslag. Dit geldt ook voor de volledige terugkeer naar de reguliere omstandigheden.

Uitval is niet iets dat u zomaar overkomt of wat u lijdzaam moet ondergaan. U kunt uitval voorkomen en uw organisatie beter wapenen voor als de verstoring daadwerkelijk optreedt. U kunt kortom, de risico's en schade voor uw organisatie en de samenleving beperken of zelfs wegnemen. Continuïteitsmanagement biedt u namelijk een beproefde werkwijze om gevaar, schade en verlies voor uw organisatie te voorkomen. Ook waar het andere continuïteitsrisico's zoals bijvoorbeeld brand, extreme weersomstandigheden, overstromingsrisico's of een ziektegolf betreft.

Deze handleiding biedt u handvatten om uw organisatie beter te wapenen tegen allerlei bedreigingen voor haar continuïteit en in het bijzonder tegen de uitval van elektriciteit en ICT. Het doel van deze handleiding is driedig:

- In de eerste plaats willen wij u bewust maken van de risico's van ICT en elektriciteitsuitval
- In de tweede plaats willen wij het belang van continuïteitsmanagement onderbouwen
- In de derde plaats willen wij u ondersteunen bij het invullen en inbedden van continuïteitsmanagement én daarmee het reduceren van de risico's van ICT en elektriciteitsuitval

Deze doelen komen achtereenvolgens in de hoofdstukken van deze handleiding aan bod.

Hoofdstuk 1 vergroot uw inzicht in de oorzaken en gevolgen van ICT- en elektriciteitsuitval. De informatie in dit hoofdstuk is ontleend aan een groot aantal binnen- en buitenlandse praktijkcases van ICT- en elektriciteitsuitval. Dit hoofdstuk biedt u de aangrijpingspunten om na te gaan wat dergelijke verstoringen betekenen voor de continuïteit van uw organisatie.

Hoofdstuk 2 verschaft u argumenten die het nut van continuïteitsmanagement in het algemeen – en in het licht van uitval van ICT of elektriciteit in het bijzonder – verhelderen. Deze argumenten zijn niet alleen bedoeld om u duidelijk te maken waarom continuïteitsmanagement van groot belang is. Tevens staan deze argumenten u als gebruiker ten dienst. U kunt deze bijvoorbeeld benutten om beslissers en andere belanghebbenden binnen uw organisatie van het nut en de noodzaak van continuïteitsmanagement te overtuigen.

Hoofdstuk 3 maakt u duidelijk wat u zelf kunt doen om continuïteitsmanagement voor uw organisatie nader invulling te geven. In dit hoofdstuk wordt aan de hand van zes stappen duidelijk gemaakt hoe u continuïteitsmanagement zelf in kunt bedden in uw organisatie. Deze stappen starten met de benodigde randvoorwaarden en eindigen met hoe u de kwaliteit van het continuïteitsmanagement van uw organisatie kunt controleren en verder verbeteren.

In aanvulling op hoofdstuk 3 is een aantal bijlagen toegevoegd. Deze bijlagen bevatten instrumenten waarmee u bijvoorbeeld zelf de impact van een verstoring voor uw organisatie inzichtelijk kunt krijgen. Maar hier vindt u ook formats voor bijvoorbeeld het continuïteitsplan voor uw organisatie.

**Andere ondersteuningsmiddelen: bewustmakingsfilm, brochure, hulpmiddel voor zelfanalyse en vervolgactie**

Naast deze handleiding heeft het Ministerie van Veiligheid & Justitie voor u een aantal andere ondersteuningsmiddelen ontwikkeld. Zo is er voor u en andere binnen uw organisatie een bewustmakingsfilm en –brochure beschikbaar. En in aanvulling op deze handleiding is er tevens een hulpmiddel ontwikkeld op basis waarvan u zelf kunt nagaan wat uw organisatie kan doen om haar continuïteit te waarborgen. Zowel in het licht van de risico's op uitval van ICT en elektriciteit, als ook in relatie tot andere continuïteitsrisico's. Naast een algemene versie van dit hulpmiddel heeft het ministerie voor een aantal typen organisaties specifieke hulpmiddelen laten ontwikkelen. Er zijn specifieke hulpmiddelen voor rijksoverheden, provincies, gemeente, waterschappen, veiligheidsregio's en politieregio's ontwikkeld. Deze hulpmiddelen zijn beschikbaar via: [www.nationale-veiligheid.nl](http://www.nationale-veiligheid.nl)

## 1 Uitval van elektriciteit en ICT: twee nauw verbonden risicotypen

### Inleiding

Elektriciteit en ICT vervullen voor onze samenleving vitale functies. Beide infra-structuren zijn bovendien in toenemende mate met elkaar verweven. De wederzijdse afhankelijkheid tussen ICT en elektriciteit is groot en groeiende. Uitval van elektriciteit heeft onherroepelijk gevolgen voor ICT. Andersom functioneren elektriciteitsvoorzieningen ook in toenemende ICT-gedreven. Uitval van ICT kan daarom ook evengoed leiden tot uitval van elektriciteit.

In dit hoofdstuk schetsen wij voor u in een beperkt aantal pagina's de belangrijkste kenmerken en bijzonderheden van ICT- en elektriciteitsuitval. Uitgangspunt daarbij is dat u de noodzakelijke kennis krijgt aangereikt om de impact van deze risico's voor uw organisatie goed in te kunnen schatten. We beschrijven beide risicotypen achtereenvolgens naar hun aard, oorzaken en impact. We maken daarbij telkens gebruik van illustratieve voorvallen en recente voorbeelden.

Vervolgens schetsen wij voor u enkele situationele risicofactoren die tezamen de impact van uitval voor uw organisatie en haar maatschappelijke dienstverlening bepalen. We besluiten het hoofdstuk met een tabel waarin we de impact van ICT- en elektriciteitsuitval voor organisatie en samenleving op overzichtelijke wijze samenvatten.

### 1.1 ICT uitval

Informatie- en communicatietechnologie – 'ICT' – is een lastig af te bakenen verzameling. Onder ICT verstaan we alle infrastructuur<sup>1</sup>, systemen, diensten en processen die het mogelijk maken informatie digitaal te verwerken, te gebruiken en te delen. We vinden ICT tegenwoordig nagenoeg overal terug. Thuis, in de vorm van onze desk- of laptop computer of in de vorm van (digitale) telefonie, televisie als ook de toegang tot Internet. Op ons werk, in de vorm van het bedrijfsnetwerk, de kantoorautomatisering, of bijvoorbeeld de betalings-, documentatie- of aansturingssystemen. En in de samenleving, in de vorm van onder meer allerlei verkeers-, vervoers- en regelsystemen of het bancaire-, fiscale- en boeteverkeer. Het aantal ICT-toepassingen lijkt eindeloos en neemt hand over hand toe. We spreken over uitval als de ICT verstoort raakt, stagneert of stopt en de continuïteit van organisaties of zelfs de gehele samenleving hierdoor negatief wordt beïnvloed.

#### 1.1.1 Oorzaken

Als landelijke netwerken, zoals het Internet of het telefonienetwerk verstoord raken, zijn uw dienstverleners mogelijk niet in staat om uw organisatie adequaat te bedienen. Wanneer uw organisatie in hoge mate afhankelijk is van deze dienstverlening – en dat geldt tegenwoordig vrijwel zonder uitzondering – dan raakt dit direct aan uw kernactiviteiten. Dergelijke verstoring of uitval heeft dan vertraging, financieel verlies en mogelijk ook schade ten gevolg. Uw organisatie kan vanzelfsprekend zelf ook te maken krijgen met uitval van ICT. Deze uitval kan verschillende vormen aannemen. Systeem- of menselijk falen kan uiteindelijk leiden tot uitval. Voorbeelden hiervan zijn gebrekkig onderhoud aan systemen of fouten in het ontwerp of de uitvoering van procedures.

<sup>1</sup> Fysieke netwerksystemen, waaronder het internet, telecomnetwerken, noodnet en het communicatienetwerk C2000.

**Landelijke telecomstoring, 2008**

Als gevolg van een interne storing in de ICT-omgeving van een telecom-provider ondervinden veel klanten problemen met het hun ADSL-verbinding en kunnen niet meer internetten, televisiekijken en/of bellen. Bij sommige bedrijven is geen telefoonverkeer mogelijk. Ook kan in veel winkels niet gepind worden. Naast het Internet werken ook enkele UMTS-masten niet meer. De storing is merkbaar in heel Nederland en duurt voor sommige afnemers bijna twee en een halve dag.

Maar ook moedwillige verstoring kan leiden tot uitval van ICT. Overheden, bedrijven en burgers worden in toenemende mate slachtoffer van gerichte virusinfecties of inbraak in computersystemen. Dergelijke vormen van kleine of meer georganiseerde cybercrime, spionage of zelfs cyberterrorisme kunnen uw ICT-omgeving flink verstoren. Dit heeft gevolgen voor de continuïteit van uw organisatie.

**ICT-storing bij een waterschap, 2010**

Een virusuitbraak in systemen van een waterschap besmet de computers op de werkplekken op het hoofdkantoor. Alle systemen zijn onbruikbaar. Een deel van de werkzaamheden moet gedurende vier dagen worden stilgelegd.

**1.1.2****Impact**

Dat organisaties hinder zullen ondervinden van ICT-uitval is evident. Ook is duidelijk dat ongeacht de aard en omvang van de uitval er sprake zal zijn van financiële schade, stagnatie, vertraging, overlast en irritatie. Zowel voor de getroffen organisatie, als voor de organisaties en personen die daarvan afhankelijk zijn. De onderlinge ketenafhankelijkheden zijn immers groot en groeiende.

**Impact op de organisatie**

ICT-uitval zal voor uw organisatie tot gevolg hebben dat een aantal van uw meest essentiële activiteiten niet, of slechts in beperkte mate, kan worden uitgevoerd. Dit kan leiden tot materiële schade, in de vorm van kosten voor herstelwerkzaamheden en het opeenstapelen van werkzaamheden als gevolg van olopende vertraging. De impact voor uw medewerkers is doorgaans groot. Zij moeten het werk staken en kunnen lang niet altijd terugvallen op alternatieve werkwijzen of -werkzaamheden. Hierdoor lopen zij achterstanden op en moeten zij klanten teleurstellen.

**ICT-storing bij een aantal politiekorpsen, 2010**

Een grootschalige ICT-storing bij een groot aantal politiekorpsen leidt er gedurende een lange periode toe dat meldingen en aangiften deels handmatig geregistreerd moeten worden. Ook voor andere processen moet de organisatie terugvallen op alternatieven. Reguliere werkzaamheden kunnen slechts met grote vertraging worden uitgevoerd. Het achteraf invoeren van handmatige registraties kost de betrokken organisaties zeer veel tijd.

Zowel bij moedwillige verstoringen als bij systeemfalen kunnen belangrijke en vertrouwelijke data verloren gaan. Terwijl het garanderen van integriteit van informatie van groot belang is voor medewerkers, klanten en derden. Bovendien kan uw organisatie ernstige schade oplopen wanneer gegevens verloren gaan, of in verkeerde handen komen. Uw betrouwbaarheid en goede reputatie lopen mogelijk averij op, en uw organisatie lijdt financiële schade en verlies.

**ICT-storing in een ziekenhuis, 2010**

Als gevolg van een gedeeltelijke uitval van ICT in een ziekenhuis heeft het personeel zorgen over de betrouwbaarheid van gegevens en cijfers in de nog wel actieve systemen. De integriteit van deze gegevens is van cruciaal belang voor goede en veilige patiëntenzorg.

**Impact op de samenleving**

Een verstoring van de ICT van uw organisatie kan uiteindelijk ook gevolgen hebben voor de samenleving. De volksgezondheid kan in het geding raken wanneer door ICT-uitval een ziekenhuis niet meer volledig functioneert of afvalwater in het oppervlaktewater terecht komt. En als de ICT-voorzieningen van bijvoorbeeld hulpdiensten niet werken, dan kan dit grote gevolgen hebben voor de openbare orde en veiligheid. Uitval van mobiele telefonie leidt er dan bijvoorbeeld toe dat hulpbehoevenden de meldkamer minder goed kunnen bereiken. En uitval van verbindingen kan leiden tot het ontbreken van communicatie met en tussen hulpverleningsdiensten en eventueel ook tot vertraagd optreden.

**ICT-storing in een ziekenhuis, 2009**

Als direct gevolg van elektriciteitsuitval valt het rekencentrum van een ziekenhuis uit. Het crisisteam besluit om alle poli's in het ziekenhuis voor twee dagen te sluiten. Alle patiënten worden persoonlijk, dan wel telefonisch over het sluiten van de poliklinieken geïnformeerd.

Recente cases van ICT-uitval maken duidelijk dat een snelle terugkeer naar de reguliere bedrijfsvoering vaak niet mogelijk is. Het diagnosticeren, repareren en gefaseerd opstarten, leiden meestal nog geruime tijd tot beperkte en instabiele beschikbaarheid.

## 1.2

### Elektriciteitsuitval

Hoewel Nederland een relatief betrouwbaar en redundant uitgevoerd distributienetwerk heeft, valt de elektriciteit gemiddeld dagelijks toch zo'n vijftig keer uit. De geleden vertraging kan per hoofd van de bevolking oplopen tot wel twintig minuten. Veelal krijgen we te maken met kleine storingen, waar overheden, bedrijven en burgers maar kort hinder van ondervinden. Grootschalige en langdurige storingen komen doorgaans minder vaak voor. Maar de impact van een grootschalige verstoring is enorm. Het leidt tot ontregeling van uw organisatie en potentiële ontwrichting van de samenleving.

#### Bron: EnergieNed, 2010

In 2009 vonden er 18.326 stroomonderbrekingen plaats. Gemiddeld waren dit er de afgelopen vijf jaar 18.065. Per storing werden in 2009 gemiddeld 140 klanten getroffen. Het gemiddelde over de afgelopen vijf jaar bedraagt 144. De belangrijkste oorzaak van stroomonderbrekingen zijn graafwerkzaamheden. In 2009 werd ruim 30% van de onderbrekingen hierdoor veroorzaakt. Dit percentage is iets lager dan voorgaande jaren. Gemiddeld vinden jaarlijks 1 tot 2 grote stroomstoringen plaats.

### 1.2.1

#### Oorzaken

Één van de belangrijkste oorzaken van elektriciteitsuitval is natuurgeweld, waaronder hevige aanhoudende sneeuwval, overstromingen, brand of storm. Onder deze omstandigheden blijkt de infrastructuur van het elektriciteitsnetwerk kwetsbaar. Bovendien vertragen slechte weersomstandigheden de herstelwerkzaamheden, waardoor een gebied voor een lange periode zonder elektriciteit kan komen te zitten. En dat juist onder omstandigheden waarin we de elektriciteit het meest nodig hebben.

#### Elektriciteitsuitval Haaksbergen, 2005

Hevige sneeuwval in het oosten en zuiden van Nederland en een stormachtige wind in het westen zorgen voor chaos. In Zeeland, Brabant, Limburg, Gelderland en Overijssel valt op meerdere plaatsen de elektriciteit uit. In en rond Haaksbergen veroorzaakt elektriciteitsuitval de grootste impact. Daar verblijven uiteindelijk 25.000 inwoners gemiddeld dertig tot maximaal eenenzestig uur zonder elektriciteit.

Tevens kan al dan niet bewust menselijk handelen of technisch falen aanleiding zijn voor uitval van elektriciteit. Onderhoudswerkzaamheden, diefstal of vernieling van onderdelen, veroorzaken met dagelijkse regelmaat uitval. Een bijkomend probleem is dat noodstroomvoorzieningen regelmatig niet functioneren. In dergelijke gevallen is uitval van elektriciteit tevens de oorzaak van uitval van ICT.

#### Elektriciteitsuitval Bommeler- en Tielerwaard, 2007

Een Apache-gevechtshelikopter vliegt in december 2007 tegen hoogspanningskabels boven de Gelderse Waal. Doordat de kabels breken, valt de elektriciteit in de regio Tieler- en Bommelerwaard uit. De uitval treft 50.000 huishoudens, veel bedrijven en het scheepvaartverkeer in de regio.

### 1.2.2

#### Impact

De recente, langduriger, nationale en internationale casus illustreren dat uitval van elektriciteit op kleine of grote schaal al snel ontwrichtende effecten kan hebben. Organisaties zijn onder omstandigheden van elektriciteitsuitval nauwelijks of niet in staat om te blijven functioneren en vallen nagenoeg stil. Dat geldt in nog grotere mate voor organisaties die een vitale maatschappelijke functie vervullen, omdat de continuïteit van hun dienstverlening juist onder moeilijke omstandigheden cruciaal is. Uitval van elektriciteit roept namelijk ook allerlei vervolgrisico's in het leven. Voor burgers – en dan in het bijzonder kwetsbare burgers – maar ook voor de algehele veiligheids-, gezondheids- en milieusituatie. Bovendien resulteert elektriciteitsuitval in forse schadeposten.

#### Impact op de organisatie

Tijdens uitval van elektriciteit is communicatie met voor u belangrijke doelgroepen cruciaal. Dit zijn de medewerkers van uw organisatie, uw klanten, burgers en partners. Uitval van elektriciteit leidt niet zelden tot uitval van Internet, radio, televisie en telefonie. Uw organisatie kan in de situatie komen waarin communiceren meer dan ooit noodzakelijk is, maar tegelijkertijd sterk bemoeilijkt wordt. Getroffen burgers, bedrijven en overheden zullen middels crisisbeheersing gezamenlijk inspanningen moeten verrichten om de ergste nood te lenigen.

#### Elektriciteitsuitval Geldermalsen, 2007

Het inzetten van de crisiscommunicatiemiddelen tijdens de uitval blijkt lastig. Door de uitval kan een groot deel van de doelgroep niet bereikt worden via de televisie, radio en via Internet. De gemeente moet terugvallen op 'ouderwetse' middelen, zoals de geluidswagen en het verspreiden van papieren informatieberichten.

Uitval kan uw organisatie sterk ontregelen. Herstel na een stroomstoring duurt vaak langer dan de uitval zelf. Net als geldt voor ICT-uitval, kan diagnose soms veel tijd in beslag nemen. Verder vergt het opstarten na de storing mogelijk de inzet van (schaarse) externe deskundigheid om de ontregelde apparatuur weer gebruiksklaar te krijgen. De kosten voor herstel en het verlies van productiviteit zijn doorgaans fors. Een verstoring van uw organisatie kan echter ook betekenen dat uw maatschappelijke taken in het geding komen. En minstens zo vervelend is het wanneer u betrouwbare imago schade oploopt door een gebrek aan voorbereiding op – en handelen tijdens – elektriciteitsuitval.

**Impact op de samenleving**

Uitval van elektriciteit heeft grote impact op de samenleving. Burgers kunnen bij slechte weersomstandigheden letterlijk in de kou zitten. Hoewel de ervaring leert dat de zelfredzaamheid van burgers tijdens uitval groot is, lopen kwetsbare groepen (zieken, ouderen, invaliden) onder deze omstandigheden een verhoogd risico.

<b>Elektriciteitsuitval Haaksbergen, 2005</b>
Enkele verzorgingstehuizen hebben onvoldoende werkende noodstroomcapaciteit. De gemeente geeft daarom voorrang bij de toedeling van de schaarse noodstroomvoorzieningen die in de regio beschikbaar is.

De openbare orde en veiligheid kunnen in het geding komen wanneer verkeerssignalering uitvalt, alarminstallaties van organisaties massaal afgaan, of mensen vast komen te zitten in liften. Ook kunnen andere risicovolle situaties voor mens, milieu en dier ontstaan. Patiënten die thuis afhankelijk zijn van zuurstof- of dialyseapparatuur lopen mogelijk gevaar en de drinkwatervoorziening kan kwalitatief of kwantitatief stagneren.

<b>Elektriciteitsuitval Bommeler- en Tieleraard, 2007</b>
Door het uitvallen van de elektriciteitsvoorziening moest de politie een Tbs-kliniek continu extra bewaken. Ook winkels zijn door de politie extra beveiligd. Enkele bedrijven zetten bewakers in omdat ze bang zijn voor diefstal als gevolg van de uitval van de beveiligingssystemen.

**1.3**

**Grootte van de impact: situationele risicofactoren**

De ernst en impact van ICT- of elektriciteitsuitval kunnen sterk uiteenlopen, afhankelijk van de situatie. De volgende risicofactoren helpen u bij het inschatten van de mogelijke impact van uitval op uw organisatie.

<b>Risicofactor</b>	<b>Toelichting</b>
Aard van de uitval	De impact van en reactie op menselijk- of systeemfalen ('een fout'), zal in de regel afwijken van de impact van bewust menselijk handelen ('een moedwillige verstoring')
Gedeeltelijke versus volledige uitval	Een volledige uitval werkt in hogere mate verstrend voor het kunnen uitvoeren van de kerntaken van organisaties. Een gedeeltelijke uitval levert voornamelijk vertraging op
Tijdstip en duur van de uitval	Afhankelijk van uw organisatie kunnen er momenten zijn waarop de uitval een grotere, dan wel kleinere impact heeft op uw kritieke processen. Naarmate de uitval langer duurt, zullen de effecten doorgaans groter zijn
Demografische situatie	Naarmate de uitval een grotere groep burgers en organisaties raakt, neemt de impact van de uitval toe
Andere incidenten of storingen	Een combinatie van storingen, of een gelijktijdig optreden van incidenten of calamiteiten vergroot de impact van de uitval
Verwevenheid met - en afhankelijkheid van derden	Indien ICT-processen in verbinding staan met processen van andere organisaties of niet kunnen functioneren zonder deze processen, dan is de impact van de uitval groter dan wanneer ze zelfstandig kunnen functioneren
Hoeveelheid kritieke processen	Indien de uitval meerdere kritieke processen verstoort, zal de impact groter zijn
Ontbreken of falen van preventieve en reactieve maatregelen	Het ontbreken of falen van maatregelen vergroot de negatieve consequenties van de uitval
Weersomstandigheden	Specifieke weersomstandigheden kunnen de impact van uitval vergroten. Denk aan aanhoudende hitte, koude of (extreme) neerslag
Geografische omvang	De geografische omvang van de uitval is mede bepalend voor de ernst van de effectwerking
Specifieke omgevingskenmerken	Specifieke omgevingskenmerken kunnen de ernst van de uitval vergroten. Denk aan de nabijheid van bepaalde (zware) industrie, het stedelijke (veel mensen) of juist landelijke karakter (veel dieren) van de omgeving



## 1.4 Uitval van elektriciteit en ICT: overzicht impact organisatie en samenleving

### 1.4.1 De impact op organisaties

Uw organisatie kan op verschillende manieren hinder, overlast en schade onder- vinden van de uitval van elektriciteit of ICT. De onder vermelde tabel maakt duidelijk met welke gevolgen uw organisatie geconfronteerd kan worden. Hoewel het overzicht is gebaseerd op uitgebreid nationaal en internationaal onderzoek, is het vanzelfsprekend niet uitputtend. Het overzicht dient vooral om voor u inzichtelijk te maken voor welke gevolgen een verstoring de organisatie stelt.

ICT
<ul style="list-style-type: none"> <li>• Uitval van kantoorautomatisering</li> <li>• Verminderde toegang tot administratieve-, documentaire-, post- en andere gegevensdragende systemen</li> <li>• Stagnatie of uitval van systemen benodigd voor de aansturing van (primaire) processen</li> <li>• Verlies, diefstal of aantasting van (gevoelige) informatie, ofwel onzekerheid over de betrouwbaarheid of integriteit van deze informatie</li> </ul>
Communicatie
<ul style="list-style-type: none"> <li>• Toenemende behoefte aan duiding over oorzaak en duur van de storing bij klanten, burgers en andere derden</li> <li>• Verminderde mogelijkheden voor communicatie met klanten, burgers en andere derden</li> <li>• Uitval van massacommunicatiemiddelen (televisie, email, intranet, Internet, sms)</li> <li>• Verminderde mogelijkheden tot interne communicatie</li> </ul>
Derden
<ul style="list-style-type: none"> <li>• Verminderde beschikbaarheid van derden voor ondersteuning en onderhoud</li> <li>• Stagnatie essentiële activiteiten door (grote) afhankelijkheid derden</li> <li>• Ontregeling van distributie- en bevoorradingsprocessen</li> <li>• Keteneffecten bij klanten of toeleveranciers</li> </ul>
Financiën
<ul style="list-style-type: none"> <li>• Stagnatie van het betalingsverkeer van – en naar – uw organisatie</li> <li>• Inkomstenderving door (forse) daling van de arbeidsproductiviteit</li> <li>• Snel oplopende kosten ten behoeve van herstel en normalisatie van de bedrijfsvoering</li> <li>• Schadeclaims van klanten of gedupeerden</li> </ul>

Bedrijfsvoering
<ul style="list-style-type: none"> <li>• Verstoring van de continuïteit van uw kernactiviteiten</li> <li>• Stagnatie in de uitvoering van publieke taken en maatschappelijke dienstverlening</li> <li>• Spanning op de naleving van wettelijke termijnen, niet-naleving</li> <li>• Verminderde mogelijkheden tot uitvoering van handhavingstaken</li> <li>• Reputatieschade als gevolg van gebrekkige voorbereiding op – of handelen tijdens – uitval</li> <li>• Vertraging en extra werk door handmatig uitvoeren van werkzaamheden</li> <li>• Verhindering en vertraging van democratische- en politiekbestuurlijke processen</li> <li>• Verminderde mobiliteit bij medewerkers als gevolg van verkeerscongestie</li> <li>• Afname personele capaciteit vanwege het door medewerkers waarnemen van zorgtaken voor minder zelfredzame naasten</li> <li>• Uitval van personeel door slechte arbeidsomstandigheden bij uitval van licht-, warmte-, verkoelings- of luchtzuiveringsvoorziening</li> </ul>
Veiligheid
<ul style="list-style-type: none"> <li>• Verslechtering van de veiligheids- en beveiligingssituatie van de organisatie</li> <li>• Afname van de mogelijkheden en slagkracht van de bedrijfshulpverlening en de bereikbaarheid van hulpdiensten</li> <li>• Uitval van geautomatiseerde (elektronische- en ICT) beveiligingsmaatregelen</li> <li>• Mogelijk risicovolle situaties voor werknemers als gevolg van herstelwerkzaamheden</li> </ul>
Herstel
<ul style="list-style-type: none"> <li>• Schaarste in kennis, expertise en middelen voor herstelwerkzaamheden</li> <li>• Soms langdurig herstel en normalisatie, tijdelijke instabiliteit leveringszekerheid of ontoegankelijkheid systemen</li> <li>• Additionele personele inzet voor het bestrijden van oorzaken, effecten en voor bespoediging van herstel</li> </ul>



1.4.2

*De impact op de samenleving*

Uitval heeft vanzelfsprekend ook gevolgen voor de samenleving. Het is enerzijds mogelijk dat de bron van uitval binnen uw organisatie ligt en u daardoor verminderd of niet in staat bent om publieke taken voort te zetten. Anderzijds kan er sprake zijn van grootschalige uitval waardoor uw organisatie 'mede-eigenaar' wordt van de effecten. De onderstaande tabel maakt duidelijk welke maatschappelijke gevolgen kunnen optreden als gevolg van uitval van elektriciteit en/of ICT. Ook voor dit overzicht geldt een voorbehoud voor wat betreft de volledigheid.

Hulpvraag
<ul style="list-style-type: none"> <li>Toename in behoefte aan opvang en verzorging</li> <li>Grotere aanspraak op de zelfredzaamheid van burgers</li> <li>Verhoogde hulpvraag bij minder zelfredzamen en kwetsbare groepen</li> <li>Groter aantal meldingen van burgers over brand, opsluiting of storing-gerelateerde vragen</li> </ul>
Communicatie
<ul style="list-style-type: none"> <li>Verminderde communicatiemogelijkheden van burgers door uitval van (vaste en mobiele) telefonie, internet en andere kanalen</li> <li>Verminderde bereikbaarheid van de meldkamer, hulpverleningsdiensten, zorginstellingen, gemeenten en andere overheden door uitval van communicatiemiddelen</li> </ul>
Schaarste
<ul style="list-style-type: none"> <li>Grote inzet van storingsmonteurs voor het verhelpen van ontregelde CV-installaties, thermostaten en alarmsystemen</li> <li>Schaarste van noodstroomvoorzieningen</li> <li>Versneld bederf van beperkt houdbare en kwetsbare producten door uitval van koelsystemen</li> <li>Verminderde watertoevoer in hoogbouw en in blusinstallaties door wegvallen waterdruk</li> </ul>
Milieu
<ul style="list-style-type: none"> <li>Uitval of verslechtering van de drinkwatervoorziening</li> <li>Lozing van ongezuiverd afvalwater op het oppervlaktewater, in rivieren, meren en bij publieke badplaatsen</li> <li>Effecten voor het dierenwelzijn (mogelijk zelfs diersterfte) bij veeteelt-bedrijven door het uitvallen van klimaatbeheersing</li> </ul>
Mobiliteit
<ul style="list-style-type: none"> <li>Verkeerscongestie of chaos op drukke verkeersknooppunten en in steden</li> <li>Beperking of stagnatie van vervoer van goederen op vaarwegen, spoorwegen en luchtwegen</li> <li>Verminderde mobiliteit door gedeeltelijk of volledige uitval van het openbaar vervoer</li> </ul>

Gezondheid
<ul style="list-style-type: none"> <li>Sluiten van poliklinieken in ziekenhuizen, mogelijke gevolgen voor spoedeisende hulp of intensive care</li> <li>Uitval van medische apparatuur bij mensen thuis</li> <li>Gevolgen voor de leefsituatie in gesloten inrichtingen</li> <li>Uitval van klimaatbeheersing in woningen en kantoorpanden</li> </ul>
Veiligheid
<ul style="list-style-type: none"> <li>Uitval van beveiligingssystemen en maatregelen ten behoeve van de toegangsverlening</li> <li>Maatschappelijke onrust of ordeverstoringen vanwege de uitval en gevolgen</li> <li>Vervolgrisco's externe veiligheid door afschakeling (zware) industrie als ook voor de opslag en het vervoer van gevaarlijke stoffen</li> <li>Uitval van veiligheidssystemen bij spoorwegovergangen</li> </ul>
Economie
<ul style="list-style-type: none"> <li>Verstoring van de import en export</li> <li>Vertraging van belastingteruggave</li> <li>Verstoring van het betalingsverkeer en beperking van betaalmogelijkheden in winkels en bij pinautomaten</li> </ul>

## 2 De meerwaarde van continuïteitsmanagement voor organisaties met een vitale maatschappelijke functie

### Inleiding

In hoofdstuk 1 schetsten we de oorzaken en mogelijke impact van ICT- en elektriciteitsuitval voor uw organisatie en de samenleving. Deze twee risicotypen bedreigen de continuïteit van uw organisatie.

Het doel van dit hoofdstuk is daarom u te informeren over het nut en de noodzaak van continuïteitsmanagement. U kunt de inzichten uit dit hoofdstuk tevens gebruiken om beslissers en andere belanghebbenden binnen uw organisatie te informeren over het belang van continuïteitsmanagement en een goede toerusting van de organisatie op continuïteitsrisico's.

### 2.1 Waarom moet mijn organisatie zich voorbereiden op uitval van elektriciteit of ICT?

Het voorgaande hoofdstuk biedt een passende illustratie bij deze vraag: deze vormen van uitval kunnen niet alleen potentieel verstrekkende gevolgen hebben voor de continuïteit van uw organisatie maar ook voor de samenleving. Bovendien is het verre van ondenkbaar dat uw organisatie te kampen krijgt met een verstoring door (grootschalige) uitval van de ICT of elektriciteit.

Desondanks is het bewustzijn van de risico's van ICT- of elektriciteitsuitval momenteel nog beperkt. Dit geldt vooral voor het zicht op en bewustzijn van de risico's van ICT-uitval. Dat heeft deels te maken met het specialistische karakter van de materie: veel mensen haken af zodra het (te) technisch wordt. Daarnaast is dit risico, net als de onderliggende structuur, in hoge mate onzichtbaar en virtueel. Het is daardoor – letterlijk – lastig om een goed beeld te vormen van de precieze impact van ICT-uitval.

Niettemin vormt verstoring van de ICT-infrastructuur één van de meest actuele en voorname risico's voor organisatie en samenleving. Zoals eerder geschetst, maakt onze toenemende afhankelijkheid van ICT ons ook in toenemende mate kwetsbaar. Afhankelijkheden die op hun beurt weer nieuwe risico's in het leven roepen. ICT vormt steeds meer het wezen van onze werk- en communicatiewijzen. Dat geldt zonder twijfel ook voor uw organisatie. Bovendien vormt de virtuele wereld een plaats waar nieuwe vormen van criminaliteit en conflict worden ontwikkeld en zich verder manifesteren. De nationale en internationale voorbeelden van ICT-uitval zijn rijk en groeien snel. En nog meer dan het geval is voor elektriciteitsuitval, vormt ICT-uitval een nadrukkelijk groot en waarschijnlijk risico voor organisatie en samenleving.

Schetst u voor uw organisatie de scenario's die passen bij deze risico's, en u zult concluderen dat de continuïteit van uw maatschappelijke dienstverlening al snel in het geding raakt. Daarbij komt dat het hervatten van de ICT- en elektriciteitsvoorzieningen veelal geen kwestie is van 'even een reparatie uitvoeren'. Het herstel neemt doorgaans geruime tijd in beslag. Dit geldt ook voor de volledige terugkeer naar de reguliere omstandigheden.

### 2.2 Wat is continuïteitsmanagement?

Continuïteitsmanagement is een verbijzondering van business continuity management (BCM) voor organisaties met een (semi-)publiek karakter. Continuïteitsmanagement is een managementstrategie gericht op het beperken van

schade als gevolg van het verlies van de continuïteit van uw bedrijfsvoering. Denk aan de gevolgen van risico's als brand, extreme weersomstandigheden, overstroming, elektriciteitsuitval en ICT-verstoringen. Continuïteitsmanagement stelt daarbij vier centrale problemen centraal: gebrek aan personeel, gebrek aan toegang tot faciliteiten, gebrek aan vitale data en gebrek aan ICT-infrastructuur.

Continuïteitsmanagement vestigt de aandacht op het voorbereiden op eventueel continuïteitsverlies door risico's te vermijden of de impact zoveel mogelijk te beperken (omschakelen, overschakelen, redundant uitvoeren et cetera). Daarnaast gaat het bij continuïteitsmanagement om het adequaat kunnen reageren op een daadwerkelijke verstoring en het realiseren van een zo spoedig mogelijk herstel.

Continuïteitsmanagement is geen wetenschap, maar een werkwijze ontwikkeld in de praktijk. Dit maakt dat de principes van continuïteitsmanagement voor allerlei typen organisaties goed en makkelijk toepasbaar zijn. Bovendien is continuïteitsmanagement niet statisch maar praktijkgedreven. Dit heeft tot gevolg dat continuïteitsmanagement op basis van wereldwijd opgedane ervaringen steeds verder professionaliseert, getuige bijvoorbeeld de inmiddels verscheidene kwaliteitsstandaarden voor continuïteitsmanagement.

Mocht u zich nader willen verdiepen in continuïteitsmanagement dan raden wij u aan één van de beschikbare handboeken (bijvoorbeeld 'The definitive handbook of Business Continuity Management' Hiles et al: 2007) of kwaliteitsstandaarden voor continuïteitsmanagement (bijvoorbeeld BS 25999 Business Continuity) danwel informatiebeveiliging te raadplegen.

### 2.3 Wat is de meerwaarde van continuïteitsmanagement voor uw organisatie?

Hoewel BCM als managementstrategie is ontstaan in het bedrijfsleven, zijn de principes breder toepasbaar – juist ook voor organisaties waar een winst oogmerk ontbreekt. Ook voor deze organisaties geldt immers dat het kunnen garanderen van de essentiële activiteiten van groot belang is. Sterker nog, we zouden kunnen betogen dat, juist vanwege hun vitale publieke taak, continuïteitsmanagement zelfs nog van groter belang is voor organisaties in het publieke domein. Voor een organisatie met vitale maatschappelijke taken is het immers van cruciaal belang dat de organisatie ongestoord kan blijven doorfunctioneren.

Continuïteitsmanagement helpt nodeloze overlast, vertraging, schade en verliezen te voorkomen. Dit maakt continuïteitsmanagement tot een belangrijk instrument om in tijden van 'ombuiging' en afslanking de financiële impact van verstoringen te voorkomen. Juist ook voor organisaties die een cruciale publieke taak vervullen. Continuïteitsmanagement verdient zichzelf, mits serieus en adequaat toegepast, ruimschoots terug.

Bovendien stelt continuïteitsmanagement uw organisatie in staat om de betrouwbaarheid van uw dienstverlening te vergroten. Een aspect dat direct samenhangt met de reputatie van uw organisatie. Zolang u in staat bent om de continuïteit van uw dienstverlening aan burgers en andere klanten te garanderen, zult u het imago van een betrouwbare dienstverlener of samenwerkingspartner hebben. Heeft uw organisatie te kampen met in principe voorzienbare en voorkombare continuïteitsproblemen, dan straalt dit zonder twijfel negatief af op de reputatie van uw organisatie.

Bezien vanuit het oogpunt van kwaliteit, is continuïteitsmanagement onderdeel van uw integrale kwaliteitszorg. Het is voor de kwaliteit van uw maatschappelijke – en mogelijk andere – dienstverlening essentieel dat u in staat bent om onder andere leveringszekerheid te kunnen garanderen. Continuïteitsmanagement stelt uw organisatie in staat om deze zekerheid te vergroten.

Continuïteitsmanagement biedt uw complexe en getrapte organisatie tevens een werkwijze die in staat stelt om gecoördineerd op te treden. De ervaring leert dat continuïteitsverstoringen in de regel de gehele organisatie treffen maar dat organisaties hier vanwege toegenomen specialisatie niet op zijn ingericht. Door continuïteitsmanagement in te bedden verzekert u de organisatie van een structuur die het mogelijk maakt om als organisatie verenigd en slagvaardig te kunnen handelen.

Tot slot is het goed om te benadrukken dat continuïteitsmanagement in opkomst is en in de toekomst naar verwachting alleen maar meer aandacht zal genieten. Enerzijds vanwege de steeds verder toenemend afhankelijkheden in onze samenleving en tussen netwerkpartners. Anderzijds ook vanuit de trend om meer risicogestuurd te willen werken en daarmee ongewenste gebeurtenissen in een zo vroegtijdig mogelijk stadium te beheersen.

#### **2.4 Hoe verhoudt continuïteitsmanagement zich tot risicomanagement?**

Continuïteitsmanagement is onderdeel van uw integraal risicomanagement. Risicomanagement is de laatste jaren in opkomst – ook in de publieke sector. De drijvende gedachte hierachter is simpel: liever voorkomen we ongewenste gebeurtenissen door deze vroegtijdig te signaleren, weg te nemen of zoveel en adequaat mogelijk te beheersen, dan later met de daaruit voortvloeiende incidenten of crises te worden geconfronteerd. Risicomanagement biedt overigens ook aangrijpingspunten voor het voorbereiden en omgaan met incidenten en crises. Hoewel risicomanagement aanvankelijk vooral gericht was op het beheersen van risico's van financieel-economische aard, is de afgelopen jaren een verschuiving waarneembaar. Steeds vaker is er vanuit risicomanagement aandacht voor 'operationele risico's' waaronder naast veiligheids- ook nadrukkelijk continuïteitsrisico's. Vanuit dat gezichtspunt is continuïteitsmanagement hét instrument waarmee u risico's voor de continuïteit van uw organisatie kunt reduceren en beheersen.

#### **2.5 Hoe verhoudt continuïteitsmanagement zich tot crisismanagement?**

De kans is groot dat u zich inmiddels afvraagt hoe continuïteitsmanagement zich verhoudt tot crisismanagement. Deze laatste managementstrategie is immers ook bedoeld om de gevolgen van ongewenste gebeurtenissen zoveel mogelijk te reduceren. Bovendien is de kans groot dat uw organisatie structureel aandacht besteedt aan crisismanagement. Zo kan er een crisismanagementorganisatie zijn ingericht, zijn er plannen voorbereid, wordt er mogelijk met enige regelmaat geoefend en is deze organisatie waarschijnlijk ook geactiveerd onder omstandigheden van (dreigende) crises. Voor veel organisaties in de (semi)publieke sector is crisismanagement al in meerdere of mindere mate een gevestigde praktijk.

Uitgaande van principes van continuïteitsmanagement vormt crisismanagement één van de cruciale elementen in het beperken van continuïteitsverlies. Als de verstoring van de continuïteit daadwerkelijk plaatsvindt, wordt er vanuit continuïteitsmanagement nadrukkelijk teruggeslagen op de basisprincipes van crisismanagement. Het hebben en onderhouden van een crisismanagementorganisatie vormt zelfs één van de randvoorwaarden voor effectief continuïteitsmanagement. Als de ICT faalt of de stroom uitvalt, zal er door uw organisatie, onder urgente omstandigheden, slag-

vaardig en eenduidig moeten worden opgetreden. Onder omstandigheden van (acute) continuïteitsproblemen, zal uw organisatie kunnen teruggrijpen op crisismanagement.

Nu zult u wellicht denken: doen we met crisismanagement dan niet voldoende om onze continuïteitsvraagstukken te adresseren? Het antwoord hierop is negatief. Weliswaar zijn er gelijkenissen en – zoals hierboven geschetst – mogelijkheden voor synergie. De invalshoek van het bevorderen en zoveel mogelijk garanderen van continuïteit is echter dermate specifiek dat specifieke aandacht geboden is: om uitval te voorkomen, de voorbereiding hierop te verbeteren, de effecten te beperken en een zo spoedig mogelijk herstel mogelijk te maken. Juist vanwege dit specifieke karakter zal crisismanagement alleen niet afdoende zijn om de continuïteit van uw dienstverlening te garanderen.

### 3 Starten met continuïteitsmanagement: zes essentiële stappen

#### Inleiding

Uit de voorgaande hoofdstukken is duidelijk geworden wat de belangrijkste oorzaken en effecten zijn van uitval van ICT en elektriciteit. Ook is meer duidelijkheid verschaft over de aard en het nut van continuïteitsmanagement. Tegen deze achtergrond wordt in dit hoofdstuk een systematische aanpak gepresenteerd. Aan de hand hiervan kan uw organisatie continuïteitsmanagement vormgeven en inbedden. Overigens gaat de aanpak uit van het vormgeven van algemeen continuïteitsmanagement. Dit uitgaande van het idee dat algemeen continuïteitsmanagement de continuïteitsrisico's elektriciteits- en ICT-uitval omvat.

Het uitgangspunt van deze aanpak is dat organisaties die continuïteitsmanagement nog niet (systematisch) toepassen, dit met behulp van de verderop vermelde stappen kunnen realiseren. De aanpak is zodoende vooral relevant voor organisaties die starten, of overwegen te starten, met continuïteitsmanagement. Voor organisaties die continuïteitsmanagement reeds hebben ingebed, zal dit hoofdstuk vooral een controlefunctie vervullen.

De hier geschetste aanpak is gebaseerd op een aantal basisprincipes van continuïteitsmanagement. Het uitgangspunt is dat u wanneer u deze stappen doorloopt, u aan een aantal basisvoorwaarden voor succesvol continuïteitsmanagement hebt voldaan. Evident vergt de werkelijke inbedding, onderhoud, optimaal gebruik en verdere professionalisering van uw continuïteitsvoorzieningen een meer langdurige inspanning. Het bewustzijn van het belang van continuïteitsmanagement moet groeien, en concrete ervaringen hiermee moeten worden opgedaan – door te testen en trainen of door werkelijke (dreigende) verstoringen.

#### Hulpmiddel voor zelfanalyse & vervolgactie: Bent u voorbereid op uitval van ICT & elektriciteit? Waarborgen en aandachtspunten voor de continuïteit van uw organisatie

Wanneer u concreet met de voorbereiding op ICT- en elektriciteitsuitval aan de slag wilt gaan, gebruikt u dan het 'Hulpmiddel voor zelfanalyse en vervolgactie', waarin zowel algemene waarborgen en aandachtspunten voor de continuïteit van uw organisatie zijn opgenomen als specifieke voor ICT- en elektriciteitsuitval. Dit hulpmiddel stoelt op de principes van continuïteitsmanagement zoals deze in de hierna volgende stappen beschreven zijn – echter op het niveau van 'checks'. U kunt dit hulpmiddel gebruiken om de hier geschetste aanpak en inbedding van continuïteitsmanagement op praktisch niveau te begeleiden. Het hulpmiddel is samen met andere relevante ondersteuningsmaterialen te verkrijgen via: [www.nationale-veiligheid.nl](http://www.nationale-veiligheid.nl)

### Stap 1 Randvoorwaarden voor continuïteitsmanagement

Zonder opdrachtgever, geen opdracht. Zonder opdracht geen continuïteitsmanagement. Ervan uitgaande dat uw organisatie continuïteitsmanagement nog niet nader of structureel heeft ingebed, is het van groot belang dat aan de basis van het project of programma geen onduidelijkheid bestaat over wie de opdracht verstrekt en wat deze inhoudt. Vanuit zowel de eindverantwoordelijkheid als de betrokkenheid ('commitment') fungeert het topmanagement c.q. de bestuurlijke leiding idealiter als opdrachtgever. Tevens wordt uw opdracht op dat niveau geformuleerd en verstrekt. Op datzelfde niveau vindt bovendien besluitvorming plaats over het plan van aanpak (project- of programmaplan).

Daarbij moeten de noodzakelijke randvoorwaarden voor de opzet, uitvoering en inrichting van continuïteitsmanagement worden gecreëerd. In beginsel zal het hierbij vooral gaan om zaken als:

- Het benadrukken van het belang van continuïteitsmanagement en het actief uitdragen hiervan
- Het vrijmaken van de benodigde middelen (zoals personele capaciteit en financiële middelen)

### Stap 2 Organisatie-analyse: ken uw organisatie (...écht!)

Deze stap lijkt evident en simpel. Maar organisaties zijn in toenemende mate complexe omgevingen. Een organisatie vervult verschillende doelen en taken, doet dit veelal vanuit verschillende vestigingen (soms ook in het buitenland), met soms grote aantallen medewerkers, een hoge mate aan specialisatie en met een groeiend aantal afhankelijkheidsrelaties met keten- of netwerkpartners. Hoewel u en uw collega's de eigen organisatie beter zullen kennen dan wie ook, is de kans groot dat het zelfs voor u lastig zal zijn om het overzicht te hebben – laat staan overzicht op alle activiteiten die worden verricht om de kerndoelstellingen te behalen.

#### Wat moet doorgang blijven vinden?

Dat vormt de kern van deze stap: vaststellen welke 'kritieke processen' binnen de organisatie niet mogen uitvallen. Voorbeelden van kritieke processen in de publieke sector zijn 'bestuurlijke ondersteuning' of 'politieke verantwoording'. Vervolgens stelt u vast welke activiteiten uw organisatie – juist onder de meest hachelijke omstandigheden – moet continueren om deze kritieke processen te garanderen. Vanuit continuïteitsmanagement wordt hiervoor vaak een 'procesbenadering' gebruikt. 'Een proces' moet dan worden opgevat als het geheel aan activiteiten, eigenschappen en middelen (input) dat gezamenlijk wordt ingezet (transformatie) om een gewenst resultaat te behalen (output). Dit resultaat kan vanzelfsprekend verschillende vormen aannemen, variërend van een concreet product of dienst tot het geven van een impuls, stimuleren van een ontwikkeling, et cetera.

#### Redeneer 'terug'

Hoe stelt u nu vast welke activiteiten zo essentieel zijn dat deze koste wat het kost doorgang moeten blijven vinden? Eén van de manieren om dit te doen is terugredeneren. Stel de belangrijkste doelen, producten en diensten (output) van uw organisatie centraal en breng vervolgens, terugredenerend, in kaart welke activiteiten er worden verricht om het gewenste eindresultaat te realiseren.

U hoeft hiervoor vanzelfsprekend niet alles zelf uit te vinden. Uw organisatie biedt u hiervoor zonder enige twijfel tal van hulpmiddelen. Denk bijvoorbeeld aan de missie, doel, strategie en kerntaken van uw organisatie, bij wet belegde taken, (prestatie) contracten of de actuele product- en dienstenportfolio. Kom zo tot een overzicht van de belangrijkste doelen, producten of diensten van uw organisatie. En ga vervolgens systematisch na wat uw organisatie precies doet om deze te realiseren.

**Ken uw afhankelijkheden**

Uw organisatie functioneert niet op zichzelf maar maakt onderdeel van netwerken en ketens. Dit maakt dat uw bedrijfsvoering afhankelijk is van 'derden' en dat 'derden' op hun beurt afhankelijk zijn van uw organisatie – ook waar het de wederzijdse continuïteit betreft. Kijkend naar de centrale doelen, producten of diensten, laten deze afhankelijkheden zich in mindere of meerdere mate gelden. Sommige zaken zult u vrij autonoom vanuit de eigen organisatie kunnen realiseren, waar u voor andere in hoge mate afhankelijk bent van bijvoorbeeld een leverancier, administrateur of onderhoudsbedrijf.

Een belangrijke trend is zelfs de complete uitbesteding ('outsourcing') van bedrijfsactiviteiten. Noodzakelijke, logische en vaak kostenefficiënte oplossingen die op hun beurt nieuwe afhankelijkheden en daarmee mogelijk ook nieuwe kwetsbaarheden aan de dag leggen. Vanuit continuïteitsmanagement is er daarom veel aandacht voor de meest pregnante afhankelijkheidsrelaties. Dat wil zeggen, de relaties met derden die mede bepalen of uw organisatie haar doelen kan realiseren. Het is daarom essentieel dat u weet welke 'derden' cruciaal zijn voor uw continuïteit.

**Mobiliseer denkracht 'over afdelingen heen'**

Continuïteitsrisico's raken niet alleen de kern van uw organisatie maar slaan vaak ook over de volle breedte toe. Het dilemma waar – in dit geval uitval van elektriciteit of ICT – uw organisatie voor staat, is dat er onder tijdsdruk overzicht moet zijn (of komen). En dat er intensief en vrijwel altijd afdelingsoverstijgend moet worden samengewerkt, om erger te voorkomen. De aanpak van continuïteitsvraagstukken staat daarmee in zekere zin haaks op hoe uw organisatie dagelijks functioneert: vanuit verschillende gespecialiseerde eenheden die veelal los van elkaar (deel)taken vervullen.

Continuïteitsmanagement vereist daarentegen een integraal – afdelingsoverstijgend – perspectief. Dit moet u al direct in de analysefase mobiliseren. Bij voorkeur met een groep – voor de gehele organisatie – representatieve collega's en op basis van een heldere opdracht van uw management. Denk vooral aan vertegenwoordigers die bekend met en betrokken zijn bij de primaire (operationele) processen en vitale diensten van uw organisatie. Maar evengoed aan vertegenwoordigers namens ondersteunende afdelingen als personeelszaken, communicatie, financiën, facilitair en ICT. Stel vervolgens gezamenlijk vast:

- Wat voor uw organisatie de meest wezenlijke doelen, diensten of producten zijn
- Welke werkprocessen achter de afzonderlijke doelen, diensten of producten schuil gaan
- Uit welke essentiële activiteiten deze processen zijn opgebouwd en van welke eigendommen en middelen deze afhankelijk zijn
- In hoeverre uw essentiële activiteiten afhankelijk zijn van cruciale 'derden'

Zet bovendien ook de denkracht van uw collega's afkomstig van andere delen uit de organisatie in, ook wanneer u de volgende stappen zet.

**Betrek de beslisser**

Vervat het resultaat van deze afdelingsoverstijgende exercitie in een advies dat u ter besluitvorming aan uw opdrachtgever aanbiedt. Het verdient daarbij de voorkeur om de besluitvorming eveneens afdelingsoverstijgend te maken. Focus daarom op de hogere of hoogste managementlagen (idealiter tevens uw opdrachtgever) en verlang instemming alvorens u de volgende stap zet.

**Stap 3 Impactanalyse: weet wat u te wachten staat**

Nu u weet welke essentiële activiteiten uw organisatie wil continueren, staat u voor een tweede analysestap: de impactanalyse. Het centrale doel van deze analyse is het vaststellen van de gevolgen van een verstoring op uw essentiële activiteiten. Bij de vaststelling van de impact staan verschillende criteria centraal. Als handvat voor de impactanalyse is in bijlage 1 een toolkit opgenomen.

**Stel de acceptabele uitvals- en hersteltijd vast**

Eén van de belangrijkste criteria is de eerder besproken maximale uitvalstermijn. Afgezet tegen uw essentiële activiteiten moet aan de hand van dit criterium in ieder geval duidelijk worden of en hoe lang een activiteit mag uitvallen. Het betreft hier de periode waarna er onacceptabele schade zal ontstaan. Dit geldt overigens ook voor die activiteiten waarvoor u afhankelijk bent van 'derden'. In dat verband moet ook worden vastgesteld binnen welke termijn de (deel)activiteiten hervat moeten worden en wanneer herstel en normalisatie van de activiteiten uiterlijk moeten plaatsvinden (hersteldoelstellingen). Beredeneer deze termijnen zoveel mogelijk in afstemming met de 'proceseigenaren'.

**Bepaal de impact van uitval**

Vanzelfsprekend is de maximaal toelaatbare uitvalstermijn niet het enige criterium dat bepalend is voor de impact van uitval. Sterker nog, of en hoe lang een essentiële activiteit stil mag komen te liggen, zal in de praktijk juist afhankelijk zijn van andere impactcriteria. Hoewel deze op basis van kenmerken als activiteiten, strategie en omgeving per organisatie kunnen verschillen, kunt u hierbij denken aan 'impactgebieden' als:

- De impact van de uitval op uw personeel
- De impact van de uitval op de samenleving
- De impact van de uitval op uw bedrijfsvoering- en eigendommen
- De impact van de uitval op uw belanghebbenden
- De impact van de uitval op uw resultaten
- De impact van de uitval op uw reputatie
- De impact van de uitval op het milieu
- De impact van de uitval op uw financiële positie
- Et cetera

In combinatie met de uitvals- en hersteltermijn, helpen deze criteria vaststellen wat de impact zal zijn als uw essentiële activiteiten stagneren of stilvallen.

- Bepaal samen met de representatieve groep collega's wat voor uw organisatie de meest belangrijke impactgebieden zijn (gebruik de bovenstaande opsomming ter inspiratie)
- Voorzie voor elke essentiële activiteit uw impactgebieden van een score. Bijvoorbeeld met behulp van het toekennen van simpele scores als 'geen impact' (score: 1), 'enige impact' (score: 2) en 'hoge impact' (score: 3)
- Relateer de scores aan het uitvalscriterium en breng vervolgens een prioritering aan waarbij de activiteiten met de hoogste impactscore en de kortste uitvalstermijn bovenaan de prioriteitenlijst komen te staan

**Let op**

Het gaat hier nog niet om concrete risico's of scenario's! Puur om het vaststellen wat de gevolgen zijn van uitval – ongeacht de oorzaken.

### Analyseer uw continuïteitsrisico's

Nu u weet welke activiteiten van uw organisatie in het licht van de uitvalstermijn en de impact het meest essentieel zijn, kunt u een risicoanalyse uitvoeren. Deze analyse is er op gericht om duidelijk te krijgen of en welke continuïteitsrisico's daadwerkelijk een bedreiging vormen voor uw organisatie. Verschillende verstoringen zullen immers verschillende gevolgen impliceren. Door de continuïteitsrisico's voor uw organisatie in te schatten, creëert u een extra wegingsfactor voor de essentiële activiteiten. Ter illustratie: als de uitval van een activiteit een hoge impact heeft en de activiteit niet mag stilvallen, kunt u uitgaande van de voor uw organisatie relevante continuïteitsrisico's, besluiten of en welke vervolgactie geboden is.

U kunt deze risicoanalyse in ieder geval uitvoeren voor de continuïteitsrisico's die hier centraal staan: uitval van elektriciteit en ICT. Maar evengoed voor andere -al dan niet moedwillig- veroorzaakte continuïteitsrisico's als:

- Brand
- Ontruiming
- Overstroming
- Diefstal
- Extreme weersomstandigheden
- Ziektegolf
- Stakingen/blokkades
- Uitval van drinkwatervoorziening
- Brandstoftekort
- Et cetera

#### Tip

Voor het analyseren van risico's bestaan verschillende methoden en technieken. Wij raden u aan om gebruik te maken van die methode(n) en technieken die binnen uw organisatie reeds toepassing vinden. Ook raden wij u aan om de risico-inschatting samen met een groep voor de organisatie representatieve collega's uit te voeren.

Nadat u de analyse hebt uitgevoerd en hebt vastgesteld welke continuïteitsrisico's het grootst zijn, is het verstandig om de bestaande continuïteitsmaatregelen in ogenschouw te nemen. Het ligt immers in de rede dat uw organisatie al maatregelen heeft getroffen om de belangrijkste kwetsbaarheden te reduceren. Uw 'bruto' risicobeeld (zonder maatregelen) zal dan naar verwachting ook afwijken van uw 'netto' risicobeeld (inclusief bestaande maatregelen).

- Schat de continuïteitsrisico's voor uw organisatie in
- Weeg de continuïteitsrisico's ook op basis van al getroffen continuïteitsmaatregelen
- Stel uw belangrijkste continuïteitsrisico's vast
- Spiegel de belangrijkste continuïteitsrisico's aan uw essentiële activiteiten
- Kom zo nodig op basis van uw risicoprofiel tot een herprioritering van uw meest essentiële activiteiten

### Stap 4 Formuleer de continuïteitsstrategie van uw organisatie

Nu u op basis van de voorgaande stappen weet welke essentiële activiteiten in welke prioriteitsvolgorde gecontinueerd moeten worden, is het van belang om een continuïteitsstrategie te formuleren. Met het formuleren van deze strategie markeert uw organisatie de overgang van 'denken' naar 'doen'. Het hoofddoel van de strategie is om te verduidelijken hoe uw organisatie de continuïteit van haar essentiële activiteiten zal waarborgen. Als handvat voor het formuleren van de continuïteitsstrategie is in bijlage 2 een model continuïteitsstrategie opgenomen.

In de eerste plaats maakt de strategie expliciet welke maatregelen er worden getroffen om verstoring van uw essentiële activiteiten te voorkomen danwel de effecten van deze te beperken. Het gaat daarbij enerzijds om reeds door uw organisatie getroffen preventieve of preparatieve maatregelen. Daarnaast betreft het vooral nog de door uw organisatie te treffen maatregelen. Ter illustratie: denk aan het wegnemen van zogeheten 'cruciale knelpunten' (single points of failure) in uw huidige ICT-infrastructuur om zo de kans op uitval te minimaliseren. Of bijvoorbeeld aan het opstellen van een uitwijkplan ten behoeve van het extern onderbrengen van uw ICT en/of kantooractiviteiten. Voor alle maatregelen geldt dat zij erop gericht moeten zijn om de uitvalsperiode zoveel mogelijk te bekorten.

#### Voorbeelden van preventieve maatregelen

- Het verbeteren van de ICT-beveiliging om het risico op ontwrichtende cybercrime te verkleinen
- Het sturen op aantoonbare continuïteitswaarborgen in de contractrelatie met 'cruciale derden'
- Het 'dubbel' (= redundant) uitvoeren van delen van uw ICT-infrastructuur
- Het compartimenteren van systemen
- Het kunnen beschikken over actuele en betrouwbare back ups
- Het nauwgezet (laten) monitoren en melden van ICT-incidenten
- Het hebben van meerdere aanbieders van vitale diensten

#### Voorbeelden van preparatieve maatregelen

- Het investeren in afdoende noodstroomvoorzieningen
- Het toegankelijk houden van de meest essentiële informatie
- Het opstellen van een afsluitprotocol
- Het opstellen van een continuïteitsplan
- Het opstellen van een herstelstrategie
- Het voorbereiden van een communicatieplan
- Testen en trainen van de plannen en de organisatie

In de tweede plaats maakt de strategie duidelijk wat uw organisatie doet om de continuïteit van essentiële activiteiten onder omstandigheden van daadwerkelijke uitval te beperken. Het betreft hier maatregelen van reactieve aard gericht op het snel beheersen van een eventueel incident. Als ook maatregelen gericht op een zo spoedig mogelijk herstel en normalisatie. Denk aan het zo snel mogelijk achterhalen van de oorzaak van ICT-uitval (diagnostiek) of aan het 'opschonen' van systemen. Ook voor deze maatregelen geldt dat zij ten doel hebben om de uitvalstermijn conform de gestelde norm te minimaliseren.

Voorbeelden van reactieve maatregelen
<ul style="list-style-type: none"> <li>• Het activeren van het continuïteitsplan</li> <li>• Het activeren van de crisismanagementorganisatie</li> <li>• Het verrichten van diagnostische inspanningen om de oorzaak te achterhalen</li> <li>• Het uitwijken naar een alternatieve locatie</li> <li>• Het acuut mobiliseren van de benodigde interne en externe expertise</li> <li>• Het communiceren naar groepen belanghebbenden</li> </ul>

Voorbeelden van herstelmaatregelen
<ul style="list-style-type: none"> <li>• Het vervangen van delen van de ICT-infrastructuur</li> <li>• Het terugplaatsen van de meest actuele back up</li> <li>• Het terugschakelen naar de reguliere elektriciteitsvoorziening</li> <li>• Het schonen van systemen</li> <li>• Het gefaseerd opstarten van systemen</li> </ul>

Uw strategie bevat de volgende elementen:

- De geprioriteerde essentiële activiteiten (inclusief de maximale uitvalstermijn)
- Een beschrijving van de maatregelen die per essentiële activiteit zijn of (kunnen) worden getroffen. Het gaat daarbij om preventieve-, preparatieve-, reactieve- en herstelmaatregelen – allen gericht op voorkomen van uitval of het reduceren van de gestelde uitvalstermijn
- De afwegingen ten grondslag aan de voorgestelde maatregelen per essentiële activiteit

De continuïteitsstrategie moet worden vastgesteld door het topmanagement danwel bestuur.

## Stap 5 Ontwikkel het continuïteitsplan voor uw organisatie

Het beschrijft hoe uw organisatie zal reageren op een daadwerkelijke verstoring. Het belangrijkste doel van dit plan is dan ook om de effecten van een verstoring zoveel mogelijk te reduceren. Uitgaande van de kwaliteitsstandaarden voor continuïteitsmanagement is dit plan opgebouwd uit een aantal onderdelen. Als handvat voor het opstellen van een continuïteitsplan is in bijlage 3 een model continuïteitsplan opgenomen.

Cruciaal is dat uw organisatie is ingericht om snel en adequaat op een verstoring te reageren. Mocht uw organisatie reeds beschikken over een structuur voor incident- of crisismanagement, dan ligt het voor de hand om deze eveneens voor uw continuïteitsmanagement te benutten. Uitgangspunt daarbij is dat deze 'nood-organisatie' over een toereikend mandaat beschikt. Het primaire doel van de crisismanagementorganisatie is om de verstoring zo snel mogelijk te beëindigen en eventuele neveneffecten te beperken. Daarnaast is de organisatie verantwoordelijk voor onder andere communicatie naar groepen belanghebbenden. Eén onderdeel van het responsplan is zodoende het crisismanagementplan. Hierin staat onder meer beschreven hoe de crisismanagementorganisatie is opgebouwd, hoe het crisisteam is samengesteld, welke criteria er worden gehanteerd voor activering van de crisisorganisatie, de (uitwijk)locatie van het crisisteam, welke taken er door de crisisorganisatie worden uitgevoerd, et cetera.

Naast het bestrijden van de 'bron' en de effecten van de verstoring, moet duidelijk zijn hoe uw organisatie de continuïteit van haar essentiële activiteiten – in afwachting van het herstel – zal garanderen. Dit vergt dat u – wederom op basis van de geprioriteerde essentiële activiteiten – duidelijk maakt welke actie uw organisatie hiertoe onderneemt. Echter niet zoals reeds in de strategie beschreven is, maar op een veel concreter niveau, rekening houdend met alles wat er (operationeel) nodig is om de continuïteit van de essentiële activiteiten te bevorderen.

Verder maakt een herstelplan eveneens onderdeel uit van het overkoepelende continuïteitsplan. In dit plan beschrijft u wat er gedaan kan worden om een snel herstel en normalisatie van essentiële activiteiten te bevorderen. Voor dit onderdeel van het plan geldt eveneens dat er op detailniveau beschreven staat welke inspanningen er worden geleverd om terug te keren naar de normale situatie.

Uw continuïteitsplan bevat onder meer:

- Een crisismanagementparagraaf gericht op de bestrijding van de bron en de directe effecten van het incident
- Een specifieke continuïteitsparagraaf waarin beschreven staat hoe uw organisatie haar essentiële activiteiten wil continueren
- Een paragraaf ten behoeve van een zo spoedig mogelijke terugkeer naar de normale situatie
- Mogelijke deelplannen, procedures et cetera

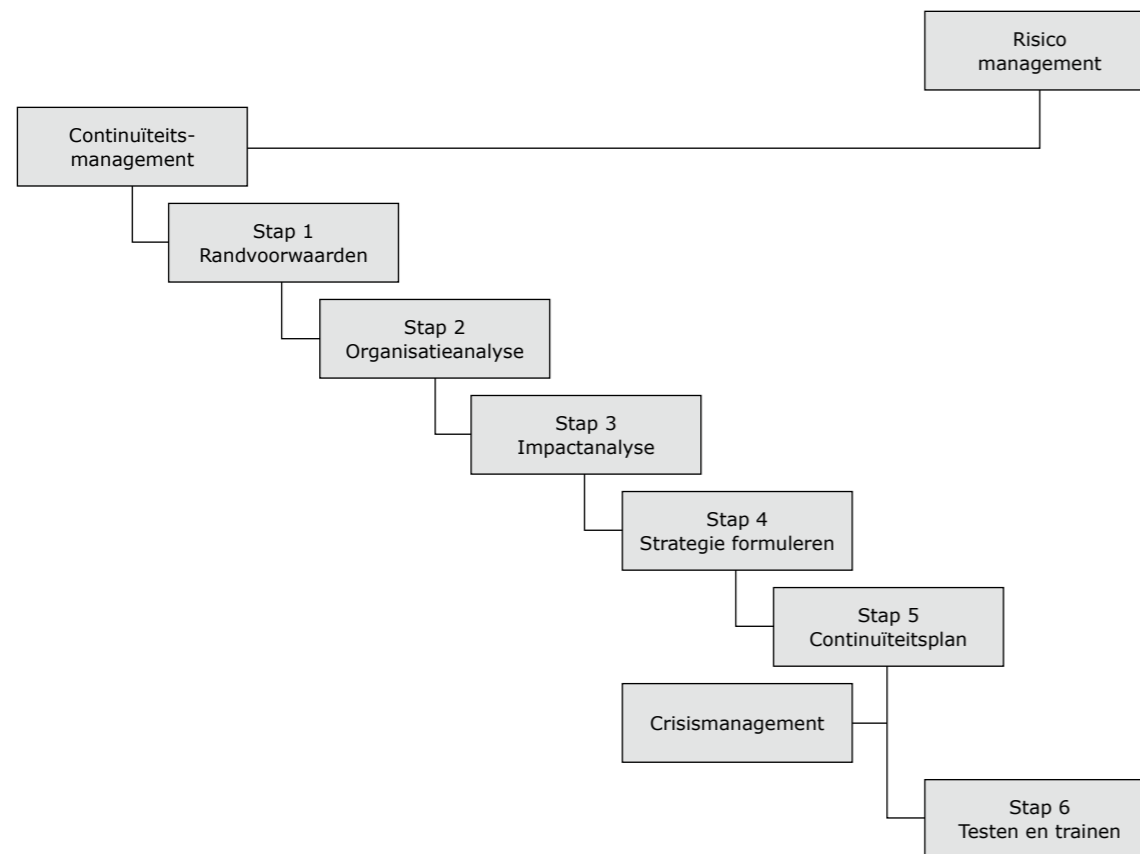
Het continuïteitsplan wordt opgesteld in samenwerking met een representatieve groep goed ingevoerde collega's. Ook het continuïteitsplan wordt expliciet vastgesteld door het bestuur c.q. topmanagement.



### Stap 6 Test uw continuïteitsvoorzieningen, train uw organisatie

Als sluitstuk voor de ontwikkeling van uw continuïteitsmanagement geldt het in de praktijk toepassen en toetsen van uw voorzieningen als ook het trainen van uw personeel. Deze activiteiten kunnen verschillende vormen aannemen. Variërend van het letterlijk testen van continuïteitsvoorzieningen zoals het oefenen van een uitwijksituatie. Of bijvoorbeeld het periodiek laten auditeren van uw continuïteitsmanagement. Tot het bevorderen van het bewustzijn van medewerkers of het trainen van personeel met een specifieke functie binnen het continuïteitsmanagement.

In onderstaand figuur is afgebeeld hoe risicomanagement, continuïteitsmanagement en crisismanagement zich tot elkaar verhouden.



In onderstaande tabel is overzichtelijk gepresenteerd welke instrumenten u kunt gebruiken ter ondersteuning van het doorlopen van de zes stappen, om een solide basis voor uw continuïteitsmanagement te leggen. Een aantal van deze instrumenten is opgenomen in de bijlagen van deze handleiding.

Stap in continuïteitsmanagement	Ondersteunend instrument
Stap 1 Randvoorwaarden	Project- of programmaplan
Stap 2 Organisatieanalyse	De missie, doel, strategie en kerntaken van uw organisatie, bij wet belegde taken, (prestatie)contracten of de actuele product- en dienstenportfolio
Stap 3 Impactanalyse	Impactanalyse Toolkit (bijlage 1)
Stap 4 Continuïteitsstrategie	Model continuïteitsstrategie (bijlage 2)
Stap 5 Continuïteitsplan	Model continuïteitsplan (bijlage 3)
Stap 6 Testen en trainen	Onder andere inbedden in het oefenbeleid, de planning- & controlcyclus, periodieke audits et cetera

## Bijlage 1 Impactanalyse Toolkit: stel zelf de impact van uitval voor uw organisatie vast

### Toelichting

Nadat u bepaald heeft welke essentiële activiteiten gecontinueerd moeten worden in uw organisatie (stap 2 continuïteitsmanagement), kunt u een impactanalyse uitvoeren. Deze bijlage helpt u daarbij. Door middel van het doorlopen van de vier vermelde stappen, komt u te weten wat de impact van uitval voor uw organisatie is. Verder komt u ook tot een betrouwbaar beeld van uw essentiële activiteiten (in prioriteitsvolgorde). Hieronder worden de volgende vier stappen nader toegelicht en waar mogelijk van hulpmiddelen voorzien.

1. Het identificeren van uw impactgebieden
2. Het vaststellen van de belangrijkste impactcriteria
3. Het prioriteren van uw essentiële activiteiten
4. Het duiden van onderlinge afhankelijkheden

### 1 Identificeer uw impactgebieden

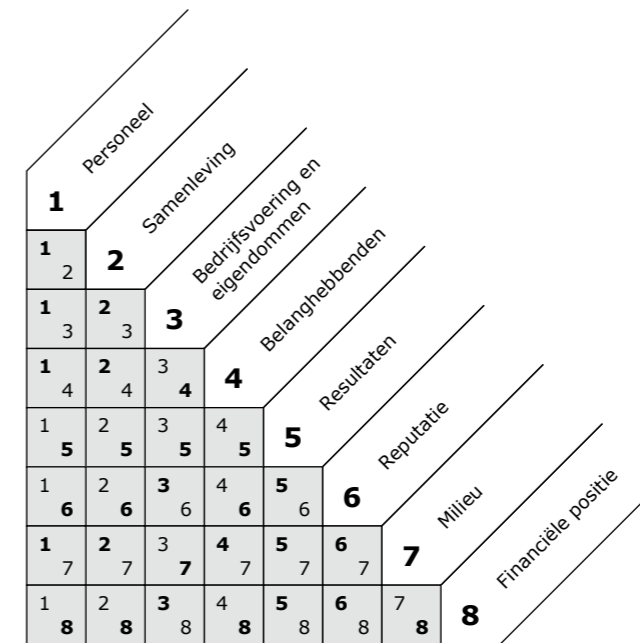
Maak om te beginnen duidelijk welke 'impactgebieden' gevolgen ondervinden van de verstoring van de continuïteit van uw organisatie. Wat heeft nu precies te lijden onder uw verstoring? Betrek hierin onder andere de taken, verantwoordelijkheden en maatschappelijke positie van uw organisatie. Denk bijvoorbeeld aan impactgebieden als:

- Uw personeel
- De samenleving
- Uw bedrijfsvoering- en eigendommen
- Uw belanghebbenden (waaronder uw klanten)
- Uw resultaten
- Uw reputatie
- Het milieu
- Uw financiële positie
- Et cetera

Deze lijst is vanzelfsprekend niet uitputtend. Gebruik deze opsomming als vertrekpunt voor de identificatie van de impactgebieden die specifieke relevantie hebben voor uw organisatie. Tracht hierbij zo concreet mogelijk te worden.

### 2 Weeg uw impactgebieden, kom tot de voor u relevante impactcriteria

De impactcriteria worden afgeleid van de impactgebieden, op basis van een gewogen onderlinge vergelijking. Wij hebben hiertoe onderstaand schema toegevoegd. Omcirkel in dit schema telkens het impactgebied dat voor uw organisatie het meest van belang is. Tel voor elk impactgebied het aantal keren dat het bijbehorende nummer is omcirkeld en plaats deze in de onderstaande tabel. Rangschik de impactgebieden op basis van het aantal keren omcirkeld. Het meest omcirkelde impactgebied krijgt de rangorde 1, de tweede krijgt de rangorde 2, enz. Bij gelijk aantal keren omcirkeld krijgen de impactgebieden dezelfde rangorde. Bepaal de wegingsfactor door de volgende formule uit te voeren:  $\text{wegingsfactor} = 1 / \text{rangorde}$ . Gebruik deze wegingsfactoren voor elk impactgebied in bovenstaande tabel. De hoogst scorende 'gebieden' vormen uw belangrijkste impactcriteria. Ter verduidelijking hebben we een rekenvoorbeeld toegevoegd.



1	2	3	4	5	6	7	8	Nummer impactcriterium
4	3	2	2	7	5	1	4	Hoeveel keer omcirkeld?
3	4	5	5	1	2	6	3	Uiteindelijke rangorde (R)
1/3	1/4	1/5	1/5	1	1/2	1/6	1/3	Wegingsfactor (1/R)

### 3 Bepaal de impactscore én breng prioriteit in uw meest essentiële activiteiten

De tabel op pagina 34 is een hulpmiddel voor het uitvoeren van de impactanalyse. Voor elke activiteit worden benoemd: wie de eigenaar is (afdeling, persoon), hoe lang een activiteit maximaal mag uitvallen en hoe snel de activiteit minimaal hersteld moet zijn. Verschillende impactcriteria worden gescoord (1: geen impact, 2: enige impact, 3: hoge impact) en vermenigvuldigd met de wegingsfactor. Ga bij het scoren van de impactcriteria uit van de worst case situatie. De wegingsfactor wordt bepaald door alle impactcriteria met elkaar te vergelijken. Hiervoor gebruikt u het schema onder stap 2. De som van de gewogen impact voor alle criteria vormt de impactscore voor de activiteit. De combinatie van de impactscore en het uitvalscriterium bepaalt de prioriteit. Een hogere impactscore betekent een hogere prioriteit. Lagere maximale uitvalstermijn en lagere minimale hersteltijd resulteren in een hogere prioriteit. Ga hierbij uit van een worst case situatie: de langst denkbare uitvalstermijn of hersteltijd. Geef elke activiteit een prioriteitscijfer in de eerste kolom en rangschik de activiteiten naar prioriteit. Bepaal zelf per activiteit wat zwaarder weegt: het uitvalscriterium of de impactscore. Gebruik voor de activiteit met de hoogste prioriteit het cijfer 1, en daarna olopend.



## Bijlage 2 Model continuïteitsstrategie

### Continuïteitsstrategie <periode> <organisatie>

Dit format is bedoeld als voorbeeld: om u een indruk te geven van de wijze waarop een continuïteitsstrategie bepaald kan worden. De invulling van dit format vereist dat u en anderen binnen uw organisatie een aantal noodzakelijke denkstappen zet. Het algemene format moet op basis van specifieke keuzes, kenmerken en behoeften worden ingevuld en aangepast (organisatiespecifiek).

Status: Concept / definitief, versie  
 Auteur:  
 Directie / Afdeling:  
 Datum:  
 Bestandsnaam:

## 1 Inleiding

In deze continuïteitsstrategie geeft **<Organisatie>** invulling aan haar ambities voor continuïteitsmanagement. De continuïteitsstrategie markeert de overgang van 'denken' naar 'doen'. Het hoofddoel van de strategie is te verduidelijken hoe de organisatie de continuïteit van haar essentiële activiteiten zal waarborgen. De strategie bevat een set van (sub)doelstellingen, in de vorm van continuïteitsmaatregelen, die gelden voor de gehele organisatie. Deze doelstellingen gelden zeker niet alleen in het geval van een verstoring. De doelstellingen zijn juist ook van toepassing ter voorkoming van, en ter voorbereiding op, verstoringen.

De doelstellingen in dit plan zijn vastgesteld op **<datum>** door **<Organisatie>** en zijn bereikt op **<datum>**. Het opstellen van de continuïteitsstrategie en het geven van leiding aan het proces continuïteitsmanagement is de verantwoordelijkheid van: **<Functie, Afdeling, Organisatie>**.

## 2 Missie

**<Organisatie>** wil zijn bedrijfsvoering en maatschappelijke verantwoordelijkheden continueren bij uitval en daarmee de gevolgen voor medewerkers, maatschappij, klanten, diensten, producten et cetera zoveel mogelijk beperken of wegnemen. De organisatie treft continuïteitsmaatregelen op basis van een gedegen organisatie- en impactanalyse, als ook een gedegen analyse van risico's. De analyses en daaruit voortvloeiende maatregelen rekenen op de expliciete steun van het (hoger) management of bestuur.

## 3 Activiteiten

### 3.1 Prioritering van activiteiten

De organisatie brengt alle kernactiviteiten in beeld en maakt een keuze voor welke activiteiten met de hoogste prioriteit maatregelen getroffen moeten worden. De prioriteit kan worden bepaald met behulp van de impactanalyse toolkit (bijlage 1 van de handleiding continuïteitsmanagement). De kernactiviteiten van de organisatie zijn gerangschikt naar prioriteit, waarbij slechts de activiteiten met de hoogste prioriteit in het overzicht zijn opgenomen.

Bij elke activiteit is beschreven wie de eigenaar is van de activiteit en wat het uitvalscriterium is (maximale uitvalstermijn, minimale hersteltijd). Per activiteit is aangegeven wat de gebieden zijn waarop enige of grote impact verwacht wordt (personeel, samenleving, bedrijfsvoering- en eigendommen, belanghebbenden, resultaten, reputatie, milieu, financiële positie, et cetera). Daarbij wordt tevens een inschatting gemaakt van de consequenties voor de organisatie wanneer er geen maatregelen getroffen zouden worden.

Prioriteit	Activiteit	Proces Eigenaar	Uitvalscriterium	Impactgebieden	Consequenties
(nummer)	(aanduiding kernactiviteit)	(functionaris)	(uitvalstermijn en hersteltijd)	(opsomming)	(opsomming)
1					
..					

De organisatie weet welke afhankelijkheden er van derden bestaan en treft daar waar nodig continuïteitsmaatregelen.

Activiteit	Afhankelijke activiteit	Consequenties	Termijn
(aanduiding kernactiviteit)	(aanduiding kernactiviteiten)	(opsomming)	(uren:min)

### 3.2 Continuïteitsmaatregelen per activiteit

De organisatie maakt een bewuste afweging voor welke kernactiviteiten maatregelen worden getroffen. Hierbij wordt uitgegaan van de prioriteit van de activiteit en de consequenties wanneer maatregelen uitblijven.

Voor elke activiteit zijn één of meerdere maatregelen benoemd. Het verwachte effect van die maatregelen is daarbij beschreven. De organisatie geeft aan welke afwegingen gemaakt zijn. Een indicatie van de kosten geeft inzicht in de kosten van continuïteitsmaatregelen en zal behulpzaam blijken bij het maken van afwegingen. Per activiteit is aangegeven of reeds in deze maatregel is voorzien, of dat deze op de planning staat om uitgevoerd te worden. De activiteiten zijn onderverdeeld in:

- Preventieve maatregelen, het verkleinen – of wegnemen - van kans en effect van oorzaken en gevolgen van incidenten
- Preparatieve maatregelen, in voorbereiding op een verstoring, om een effectieve reactie mogelijk te maken en de schade zoveel mogelijk te beperken
- Reactieve maatregelen, voor het zo snel mogelijk beheersen en beëindigen van een verstoring
- Herstelmaatregelen, voor een zo spoedig mogelijk herstel en normalisatie na een verstoring

Activiteit	Maatregel(en)	Effect	Afwegingen	Kosten	Status
(aanduiding kernactiviteit)	(opsomming)	(opsomming)	(tekstuele duiding)	(in €)	(□ of ☒)
<b>Preventieve maatregelen</b>					
<b>Preparatieve maatregelen</b>					
<b>Reactieve maatregelen</b>					
<b>Herstelmaatregelen</b>					

### 3.3 Geaccepteerde risico's

De organisatie maakt een bewuste afweging voor welke activiteiten maatregelen worden getroffen en accepteert het risico dat hiermee gepaard gaat. Deze afwegingen zijn gemaakt voor:

- Activiteiten die uitvallen langer dan de maximale uitvalstijd
- Activiteiten die volledig stopgezet worden
- Activiteiten waarvoor deels maatregelen getroffen worden, maar restrisico's blijven bestaan
- Activiteiten die niet als essentieel zijn aangemerkt door de organisatie

Activiteit	Geaccepteerde risico's	Afwegingen
(aanduiding kernactiviteit)	(opsomming)	(tekstuele duiding)

## Bijlage 3 Model continuïteitsplan

### Continuïteitsplan <organisatie>

Dit format is bedoeld als voorbeeld: om u een indruk te geven van hoe een continuïteitsplan kan worden vormgegeven. De invulling van dit format vereist dat u en anderen binnen uw organisatie een aantal noodzakelijke denkstappen zet. Het algemene format moet op basis van specifieke keuzes, kenmerken en behoeften worden ingevuld en aangepast (organisatie-specifiek).

Status: Concept / definitief, versie  
 Auteur:  
 Directie / Afdeling:  
 Datum:  
 Bestandsnaam:

## 1 Inleiding

Het continuïteitsplan stelt de organisatie in staat om kernactiviteiten te continueren of te herstellen. Het plan beschrijft hoe uw organisatie zal reageren op een daadwerkelijke verstoring. Het continuïteitsplan van de organisatie bestaat uit drie deelplannen:

- Deelplan 1 crisismanagement: het activeren en opstarten van de crisis/continuïteitsorganisatie;
- Deelplan 2 continuïteitsmanagement: het continueren van kernactiviteiten van de organisatie;
- Deelplan 3 herstel: het terugkeren naar de reguliere bedrijfsvoering

Het plan beschrijft allereerst de doelgroepen, doelstellingen, de afspraken met betrekking tot het beheren van dit plan en de relatie met andere plannen. Aansluitend volgen de drie deelplannen.

### 1.1 Doelgroepen

De betrokken doelgroepen zijn:

- 
- 

Alle leden van de doelgroepen zijn te vinden in bijlage A.

### 1.2 Doelstelling

Het belangrijkste doel van dit plan is de effecten van een verstoring zoveel mogelijk te reduceren, de kernactiviteiten van uw organisatie te continueren en het herstel te bespoedigen. De doelstelling en strekking van het continuïteitsplan zijn gedefinieerd en geaccepteerd door het management van <organisatie>. Het continuïteitsplan is verspreid onder – en bekend bij – de doelgroepen.

### 1.3 Documentbeheer

De organisatie heeft <functionaris, team> aangewezen als eigenaar van het continuïteitsplan. Het plan wordt <periode> herzien en geactualiseerd door <functionaris, team>.

Datum	Versie	Wijziging(en)	Auteur
(dag, maand, jaar)	(nummer)	(opsomming)	(functionaris, naam)

De doelgroepen worden op de hoogte gesteld van vastgestelde wijzigingen aan het continuïteitsplan. Hiervoor maakt de auteur gebruik van de contactgegevens in bijlage A.

### 1.4 Relatie met andere plannen en structuren

De relatie met andere relevante plannen en documenten binnen de organisatie, of van belangrijke externe partners, is benoemd. De relatie tot een incident- of crisisorganisatie is benoemd.

## 2 Deelplan 1: crisismanagement

Dit deelplan is gericht op het zo snel en effectief mogelijk beperken van de effecten en het wegnemen van de bron van de verstoring. Maakt u hiervoor – mits hierin door uw organisatie voorzien – gebruik van de bestaande crisismanagementvoorzieningen. De procedure voor het in werking stellen van het continuïteitsplan is beschreven en de taken en verantwoordelijkheden van functionarissen, teams en organisatieonderdelen zijn benoemd. De activiteiten die tijdens een verstoring doorgang vinden zijn genoemd, evenals activiteiten die gestaakt zullen worden en de consequenties daarvan. De procedure voor het informeren en mobiliseren van doelgroepen en derden is beschreven, zodat na uitval van ICT of elektriciteit tijdig wordt gehandeld. De benodigde middelen zijn beschreven. De contactgegevens van alle doelgroepen, interne en externe diensten en derden zijn opgenomen in het plan.

### 2.1 Crisisorganisatie

De organisatie beschikt over een structuur voor incident- of crisismanagement. De crisisorganisatie beschikt tevens over toereikend mandaat om het continuïteitsplan in werking te stellen en maatregelen uit te voeren. De crisisorganisatie opereert onder de directe verantwoordelijkheid van het bestuur c.q. hoger management. De crisisorganisatie is een afspiegeling van de organisatie. De crisisorganisatie is in staat om de samenstelling op basis van de kenmerken van de verstoring aan te passen en de benodigde expertise te mobiliseren.

<voeg hier het organogram van uw crisis-/ of continuïteitsorganisatie in>

### 2.2 Activering

Alarmering en opschaling van de crisisorganisatie vinden plaats volgens de vaste structuur én criteria die uw organisatie hanteert. In het geval van een serieus te nemen (dreigende) verstoring, wordt het continuïteitsplan geactiveerd, met als doel om de kernactiviteiten te ondersteunen die nodig zijn om de doelstellingen van de organisatie te behalen.

Het plan kan als geheel, of in delen, in werking gesteld worden bij een continuïteitsverstoring. Voor elk (deel)plan is vastgelegd welke functionaris het plan in werking kan stellen en onder welke omstandigheden, voorwaarden en in overleg met wie, het plan geactiveerd kan worden. De handelingen en lijnen om het plan in werking te stellen en de teams te mobiliseren zijn beschreven.

(Deel)plan	Geautoriseerde functionaris	Voorwaarden in werking stelling	Handelingen
(document, nummer)	(functionaris)	(opsomming)	(stappenplan)

Afspraken over tijdstippen en locaties voor briefings en teambijeenkomsten zijn vooraf vastgelegd.

Team	Locatie	Uitwijklocatie	Tijdstippen en frequentie
(naam team)	(gebouw, ruimte)	(gebouw, ruimte)	(vergaderklok, uren:min)

De inwerkingstelling van het continuïteitsplan wordt gecommuniceerd aan alle doelgroepen. Hiervoor maakt de geautoriseerde functionaris gebruik van de contactgegevens in bijlage A.

### 2.3 Taken en verantwoordelijkheden

De taken en verantwoordelijkheden van de mensen en teams die een rol spelen bij de besluitvorming, het verdelen van taken, of het bijstaan in de uitvoering van het continuïteitsplan, zijn vastgelegd.

<Functionaris/team>

### 2.4 Informeren

De volgende activiteiten hebben een directe impact op de continuïteit van klanten of doelgroepen, of hebben impact op de samenleving. Onderdeel van crisismanagement is het informeren van deze doelgroepen. De termijn waarbinnen de organisatie na uitval deze doelgroepen informeert is bepaald.

Activiteit	Doelgroep	Procedure voor informeren	Termijn
(aanduiding kernactiviteit)	(organisatie, functionaris)	(stappenplan)	(uren:min)

## 3 Deelplan 2: continuïteitsmanagement

### 3.1 Continuïteit activiteiten

In de continuïteitsstrategie <periode> voor continuïteitsmanagement in geval van een verstoring is vastgesteld welke maatregelen er zijn getroffen voor de continuïteit van activiteiten van de organisatie. Bij goed functioneren van deze maatregelen verwacht de organisatie dat de volgende activiteiten ook onder omstandigheden van uitval beschikbaar zijn. Hierbij is aangegeven op welke termijn na de uitval de activiteit beschikbaar moet zijn en welke aanvullende handelingen daarvoor nog eventueel verricht dienen te worden. Verwijzingen naar gedetailleerde procedures of plannen zijn opgenomen. De proceseigenaar is verantwoordelijk voor het continueren van deze activiteit.



Activiteit	Termijn beschikbaarheid	Proces eigenaar	Handelingen	Verwijzing gedetailleerde procedures of plannen
(aanduiding kernactiviteit)	(uren:min)	(functionaris)	(opsomming)	(document, nummer)

Tevens is bekend welke activiteiten niet beschikbaar zullen zijn onder omstandigheden van verstoring. De consequenties van de uitval van deze activiteiten, zoals geformuleerd in de continuïteitsstrategie <periode> zijn benoemd.

Activiteit	Proces eigenaar	Consequenties
(aanduiding kernactiviteit)	(functionaris)	(opsomming)

### 3.2 Mobiliseren derden

De volgende activiteiten zijn afhankelijk van de dienstverlening van derden. Voor de volgende activiteiten zijn reeds afspraken gemaakt met derden. Voor elke activiteit waar relaties zijn met diensten van derden is dit benoemd en worden getroffen maatregelen en de afgesproken maximale uitvalstermijn beschreven.

Activiteit	Derde	Getroffen maatregelen	Termijn
(aanduiding kernactiviteit)	(organisatie, functionaris)	(opsomming)	(uren:min)

Voor andere activiteiten zijn dergelijke afspraken met derden nog niet gemaakt. Hiervoor legt de organisatie vast wat de procedure is voor het mobiliseren van middelen en inzet van derden ten tijde van een verstoring van de continuïteit. De termijn waarbinnen de organisatie dienstverleners na uitval mobiliseert is een gegeven.

Activiteit	Derde	Procedure voor mobiliseren	Termijn
(aanduiding kernactiviteit)	(organisatie, functionaris)	(stappenplan)	(uren:min)

### 3.3 Middelen

De benodigde middelen voor het continueren van de kernactiviteiten kunnen op voorhand in kaart worden gebracht. De organisatie draagt er zorg voor dat deze middelen tijdig beschikbaar zijn. De tijdsspanne na uitval is opgedeeld in meerdere perioden. Voor elke periode is per middel aangegeven welke hoeveelheid noodzakelijk is.

Activiteit	Middelen	<Periode>	<Periode>	<Periode>	<Herstel Periode>
(aanduiding kernactiviteit)	(opsomming)	(aantal)	(aantal)	(aantal)	(aantal)
<b>Mensen (beveiliging, transport, logistiek, welzijn, noodvoorzieningen)</b>					
<b>Locaties, gebouwen</b>					
<b>Noodstroomvoorzieningen</b>					
<b>Technologie, ICT en communicatiemiddelen</b>					
<b>Informatie (financiële gegevens, klantgegevens, leverancier en stakeholder gegevens, contracten, verzekeringspapieren, service level agreements)</b>					
<b>Voorraden</b>					
<b>Management van – en communicatie met – stakeholders</b>					

**4 Deelplan 3: herstel**  
 Nadat de oorzaak van de uitval verholpen is, dient de organisatie nog stappen te nemen om te komen tot volledig herstel en normalisatie van de organisatie. In de herstelfase, onderdeel van de nafase, schaal de crisisorganisatie – zodra mogelijk – af en worden activiteiten overgedragen aan de reguliere organisatie (of zo nodig aan een specifiek voor het herstel ingerichte projectorganisatie). Verder besteedt de organisatie aandacht aan het op gang brengen van activiteiten die stil kwamen te liggen. De situatie wordt geëvalueerd en leerpunten worden doorgevoerd in bestaande plannen en procedures.

**4.1 Afschalen crisisorganisatie**  
 De organisatie schaal de crisisorganisatie af volgens de vaste structuur voor op- en afschaling die gehanteerd wordt voor calamiteiten. Aanvullende afspraken, voor het afschalen van de crisisorganisatie of het verlaten van een uitwijklocatie, na uitval van ICT of elektriciteit worden hier benoemd.

**4.2 Herstel en normalisatie van activiteiten**  
 Activiteiten die tijdens uitval om welke reden dan ook zijn stil komen te liggen, dienen opnieuw te worden opgestart. De verwachte termijn voor beschikbaarheid is benoemd en de handelingen die daarvoor nodig zijn worden weergegeven. De eigenaar van deze activiteit is verantwoordelijk voor het halen van de gestelde hersteltermijn.

Activiteit	Termijn beschikbaarheid	Proces eigenaar	Handelingen
(aanduiding kernactiviteit)	(uren:min)	(functionaris)	(opsomming)

De middelen die noodzakelijk zijn voor het herstellen van alle activiteiten zijn benoemd in de tabel in paragraaf 3.3, in de kolom **<herstel periode>**. De organisatie draagt zorg dat deze middelen beschikbaar zijn alvorens de herstelperiode in gaat.

## Bijlage A. Contactgegevens

De contactgegevens van alle interne en externe diensten, organisaties en dienstverleners die van belang zijn voor de continuïteit van de organisatie zijn vastgelegd.

### Interne organisatie

Functionaris	Team	Locatie	Email	Telefoon (vast, mobiel)	Alternatieve bereikbaarheid

### Dienstverleners en externe partners

Dienstverlener	Locatie	Email	Telefoon (vast, mobiel)	Alternatieve bereikbaarheid

### Klanten en doelgroepen

Klant/doelgroep	Locatie	Email	Telefoon (vast, mobiel)	Alternatieve bereikbaarheid

## Bijlage B. Registratieformulier

Alle genomen besluiten, vitale informatie en incidenten worden geregistreerd door middel van een vast format. Deze informatie dient in de nafase voor het evalueren van de crisisbeheersing en het aanmerken van verbeterpunten voor het continuïteitsplan en de continuïteitsstrategie.

Activiteit	Functionaris	Datum, tijdstip	Logboek
(aanduiding kernactiviteit)	(naam)	(datum)	(melding, registratie incident, besluiten)



Deze handleiding is een uitgave van:

Ministerie van Veiligheid en Justitie  
Directoraat-Generaal Veiligheid

[www.nationale-veiligheid.nl](http://www.nationale-veiligheid.nl)

Schedeldoekshaven 200  
Postbus 20011 | 2500 EA Den Haag