Berenschot

“Alles mag omvallen behalve dát” Werken aan Continuïteit

tips en trucs voor gemeenten
over continuïteitsmanagement
bij uitval van ICT en/of elektriciteit

Margreeth van Dorssen
Frederik van Dalfsen

November 2014

55888

Berenschot

Inhoud Pagina

Berenschot

Voorwoord

Continuïteitsmanagement bij uitval van ICT of elektriciteit is vaak een ondergeschoven kindje: het onderwerp waar men 'ook nog wat mee moet'. En dat terwijl gemeenten meer en meer afhankelijk zijn van informatie, software en communicatiemiddelen – en dus in hoge mate kwetsbaar voor uitval van ICT en/of elektriciteit. De continuïteit van dienstverlening van gemeenten kan bij uitval dan ook zwaar onder druk komen te staan.

Voor veel organisaties is de kwetsbaarheid voor uitval van ICT en/of elektriciteit buitengewoon vervelend. Voor gemeenten echter is die kwetsbaarheid op sommige vlakken eigenlijk onacceptabel omdat zij een cruciale rol hebben in de openbare orde en veiligheid en het openbaar bestuur. Vanwege de cruciale rol, de kwetsbaarheid en grote impact bij een verstoring werken veel gemeenten aan het ontwikkelen van volwassen continuïteitsmanagement bij uitval van ICT en/of elektriciteit. Deze publicatie kan daarbij als een handvat dienen.

Deze publicatie is in eerste plaats bedoeld voor adviseurs en management van gemeenten. Niettemin zullen adviseurs en managers van provincies en waterschappen zien dat de voorbeelden in deze publicatie weliswaar betrekking hebben op gemeenten, maar dat onze denkwijze rond continuïteitsmanagement ook toepasbaar is op hun eigen organisatie. Kortom, deze publicatie is voor:

- diegenen die aan de slag willen met continuïteit bij uitval van ICT en/of elektriciteit
- diegenen die hun collega's/ leidinggevende/bestuurders willen overtuigen dat actie écht noodzakelijk en haalbaar is
- én degenen die door de bomen het bos niet meer zien en zoeken naar houvast: wat betekent continuïteit bij uitval van ICT en/of elektriciteit voor mijn gemeente?

De inzichten die in deze publicatie zijn gebundeld, zijn tot stand gekomen mede dankzij onze ervaringen bij verschillende organisaties in de publieke sector, zoals veiligheidsregio Twente, veiligheidsregio Rotterdam Rijnmond, provincie Noord-Holland, provincie Zuid-Holland, gemeente Zaanstad, gemeente Den Haag, het hoogheemraadschap van Schieland en de Krimpenerwaard, het ministerie van BZK, het ministerie van Veiligheid en Justitie en TNO. We hebben gezamenlijk en met plezier aan de totstandkoming van de inzichten gewerkt die in deze publicatie gebundeld zijn.

Margreeth van Dorssen, Berenschot

Frederik van Dalfsen, Berenschot

Berenschot

Continuïteit(smanagement) bij gemeenten

1. Wat bedoelen we met continuïteit(smanagement)?

Wat ons betreft gaat continuïteit(s)management bij gemeenten over het continueren van de gemeentelijke dienstverlening onder moeilijke omstandigheden. We weten dat het niet realistisch is dat de gehele dienstverlening 'in business' blijft. We verwachten wel dat een gemeente met behulp van continuïteitsmanagement datgene overeind houdt wat écht belangrijk is – het 'stukje' dienstverlening dat niet mag uitvallen ('alles mag omvallen behalve dát').

Het begrip continuïteit kan op veel verschillende associaties en interpretaties rekenen. Het wordt in veel hoedanigheden gebruikt en niet altijd is duidelijk wat precies wordt bedoeld. Door de oogharen heen zien we twee verschijningsvormen: Enerzijds wordt het technisch-instrumenteel aangevlogen, gepaard met de termen *risk management control, business continuity* en operationele bedrijfsvoeringsprocessen. Niet zelden wordt daarbij gemakshalve de link met *cybersecurity* gelegd. Anderzijds zien we dat continuïteit(smanagement) wordt gebruikt als generiek toepasbaar *buzz-woord*: 'continuïteitsmanagement als oplossing voor al uw problemen', waarbij het gaat om 'bewustwording', 'samenwerking' en 'een strategische baseline' – ware woorden, maar dikwijls blijft het precieze probleem en de exacte oplossing boven de markt blijven hangen …

Vele associaties en interpretaties dus. Daarom beginnen we deze publicatie met een omschrijving van de scope. Het gaat wat ons betreft om de continuïteit van de gemeentelijke dienstverlening. Niet de gehele dienstverlening, maar *alleen* dat 'stukje' dienstverlening van de gemeente dat niet mag omvallen – *no matter what*. Het gaat om die taken die wettelijk zijn voorgeschreven of die een belangrijke maatschappelijke functie hebben. Bijvoorbeeld het bereikbaar zijn van de gemeente (via de publieksbalie of anderszins), de gemeentelijke crisisorganisatie, het uitbetalen van schuldhulpverlening en uitkeringen, enzovoorts. De continuïteit van deze dienstverlening kan om allerlei redenen onder druk komen te staan. In deze publicatie ligt de focus op het continueren van datgene dat afhankelijk is van ICT en/of elektriciteit – en dus bij uitval van ICT en/of elektriciteit onderuit zou kunnen gaan. En voor de volledigheid: het gaat dan om de continuïteit van de uitvoering van het proces, niet noodzakelijkerwijs om de continuïteit van de ICT-voorziening.

Meer verantwoordelijkheid leidt tot meer noodzaak voor continuïteit!

Sinds 2007 (VNG-commissie gemeentewet en grondwet, ook wel commissie Van Aartsen) worden gemeenten geduid als de eerste overheid. Het is de gemeente die het dichtst bij de burgers staat, en het is de gemeente die dienstverlening en publieke taken het beste uit kan voeren. Dit uitgangspunt leidt tot een systematische en verregaande decentralisatie van rijks- en provincietaken naar de gemeente.

Het groeiende takenpakket van gemeenten maakt de kwetsbaarheid van gemeenten groter (meer systemen, meer verbindingen, meer gebruikers), de rol van de gemeente in de maatschappij vitaler en daarmee de impact van een verstoring groter. Meer verantwoordelijkheid leidt tot meer noodzaak voor het op orde hebben van continuïteit.

2. Hoe vaak gaat het eigenlijk mis? Welke voorbeelden zijn er?

In juli 2012 werd een aanslag gepleegd op het gemeentehuis van de gemeente Waalre. Twee auto's ramden het gebouw, waarna dat vlam vatte en grotendeels afbrandde. De meeste processen van de gemeente lagen de dagen erna volledig plat. De fysieke locatie was 'onbewoonbaar', de werkplekken waren in as opgegaan, het digitale archief was (tijdelijk) ontoegankelijk, de gemeente was onbereikbaar voor burgers en het politieke systeem lag stil. Na een week kon de gemeente een tijdelijk burgerloket openen in de brandweerkazerne en kwam de dienstverlening weer mondjesmaat op gang[1].

Gelukkig is een aanslag van de omvang op het gemeentehuis van Waalre geen normale dreiging voor een gemeentehuis in Nederland. Tegelijkertijd toont het de kwetsbaarheid van de gemeentelijke organisatie aan. Want dat de kwetsbaarheid van de gemeente Waalre geen uitzondering is, blijkt wel uit andere situaties waarin dienstverlening van gemeenten en andere publieke organisaties in het gedrang kwam – in het bijzonder door uitval van ICT en/of elektriciteit: het Waalhaven incident (2012, uitval communicatiecentrum), stroomuitval in het centrum van Enschede (2013), de stroomuitval in de Bommelerwaard (2007, apache-helikopter vloog door hoogspanningskabel) en de helaas regelmatige lokale uitval van ICT en/of 112 laten allemaal het belang zien van ICT en/of elektriciteit voor het functioneren van vitale publieke dienstverlening. Dit lijstje voorbeelden is geenszins uitputtend.

De kans op grootschalige uitval is zeer klein?!

In 2011 voerden Berenschot en I&O research een telefonische enquête uit onder een groot aantal overheidsorganisaties (gemeenten, veiligheidsregio's, provincies, waterschappen). Destijds gaf 82% van de ondervraagde organisaties aan de kans op grootschalige uitval van ICT en/of elektriciteit als 'zeer klein' in te schatten. De helft van alle ondervraagden was van mening dat uitval van ICT en/of elektriciteit de continuïteit van de primaire dienstverlening niet zou verstoren.

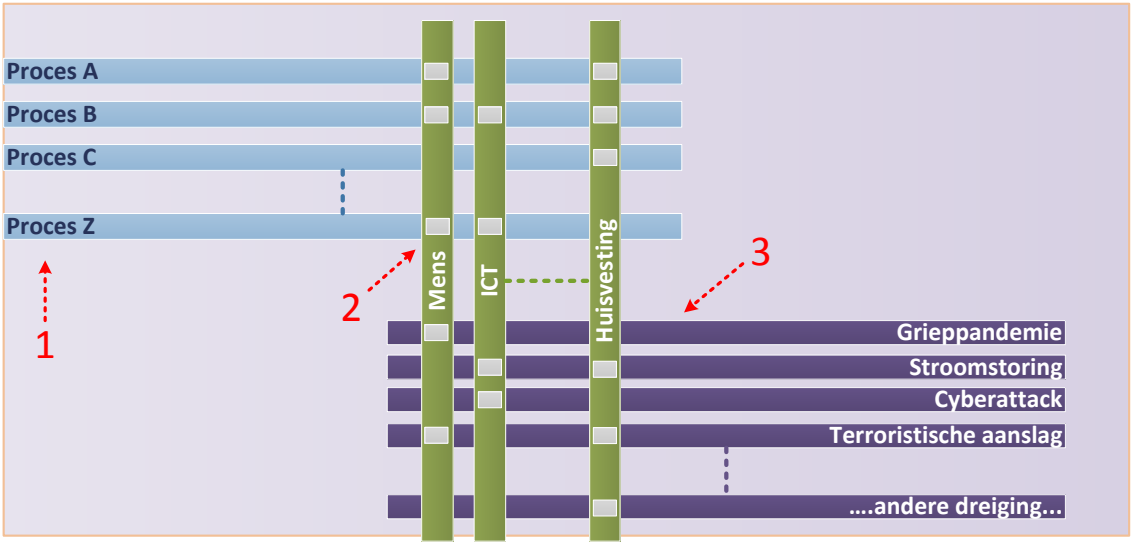
Deze uitkomsten zijn illustratief voor de lage risicoperceptie binnen de publieke sector ten aanzien van uitval van ICT en/of elektriciteit. In toenemende mate merken we dat de risicoperceptie bij bestuurders en management groeit, maar deze lijkt nog lang niet in balans te zijn met het risico op grootschalige uitval van ICT en/of elektriciteit .[2]

[1] Op basis van artikelen in het Eindhovens Dagblad op 18 & 24 juli en 26 september 2012 via www.ed.nl/extra/dossiers/brand-gemeentehuis-waalre

[2] In 2011 verrichtte Berenschot samen met I&O Research in opdracht van het WODC in geval van grootschalige uitval van ICT en/of elektriciteit bij gemeenten, provincies, veiligheidsregio's, politieregio's en waterschappen. Zie http://wodc.nl/onderzoeksdatabase/stand-van-zaken-continuiteitsplannen-van-de-sectoren-ob-en-oov.aspx?cp=44&cs=6796

3. Welk denkraam helpt bij continuïteitsmanagement?

Als hulp bij continuïteitsmanagement gebruiken wij een denkraam waarmee afhankelijkheden tussen dreiging, middelen en kritieke processen inzichtelijk kunnen worden gemaakt. De rode draad is als volgt: er zijn kritieke processen die niet mogen 'omvallen' – no matter what. Bij de uitvoering van de kritieke processen zijn middelen nodig (ICT, elektriciteit, personeel). Deze middelen kunnen echter wegvallen doordat ze geraakt worden doordat de dreiging van uitval werkelijkheid wordt..



Links bovenaan (1) is een aantal kritieke gemeentelijke dienstverleningsprocessen weergegeven. Verticaal staat een aantal middelen die nodig zijn om deze processen uit te kunnen voeren, zoals 'het middel' mens (personeel), ICT en huisvesting. Er zijn vanzelfsprekend andere middelen denkbaar (zoals elektriciteit, water, bepaalde specifieke voertuigen enzovoorts). Afhankelijkheden tussen processen en middelen is aangegeven als zij elkaar kruisen (2). Rechts onderaan is een aantal dreigingen afgebeeld, die de verschillende middelen kunnen raken (3).

Essentieel kenmerk van dit denkraam is dat een kritisch proces nooit rechtstreeks onderuit gaat door een dreiging. Het zijn immers de middelen die kwetsbaar zijn. En de kritieke processen zijn afhankelijk van deze middelen.

NB. Niet-kritieke processen zijn ook belangrijk, maar kunnen enig uitstel verdragen. Niet-kritieke processen zijn bijvoorbeeld 'planvorming', 'beleid maken', 'financial control', enzovoorts. Het is niet nodig voor deze processen speciale voorzieningen te treffen om ervoor te zorgen dat ze *no matter what* uitgevoerd ('gecontinueerd') kunnen blijven.

NB. Deze publicatie is niet gericht op álle middelen, maar alleen op de ICT en/of elektriciteit die nodig is voor de uitvoering van de kritieke processen. Het gaat om de uitval van ICT (computers, systemen, netwerk, software), al dan niet in combinatie met uitval van elektriciteit. Het plan gaat ook over situaties waarin slechts één van de twee middelen uitvalt. In zekere mate overlappen situaties van uitval ook. Continuïteit van elektriciteit is een *voorwaarde* voor continuïteit van ICT.

4. Wat verstaan we onder kritieke processen?

Bij uitval van ICT en/of elektriciteit vallen één of twee belangrijke middelen weg die nodig zijn voor de uitvoering van de dienstverleningsprocessen van de gemeente. Sommige processen kunnen best even stilvallen – zoals beleidsvorming op onderwerpen als onderwijsbeleid of het maken van bestemmingsplannen. Dit zijn de niet kritieke processen. Andere processen kunnen géén uitstel verdragen, 'alles mag omvallen behalve dát'. Dit zijn de kritieke processen.

Gemeenten zijn, net als elke moderne organisatie, in toenemende mate afhankelijk van ICT en/of elektriciteit voor hun dienstverlening. Communicatie met burgers, tussen medewerkers, de archieffunctie, het digitale parafen-systeem, het klantmanagementsysteem, de aanvraag van paspoorten en rijbewijzen, de toegang tot het GBA, de administratie van uitkeringen, de financiële huishouding, de interne telefoonlijst: het zijn allemaal voorbeelden van digitale middelen (applicaties en middelen) waarvan een gemeente in deze tijd volkomen afhankelijk is. Die afhankelijkheid maakt gemeenten kwetsbaar voor uitval van ICT en/of elektriciteit (en het maakt daarbij in wezen niet uit waardoor ICT en/of elektriciteit uitvalt).

Elke gemeente bepaalt zelf wat de kritieke processen zijn en bepaalt dus zelf welke dienstverlening niet mag stilvallen. Met uitzondering van enkele processen waarvan bij wet bepaald dat deze altijd beschikbaar moet zijn, bijvoorbeeld de Basisregistratie personen (BPR)[3]. In aanvulling daarop kan je denken aan de crisisbeheersingsprocessen in het kader van de bevolkingszorg (denk aan crisiscommunicatie, contact met de burgemeester, contact met hulpverleningsdiensten, opvang), processen die te maken hebben met de publieksbalie, het klantcontactcentrum en de website enzovoorts. Het is onze ervaring dat het lijstje kritieke processen dat een gemeente vaststelt doorgaans niet omvangrijk is en daarmee vrij overzichtelijk.

Kritieke of kritische processen?

Sommigen hebben het over *kritieke* processen, anderen hebben het over *kritische* processen. Over het algemeen bedoelt men hetzelfde. Zwart-wit bezien is er een verschil van betekenis: *kritisch* in de zin van 'het uiten van kritiek' en *kritiek* in de zin van 'belangrijk, gevaarlijk, cruciaal'. Vergelijk bijvoorbeeld: 'De slachtoffers werden in *kritieke* toestand naar het ziekenhuis gebracht' en 'De omstanders waren *kritisch* over de geleverde zorg'.

Tegelijkertijd zien we dat tegenwoordig *kritisch* en *kritiek* beide gebruikt worden in de betekenis 'cruciaal, beslissend' [4]. Het is onze ervaring dat op het terrein van continuïteit(smanagement) én op het terrein van crisismanagement vrijwel uitsluitend gesproken wordt van *kritische* processen.

[3] Voorheen bekend als gemeentelijke basisadministratie (GBA)

[4] https://onzetaal.nl/taaladvies/advies/kritisch-kritiek

Berenschot

Continuïteit(smanagement) in relatie tot …

5. … het grieppandemieplan uit 2009?

Het Continuïteitsplan Grieppandemie uit 2009 gaat over uitval van personeel door de Mexicaanse griep. Het zou dan ook in beeld moeten brengen welk en hoeveel personeel nodig is om de kritieke processen in de lucht te houden. Het Continuïteitsplan Grieppandemie uit 2009 is eenzelfde soort plan als het Continuïteitsplan ICT en/of uitval van elektriciteit – met dien verstande dat ándere afhankelijkheden belicht worden (enerzijds 'het middel' mens, anderzijds ICT en/of elektriciteit).

In 2009 werden gemeenten door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties dringend verzocht een Continuïteitsplan Grieppandemie op te stellen. De gedachte achter dit plan was de continuïteit van de dienstverlening te garanderen, óók als 20% of 30% van het personeelsbestand zou wegvallen. Het Continuïteitsplan Grieppandemie heeft dan ook niet zozeer te maken met de Mexicaanse griep, maar des te meer met 'het middel' mens. Namelijk het personeel van de gemeente, zonder wie een aantal (kritieke) gemeentelijke dienstverleningsprocessen geen doorgang kan vinden.[5]

In het Continuïteitsplan Grieppandemie – als het goed is – een lijst met kritieke processen aan (dat – als het goed is – hetzelfde is als degene in het Continuïteitsplan ICT en/of elektriciteit). Bovendien mag je per kritiek proces een inschatting verwachten van het aantal en het type functionarissen dat minimaal nodig is om het kritieke proces uit te voeren. En tot slot zal het Continuïteitsplan Grieppandemie beschrijven wat de gemeente geregeld heeft om ervoor te zorgen dat het kritieke proces kan blijven draaien als bijvoorbeeld 30% van het personeel wegvalt (door griep, ebola of anderszins). Dus: welke functies zijn onmisbaar, en wie vervult deze, wie is de achtervang, en wie is de achtervang van de achtervang?

Een integraal continuïteitsplan?

Het is niet onlogisch om één *integraal* continuïteitsplan te maken, waarin het wegvallen van alle middelen (personeel, ICT, elektriciteit, huisvesting enzovoorts) en de effecten daarvan op de uitvoering van de kritieke dienstverleningsprocessen in samenhang worden bekeken. Het is echter onze ervaring dat de scope van een dergelijk continuïteitsplan dermate grote proporties krijgt dat het een verlammend effect heeft – wat een aanmerkelijke barrière is om concrete stappen te zetten. Ons advies is dan ook om met een behapbaar onderdeel aan de slag te gaan. Eerst de continuïteit bij uitval van ICT en/of elektriciteit. En daarna de continuïteit bij uitval van personeel/menselijk kapitaal. En tot slot de continuïteit bij uitval van huisvesting. Omdat de onderliggende kritieke processen identiek zijn (althans, dat mag je verwachten), kunnen de drie afzonderlijke (deel)plannen uiteindelijk relatief eenvoudig worden geïntegreerd tot één geheel.

[5] In 2010 evalueerde Berenschot in opdracht van het ministerie van Volksgezondheid, Welzijn en Sport de aanpak bij Nieuwe Influenza A (H1N1 - Mexicaanse griep)in 2009. Eén van de negen evaluatievragen had betrekking op de op te stellen continuïteitsplannen binnen de publieke sector. Zie http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2011/03/14/kamerbrief-evaluatie-nieuwe-influenza-a-h1n1---de-mexicaanse-griep.html en Kamerstukken II, 22 894, nr. 297.

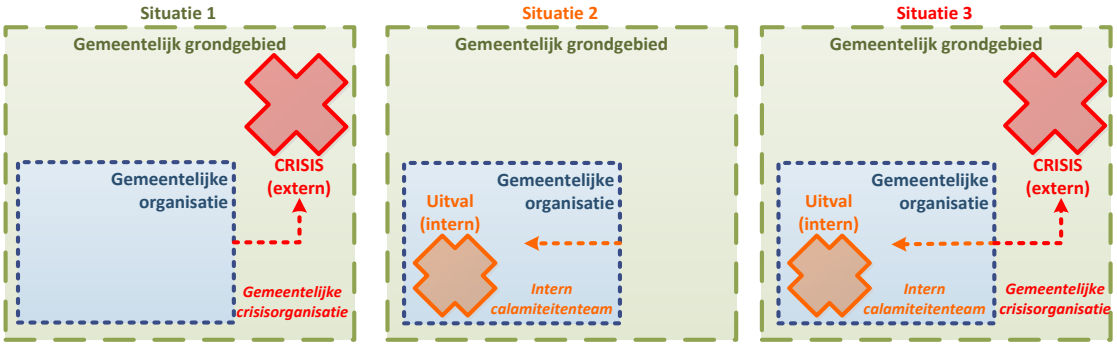
6. … crisismanagement?

Continuïteitsmanagement en crisismanagement zijn aan elkaar gerelateerd. En wel op twee manieren. In de eerste plaats richt continuïteitsmanagement zich op de kritieke processen – en daaronder vallen doorgaans ook de crisisbeheersingsprocessen (bijvoorbeeld crisiscommunicatie en opvang). In tweede plaats houdt continuïteitsmanagement in dat – in het uiterste geval – een beroep gedaan wordt op een (interne) crisismanagementorganisatie. In die zin is continuïteitsmanagement in de acute fase (als er sprake is van uitval) een vorm van crisismanagement.

Daarom vraag continuïteitsmanagement een keuze ten aanzien van het *intern* crisismanagement. Want als het dan toch misgaat, en ICT en/of elektriciteit valt uit, dan zal dat allerlei acties vragen van een aantal gemeentelijke functionarissen. Bijvoorbeeld om noodvoorzieningen te treffen en de schade te beperken. Als de effecten van de uitval beperkt zijn, dan zullen de acties binnen de reguliere lijnorganisatie van de gemeente worden opgepakt. Maar er zijn situaties denkbaar waarbij de reguliere lijnorganisatie niet meer afdoende is. In dat geval is er een 'gelegenheidsorganisatie' nodig, die als *interne* crisisorganisatie aan de slag gaat.

Nu kent elke gemeente een crisisorganisatie, maar deze crisisorganisatie is gericht op de wereld *buiten* het gemeente- of stadhuis (denk aan een grootschalige brand met giftige stoffen, maatschappelijke onrust in een wijk, enzovoorts). Deze crisisorganisatie – doorgaans opgebouwd rond een Gemeentelijk Beleidsteam of een Team Bevolkingszorg met actiecentra voor de uitvoering van de diverse crisisbeheersingsprocessen – heeft een *externe* focus en deze is niet per definitie behulpzaam bij uitval van ICT en/of elektriciteit met effecten op de dienstverleningsprocessen van de gemeente *zelf*.

In 'het ergste geval' is er zowel buiten als binnen de gemeente een crisissituatie: buiten is er een ramp gaande, binnen is er ICT-uitval.



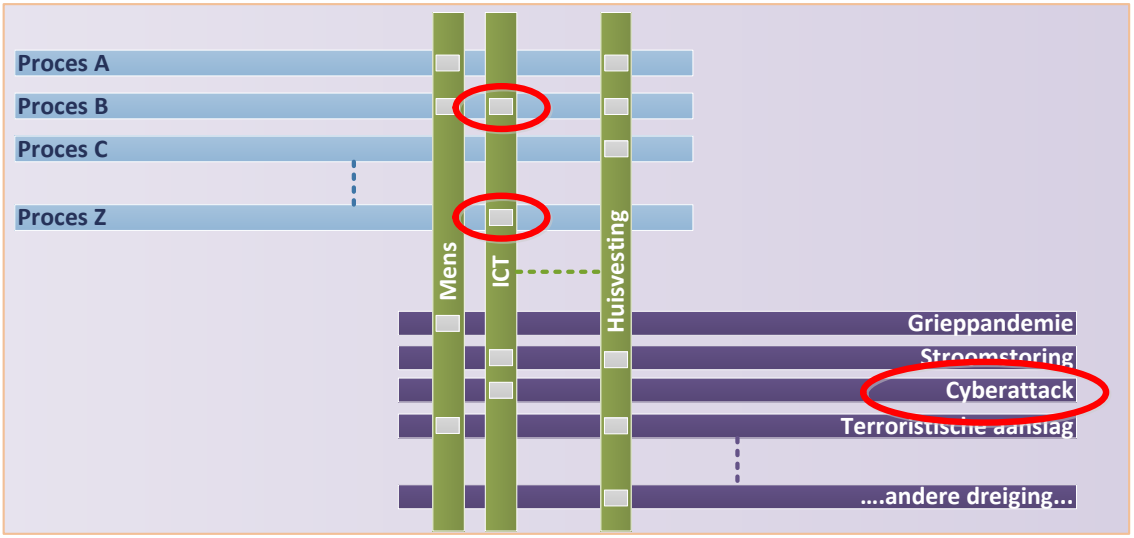
Aan gemeenten is de opgave om in het kader van de continuïteit bij uitval van ICT en/of elektriciteit het *intern* crisismanagement in te richten – en daarbij een eventuele verbinding met de gemeentelijke crisisorganisatie vorm te geven.

7. … cybercrime?

Vaak worden continuïteitsmanagement en cybercrime in één adem genoemd. Dat is begrijpelijk maar niet helemaal juist. Vanuit onze optiek is cybercrime een serieuze dreiging die de noodzaak voor continuïteitsmanagement onderstreept. Tegelijkertijd is cybercrime één van de oorzaken waardoor ICT en/of elektriciteit kan uitvallen en heeft het bij de vormgeving van continuïteitsmanagement geen wezenlijk andere plek dan de overige dreigingen

Cybercrime is een vorm van digitale criminaliteit die een ernstige bedreiging vormt of kan vormen voor de continuïteit van één of meerdere gemeenten. Denk bijvoorbeeld aan de Diginotar-affaire of stel je een digitale aanval op het gemeentelijke systeem van de gemeentelijke basisadministratie …. In die zin is cybercrime één van de dreigingen die in beeld kunnen komen bij het denken over continuïteit.

Tegelijkertijd staat bij continuïteitsmanagement het 'afhankelijkheids-denken' centraal – en niet zozeer het 'dreiging-denken'. Daarom is het in de meeste gevallen niet relevant door welk risico de ICT of de elektriciteit precies uitvalt. Het is wel relevant om te bepalen wat in geen geval mag omvallen en daartoe eventuele noodvoorzieningen te treffen.



Dát er maatregelen nodig zijn om weerbaar te zijn tegen cybercrime staat overigens als een paal boven water. Daarom is dit een punt van aandacht bij ontwerp, inrichting en beheer van ICT.

8. … informatieveiligheid?

Informatieveiligheid is gericht op het garanderen van de beschikbaarheid, vertrouwelijkheid en betrouwbaarheid van informatie van een gemeente én op de continuïteit van de informatievoorziening. Het continuïteitsdenken bij uitval van ICT en/of elektriciteit richt zich in het bijzonder op datgene dat niet (no matter what) mag uitvallen. In situaties waar de informatievoorziening onderdeel is van de kritieke processen (en waar is dat niet…) raken beide begrippen elkaar.

Schematisch laat het zich als volgt schematiseren:

Gemeenten staan aan de lat om zowel de informatieveiligheid als de continuïteit van dienstverlening bij uitval van ICT en/of elektriciteit op orde te hebben. Daarom wordt vanuit het Rijk zowel ten aanzien van informatieveiligheid als op het terrein van continuïteit een aantal handreikingen gedaan[6]. Het gaat dan om de volgende zaken:

- Informatieveiligheid: In 2012 stelde de ministerie van Binnenlandse Zaken en Koninkrijksrelaties de Taskforce Bestuur en Informatieveiligheid Dienstverlening in. Op de website van de taskforce is allerlei informatie voorhanden rondom (de continuïteit van) informatieveiligheid. In 2015 wordt de Taskforce ontbonden en wordt het werk overdragen aan de in 2014 aangestelde Digicommissaris.
- Continuïteit bij uitval van ICT en/of elektriciteit: In 2011 is een peiling is gedaan naar de stand van zaken rond continuïteitsplannen, waarna in 2013 zijn onder meer veiligheidsregio's met externe ondersteuning zijn begeleid bij het opstellen van hun continuïteitsplan. De inzichten en best-practices die hierbij zijn opgedaan stelt het ministerie van Binnenlandse Zaken en Koninkrijksrelaties met deze publicatie beschikbaar aan gemeenten, samen met het daarbij horende Model-Continuïteitsplan bij uitval van ICT en/of elektriciteit.

[6] In de voortgangsbrief Nationale Veiligheid is de noodzaak van continuïteitsmanagement onderstreept en is gewezen op de verantwoordelijkheden van de betrokken sectoren. In de brief is opgenomen dat samen met koepelorganisaties van gemeenten, provincies en waterschappen ondersteuning wordt geboden om continuïteitsmanagement te verbeteren. Zie Kamerstukken II, 2013 -2014, 30 821, nr. 19. https://zoek.officielebekendmakingen.nl/kst-30821-19.html

Berenschot

Continuïteitsplan uitval ICT en/of elektriciteit

9. Wat voegt een plan toe aan continuïteit?

Alleen een plan zal weinig toevoegen aan de continuïteit van een gemeente. Een planvormingstraject kan dat wel. Zeker als het planvormingstraject aan een aantal kenmerken voldoet en gedragen wordt door een sterke 'plannenmaker'. Dan wordt een gemeente geholpen om op gestructureerde en efficiënte wijze na te denken over - en keuzes te maken met betrekking tot - de continuïteit van de gemeentelijke dienstverlening bij uitval van ICT en/of elektriciteit.

Ervaring leert dat alleen een papieren document met de noemer 'plan' doorgaans weinig toegevoegde waarde heeft, waarmee het simpelweg hebben van een plan beschouwd kan worden als, op zijn minst, een inefficiënte besteding van tijd en geld. Desondanks pleiten wij voor het opstellen van een continuïteitsplan – als vehikel om het continuïteitsmanagement van de grond te krijgen. Een dergelijk plan vraagt het één en ander van planvormingstraject en de plannenmaker(s). Namelijk:

- Het bij elkaar brengen van verschillende functionarissen van zowel ICT, beheer, facilitair, beleid, planvorming en crisismanagement.
- Het expliciteren van een gemeenschappelijke taal – zodat men elkaar minder glazig aankijkt bij termen als *serverparken, switches en fiber rings* enerzijds en *GRIP, SIS en bevolkingszorg* anderzijds.
- Het 'opschudden' van verbeeldingskracht ten aanzien van mogelijke situaties en het handelingsrepertoire – om het denken vanuit de eigen koker te doorbreken.
- Het scheppen van kaders waarbinnen de gemeente moet (kunnen) opereren.
- En niet onbelangrijk: het in kaart brengen van keuzes ten aanzien van kritieke processen, afhankelijkheden en beschikbaarheid van ICT en/of elektriciteit, benodigde noodvoorzieningen, rest-risico's en crisisorganisatie.

Een planvormingstraject dat aandacht heeft voor deze zaken zal waardevol bijdragen aan de continuïteit van de gemeentelijke dienstverlening bij uitval van ICT en/of elektriciteit.

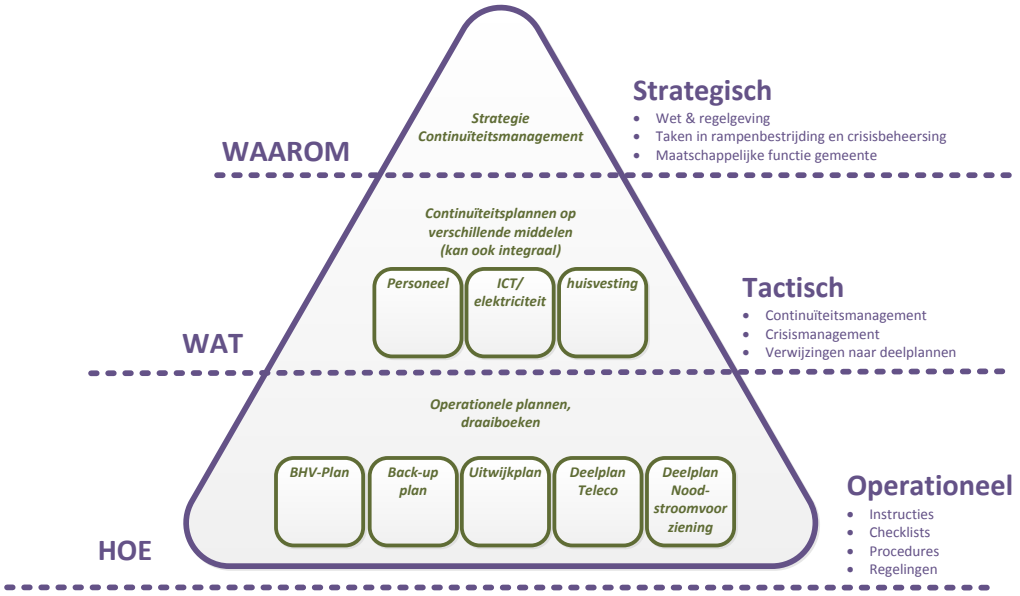
Een plan opstellen leidt tot (meer) bewustwording van de problematiek en inzicht in de risico's en consequenties. Een plan creëert ruimte om afspraken te maken met partners en in de praktijk te testen of te oefenen hoe het werkt. Zie het plan niet als statisch resultaat, benut de kansen die het planvormingstraject biedt.[7]

[7] In 2009 heeft Berenschot, samen met Nicis/ Platform 31, TU Delft en Brandweer Amsterdam Amstelland een publicatie uitgebracht over de kloof tussen plannen en de praktijk. Zie http://www.berenschot.nl/inspiratie/publicaties-0/publicaties/uitgaven-fundatie/plannen-praktijk/

10. Wat voor type plan is een continuïteitsplan?

Het continuïteitsplan is wat plan-theoretici een tactisch plan noemen. Het zet niet de richtinggevende kaders uit, zoals een strategisch plan. Het omvat evenmin telefoonlijsten of checklists zoals een operationeel plan. Een tactisch plan brengt consequenties van de richtinggevende (strategische) kaders in beeld en beschrijft besluiten en activiteiten – welke nadere (operationele) uitwerking vragen.

Om het onderscheid tussen strategisch, tactisch en operationeel te verhelderen wordt onderstaande piramide vaak gebruikt. De piramide geeft de drie 'planniveaus' weer: strategisch, tactisch, operationeel.



- Het strategische niveau heeft betrekking op de kaders. Een strategisch plan bevat interpretaties van wet- en regelgeving, beschrijft op hoofdlijnen welke doelen en taken relevant zijn en koppelt deze aan de maatschappelijke functie van de gemeente.
- Het tactische niveau heeft betrekking op het realiseren van de doelen en taken – gegeven de strategische kaders. Wat moet er gedaan worden om deze te realiseren? Welke stappen moeten doorlopen worden om de continuïteit van de kritieke processen te borgen?
- Het operationele niveau omvat concrete instructies, actiepuntenlijsten en checklists, die beschrijven hoe de in het tactische plan benoemde stappen gerealiseerd gaan worden.

Overigens zien we in de praktijk dat de scheiding minder strikt wordt gehanteerd dan de piramide doet vermoeden. We treffen niet zelden continuïteitsplannen aan die zowel strategische, tactische als operationele elementen bevatten. Ook zien we dat het strategisch kader waarbinnen een continuïteitsplan valt niet altijd expliciet wordt gemaakt – maar min of meer volgt uit wet- en regelgeving en de beleidskaders op basis waarvan de gemeentelijke dienstverlening vorm is gegeven.

11. Wat levert het continuïteitsplan concreet op?

Het doorlopen voor het planvormingstraject levert een aantal concrete inzichten op met betrekking tot de continuïteit van de gemeentelijke organisatie bij uitval van ICT en/of elektricteit. Daarbij valt te denken aan:

- Een lijst van kritieke processen en niet-kritieke processen (‘deze wel, deze niet’) (‘deze processen mogen niet omvallen, deze wel’).
- Een inventarisatie van afhankelijkheid en beschikbaarheid van ICT, zowel software en hardware (‘deze kritieke processen kunnen bij uitval waarschijnlijk wel in de lucht blijven, deze waarschijnlijk niet’).
- Overzicht van reeds getroffen noodvoorzieningen (‘dit is wat we geregeld hebben aan back-ups, uitwijklocaties, fall-back enzovoorts’).
- Inzicht in het rest-risico – 100% continuïteit is immers niet te garanderen – met mogelijke alternatieven (‘het rest-risico kan verkleind worden als we noodvoorziening x organiseren, maar dat kost wat’).
- Een keuze ten aanzien van de crisisorganisatie waarop een beroep gedaan kan worden als het toch mis gaat (‘functionaris x staat aan de lat, en formeert een crisisteam met y en z’ of ‘we gebruiken onze reguliere crisisorganisatie’ of ‘we richten een intern crisisteam op met de focus op ICT’).

Uitvalsduur van kritieke processen

Één van de redenen waarom het continuïteitsplan scherpe inzichten oplevert, is dat het plan een strikte definitie van uitval hanteert. Doordat het plan zich richt op die processen die niet mogen uitvallen, is het mogelijk scherp aan de wind te varen. Echter, er zijn ook gemeenten die een nadere prioritering van processen aanbrengen. Zij beschrijven naast de enkele processen die *niet* (‘*no matter what’)* mogen uitvallen ook een aantal processen die bijvoorbeeld ‘*wel een paar uur, maar geen dag of week’* mogen uitvallen.

In onze visie op continuïteit kiezen we een helder standpunt: continuïteit gaat over de processen die *niet* mogen uitvallen. Voor díe processen moet je continuïteit borgen. Overige processen zijn ook belangrijk, maar kunnen enig uitstel verdragen.

Het is aan de gemeente om een eigen afweging in deze te maken: richten we ons alleen op de processen die *geen* uitstel verdragen (écht kritiek), of nemen we ook processen mee waarbij tijdelijke uitval mogelijk is (bijvoorbeeld een aantal uur). Ons advies is om deze wel haarscherp te onderscheiden omdat dit effect zal hebben op de investeringsbeslissingen die je voorlegt aan het managementteam of college met betrekking tot het versterken van continuïteit.

Het doorlopen van het planvormingsproces

12. Van start, maar hoe?

Het opstellen van een continuïteitsplan hoeft geen zwaarbeladen en moeizaam planvormingstraject te zijn. De benodigde kennis is al in de gemeente aanwezig. Het gaat om het zo efficiënt mogelijk verzamelen, selecteren en bundelen van deze kennis.

Een planvormingstraject om te komen tot een continuïteitsplan voor uitval van ICT en/of elektriciteit laat zich opknippen in drie fases. Na de beginfase, waarin de piketpalen voor het continuïteitsplan geslagen worden, volgt de planfase, wat onder meer het daadwerkelijke schrijfwerk omvat. Na vaststelling wordt het plan in de implementatiefase concreet geoperationaliseerd – inclusief het trainen en oefenen van situaties waarin sprake is van uitval van ICT en/of elektriciteit.

Onze ervaring is dat de beginfase en de planfase gezamenlijk een tijdshorizon kennen van minimaal 3 maanden. De implementatiefase is meer een continu proces van operationaliseren, trainen, oefenen en updaten. De volgende stappen helpen je bij de eerste twee fasen een eind op weg:

- Zorg voor **commitment** van je bestuurder(s) en/of management
- Organiseer een 'Plansessie' voor het betrokken team om
  - urgentie en noodzaak van plan creëren
  - inzichtelijk te maken wat en wie nodig zijn in het planvormingstraject
- Inventariseer en bepaal de kritieke processen voor de eigen dienstverlening
- Breng het ICT-landschap in kaart gegeven de kritieke processen:
  - Van welke applicaties zijn de kritieke processen afhankelijk?
  - Van welke hardware zijn die applicaties afhankelijk?
  - Hoe beschikbaar zijn de applicaties en systemen bij uitval van ICT en/of elektriciteit?

De opbrengst van deze exercitie is een inschatting van de mate waarin kritieke processen 'in de lucht blijven' bij uitval van ICT en/of elektriciteit (zeker niet, waarschijnlijk, zeker wel).

13. Van start, maar met wie?

Bij het opstellen van een continuïteitsplan ICT en/of elektriciteit is een multidisciplinair team nodig. Ten minste één 'plannenmaker' en één ICT-expert. Afhankelijk van de gemeente betrek je meerdere collega's, bijvoorbeeld ook een OOV-er, een facilitair beheerder, een beveiligingsfunctionaris, enzovoorts.

Het organiseren van de continuïteit van de dienstverlening van de kritieke gemeentelijke processen vraagt input en draagvlak van verschillende onderdelen van de gemeente zoals ICT, bedrijfsvoering en OOV/ Crisisbeheersing. Denk aan functionarissen van:

- ICT en/of automatisering
- Bedrijfsvoering en/of facilitaire dienst
- Publiekszaken en/of communicatie
- Gebouwbeheer en/of beveiliging
- OOV-taken/crisisbeheersing

Ook kan het raadzaam zijn het team te versterken met één of twee 'externe meedenkers', bijvoorbeeld iemand van het energiebedrijf, de beheerder van het externe serverpark of van de hulpverleningsdiensten en/of veiligheidsregio of anderszins.

Taalbarrière

De betrokken collega's zijn (gemeentelijke) functionarissen die elkaar niet per definitie goed verstaan. En dat bedoelen we letterlijk. De ervaring leert dat er zeker in de **beginfase** sprake kan zijn van een taalbarrière tussen met name de plannenmaker en de meer technische teamleden. Zorg er dan ook voor dat je in je team iemand betrekt die de vertaling kan maken tussen de wereld van veiligheid en crisismanagement en de technische wereld van *switches*, *serverparken*, *hubs* en *fiber rings*.

Vier (technische ICT) termen en hun betekenis

- **Servers:** Servers zijn de 'computers' waarop het netwerk van de gemeente draait. Alle gemeenschappelijke data staan op deze computers. De programma's waar medewerkers mee werken staan vaak (nog) op de eigen computer, maar de databases waarmee deze programma's werken staan meestal op de servers. Daardoor worden veel programma's onbruikbaar bij uitval van servers. Ook het netwerk valt dan uit, waarmee ook e-mail en internet (vaak) uitvallen. Servers zijn doorgaans extern ingekocht en soms wel / soms niet in eigen beheer gebracht. Dit laatste geldt voor de meeste gemeenten. Je hebt dan te maken met een externe leverancier voor deze vitale infrastructuur
- **Netwerk:** Een netwerk kan betrekking hebben op een fysiek netwerk: de kabels tussen de werkstations (pc's van medewerkers) en de servers, wat het mogelijk maakt om te internetten, e-mailen, data uit te wisselen, bij de gemeenschappelijk schijf te komen etc. Dit fysieke netwerk kan ook draadloos zijn (WiFi). Tot slot kan een netwerk betrekking hebben op een virtuele omgeving waarin computers met elkaar communiceren, informatie delen, waarin programma's draaien etc.
- **Switches & hubs:** Dit zijn de apparaten die onderdeel uitmaken van het netwerk en het mogelijk maken dat computers met elkaar communiceren. Ze zijn als het ware de verkeersregelaars van het netwerk. Hoewel hubs eigenlijk een net andere (iets slimmere) vorm van verkeersregelaars zijn dan switches, volstaat het ze onder één noemer te scharen – alhoewel de echte ICT'er hier de wenkbrauwen zal fronsen …
- **Applicatielandschap:** Het applicatielandschap is een verzamelnaam van alle programma's die een gemeente op haar netwerk heeft draaien. Dit zijn dus zowel de frontoffice applicaties (die je gebruikt en op je bureaublad ziet), de midoffice applicaties (die de communicatie van frontoffice met backoffice organiseren) en de backoffice applicaties (de databases). Let wel, in deze context hebben frontoffice, midoffice en backoffice niets te maken met de frontoffice en backoffice in de afdeling dienstverlening. Het is belangrijk te beseffen dat het totale applicatielandschap van een gemeente al gauw honderden applicaties kan omvatten en dikwijls in totaliteit niet wordt overzien.

14. Hoe en wanneer betrek je je bestuurder?

Continuïteitsmanagement en het opstellen van een continuïteitsplan is onbegonnen werk zonder commitment en akkoord van de verantwoordelijke bestuurder(s) en /of manager. Alles overziend is zijn haar/hun betrokkenheid nodig op drie onderdelen: 1) commitment om met continuïteit aan de slag te gaan 2) vaststellen van de gemeentelijke kritieke processen 3) besef van de rest-risico's.

1) (Bestuurlijk) commitment aan de noodzaak om het continuïteitsmanagement vorm te geven lijkt triviaal – maar al te vaak zien we dat daar gemakshalve aan voorbij wordt gegaan. Met als gevolg dat degene die het planvormingstraject moet trekken, de 'plannenmaker' bij collega's geen tijd en inzet vrijgemaakt krijgt om met het onderwerp aan de slag te gaan. En de betrokkenheid van de collega's is bij continuïteitsmanagement cruciaal. Zonder commitment is de kans groot dat je als plannenmaker tot de conclusie moet komen dat het trekken aan een dood paard is. Om je die ervaring te besparen, raden we je aan op bestuurlijk en/of managerial niveau een 'go' te krijgen – voordat je echt van start gaat.

2) Een volgende mijlpaal in het planvormingstraject is het laten vaststellen van de kritieke processen van de gemeente door het college of managementteam. Met het vaststellen van de kritieke processen wordt ook bepaald welke processen níet kritiek zijn: voor de niet-kritieke processen worden geen aanvullende maatregelen of noodvoorzieningen getroffen.

3) Tot slot gaat het vaststellen van de kritieke processen hand in hand met het aanvaarden van de rest-risico's. De investeringen die gedaan moeten worden om kritieke processen 'in de lucht' te houden, kennen grenzen. Uiteindelijk is het een (vaak) bestuurlijke keuze welke investeringen continuïteit van de kritieke processen waard is. Belangrijke notie is dat het per definitie onmogelijk is om alle risico's op uitval van kritieke processen weg te nemen.

15. Hoe blijf je voortgang maken?

In een planvormingstraject is het de kunst de vaart er in te houden en de gezamenlijke betrokkenheid zo efficiënt en doeltreffend mogelijk te benutten. Een aantal – algemeen geldende – tips kunnen daarbij helpen.

- Zorg voor één of twee penvoerders (plannenmakers) van het conceptplan om het schrijfproces te vergemakkelijken.
- Hou er rekening mee dat het 'achter de broek zitten' van inputleveraars tijd kost. Met commitment van je bestuurder(s) en/of management zal dat aanzienlijk gemakkelijker gaan dan zonder.
- Organiseer een 'Plansessie' om urgentie en noodzaak te delen. Ook kun je hier goed inzichtelijk maken 'wie en wat, wanneer' nodig zijn in het planvormingstraject.
- Organiseer een 'Papieren tijgerscan' om een eventueel concept continuïteitsplan te beoordelen op de (toegevoegde waarde van) inhoudelijke aspecten: staat er alléén dat in wat nodig is? Staan er geen overbodige dingen in? Is duidelijk voor wie de informatie relevant is?
- Voorkom tunnelvisie door 'externe meedenkers' te betrekken (bijvoorbeeld iemand van het energiebedrijf, de beheerder van het externe serverpark of van de hulpverleningsdiensten en/of veiligheidsregio of anderszins). Deze 'ogen van buiten' kunnen helpen om '*taken for granted*-opvattingen' te doorbreken en de verbeelding te prikkelen.

Berenschot

Het vullen van het Model-Continuïteitsplan

16. Wat is het Model-Continuïteitsplan?

Op basis van ervaringen bij verschillende veiligheidsregio's, gemeenten en provincies is een Model-Continuïteitsplan tot stand gebracht. Dit Model-Continuïteitsplan is een geannoteerde inhoudsopgave die als leidraad kan dienen in het planvormingstraject. Het Model-Continuïteitsplan bevat alle basiselementen die je in een continuiteïtsplan bij uitval van ICT en/of elektriciteit mag verwachten en het markeert de onderwerpen waarover een gemeente (in casu de bestuurder) ten minste beslissen moet.

Het is niet verplicht om het Model-Continuïteitsplan te gebruiken. Het dient ter ondersteuning en kan al gelang de behoefte in meer of mindere mate als leidraad dienen.

- Het plan heeft een **interne focus** en is gericht op de situatie waarbij de uitval van ICT en/of elektriciteit de organisatie van de gemeente zélf raakt. Dus: dit plan heeft géén betrekking op wat de gemeente te doen staat in geval van uitval richting burgers en bedrijven (daarvoor dient andere planvorming). In de realiteit kunnen deze twee situaties wél hand in hand gaan.
- Het plan beschrijft **maatregelen** bij uitval van ICT en/of elektriciteit. Hierbij gaat het niet om maatregelen om uitval van ICT en/of elektriciteit te voorkomen (bijvoorbeeld preventieve maatregelen om ICT-incidenten te melden of het redundant (dubbel) uitvoeren van ICT-infrastructuur), maar om de gevolgen op te vangen.
- Het plan beschrijft de **crisisbeheersing** bij uitval van ICT en/of elektriciteit. Hierbij gaat het bijvoorbeeld om (reactieve) acties, zoals het uitwijken naar een alternatieve locatie, het acuut mobiliseren van de benodigde interne en externe expertise, of het terugplaatsen van de meest actuele back up of het terugschakelen naar de reguliere elektriciteitsvoorziening (in het kader van herstel).

Het Model-Continuïteitsplan bevat een tool (Excelwerkmap) om de afhankelijkheden tussen kritieke processen, software (applicaties) en hardware (systemen) inzichtelijk te maken en te scoren op beschikbaarheid. Met deze tool kun je inzichtelijk maken welke kritieke processen bij uitval *zeker* gecontinueerd kunnen worden, *waarschijnlijk* gecontinueerd kunnen worden of *zeker niet* gecontinueerd kunnen worden.

Het is niet verplicht de tool te gebruiken. In de bijlage is het Model-Continuïteitsplan, inclusief tool, opgenomen.

17. "Wat zijn de kritieke processen"?

Vraag een gemiddelde medewerker wat binnen zijn organisatie kritieke processen zijn en deze komt na enig nadenken met een waslijst aan producten, diensten en processen. Maar zo complex is continuïteitsmanagement helemaal niet; op de keper beschouwd zijn er maar heel weinig écht kritieke processen. Het gaat immers om de processen die niet mogen uitvallen, 'no matter what'.

Enkele voorbeelden van kritieke processen zoals wij die tot dusver bij gemeenten zijn tegen gekomen in het kader van continuïteitsmanagement:

Crisisbeheersingsprocessen	Dienstverleningsprocessen
- Crisiscommunicatie - Opvang en verzorging - Verplaatsing - Primaire levensbehoeften - ……	- Publieksbalie (het bereikbaar kunnen zijn), voorlichting (website), Klantcontactservice (call center), - Bedienen van bruggen, sluizen, gemalen, verkeerslichten - Bijstandsuitkering, schuldhulpverlening - ….

Het bepalen van de kritieke processen verloopt doorgaans in twee stappen. Eerst leveren de verschillende (dienst)onderdelen van de gemeente onderwerpen aan voor een groslijst. Op de groslijst staan vaak allerlei processen, zoals 'crisiscommunicatie', 'salarisadministratie' en 'toezicht en handhaving'. Daarna vindt een brede bespreking plaats (met het team, met de bestuurder). Dan blijkt dat een aantal processen wel belangrijk zijn, maar niet kritiek (bijvoorbeeld: crisiscommunicatie wel, salarisadministratie niet). Desgewenst vindt een nadere prioritering binnen de kritieke processen plaats, zodat duidelijk is welk kritieke proces met stip boven aan staat.

Met de uiteindelijke selectie van kritieke processen kan je aan de slag: Van welke ICT-componenten zijn deze processen afhankelijk? Hoe zit het met de stroomvoorziening? Wat kan worden gedaan om 'uitval' te voorkomen? Wat is het plan als dat toch gebeurt?

Kritieke locaties

We richten ons in dit boekje en het plan op de kritieke processen. Echter, de concrete uitvoering van veel processen heeft doorgaans plaats op één of meerdere locaties. Bijvoorbeeld op het stadhuis, stadsdeelkantoor, gemeentewerf of andere vestiging van de gemeente.

Daarom is het de moeite waard om stil te staan bij de relatie tussen processen en locaties. Immers: welke fysieke locaties zijn essentieel voor de uitvoering van de kritieke processen? Als de gemeente over veel locaties beschikt, dan is het raadzaam om te werken met prioritering van locaties. Consequentie van het aanwijzen van prioritaire locaties betekent dat er **geen** noodvoorzieningen worden getroffen voor de overige locaties.

18. "Van welke ICT zijn de kritieke processen afhankelijk?"

Nadat kritieke processen zijn benoemd kan het ICT-landschap in kaart worden gebracht. Dat wil zeggen dat per kritiek proces wordt bepaald welke ICT nodig is om 'in de lucht te blijven'. De inventarisatie van het ICT-landschap is, mits goed georganiseerd, geen ingewikkelde opgave. Sterker nog: omdat de inventarisatie alleen gedaan wordt voor de kritieke processen, is de vereiste inspanning goed te overzien.

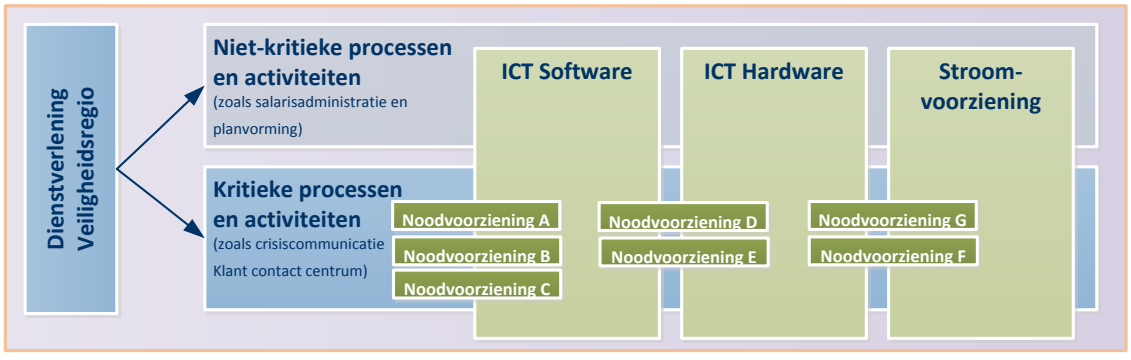
Bij het in kaart brengen van het ICT-landschap gaat het in elk geval om de volgende zaken:

Afhankelijkheden van het kritieke proces qua software (applicaties) en hardware (apparaten, netwerkverbindingen etc.). Centrale vraag is: wat heeft het betreffende kritieke proces nodig om te draaien?

Beschikbaarheid van software en hardware bij uitval van ICT en/of elektriciteit. Immers: sommige applicaties en systemen zijn dubbel uitgevoerd of kunnen in zeer korte tijd op een andere locatie/netwerk uitgerold worden. Andere applicaties of systemen zijn zeer kwetsbaar. Centrale vraag is steeds: in hoeverre zal software en hardware beschikbaar zijn bij uitval? Daarbij hanteren we een grofmazige inschatting, en wel als volgt.

- Score 1: Niet bestand tegen uitval van onderdelen en uitval bij onderhoud: onderdelen zijn niet dubbel uitgevoerd en er zijn geen dubbele aanvoerlijnen, hardware zit niet op noodstroom (en dus niet beschikbaar bij uitval of onderhoud).
- Score 2: Meer bestand tegen uitval van onderdelen. Dubbel uitgevoerde onderdelen en dubbele aanvoerlijnen. Niet altijd bestand tegen onderhoud (waarschijnlijk wel beschikbaar bij uitval stroom, niet beschikbaar bij onderhoud).
- Score 3: Meest bestand tegen uitval van onderdelen. Alle onderdelen dubbel uitgevoerd, aanvoerlijnen dubbel en achter noodstroom. Ieder onderdeel is te onderhouden zonder uitval. Hardware kan verdeeld zijn over meerdere locaties (deze componenten zijn beschikbaar bij uitval).

Voor deze inventarisatie is een tool beschikbaar, als onderdeel van het Model-Continuïteitsplan. Op basis van de inventarisatie kan een inschatting gemaakt worden over de continuïteit van de kritieke gemeentelijke processen: namelijk, welke kunnen vrijwel zeker 'in de lucht blijven', welke 'misschien' en welke 'zeker niet'?



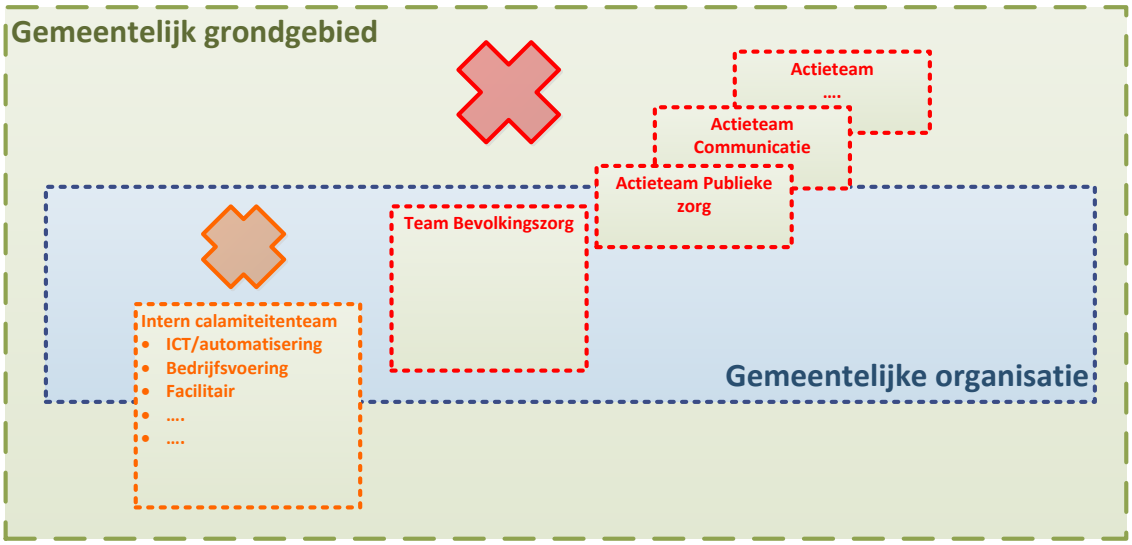
19. "Welke crisisorganisatie wordt gebruikt?"

Continuïteitsmanagement vraagt een keuze ten aanzien van het intern crisismanagement. Want als het dan toch misgaat, en de ICT en/of elektriciteit valt uit, dan zal dat allerlei acties vragen van een aantal gemeentelijke functionarissen om noodvoorzieningen te treffen en de schade te beperken. Zijn de effecten van de uitval beperkt, dan zullen de acties binnen de reguliere lijnorganisatie van de gemeente worden opgepakt. Er zijn echter situaties denkbaar waarbij de reguliere lijnorganisatie niet meer afdoende is. In dat geval is er een 'gelegenheidsorganisatie' nodig, die als interne crisisorganisatie aan de slag gaat.

Bij het bepalen van de passende crisisbeheersingsorganisatie zijn er, zwart-wit bezien, twee uitersten.

Enerzijds kan aansluiting gezocht worden bij 'reguliere' gemeentelijke crisisorganisatie door instelling van bijvoorbeeld een 'Actieteam Interne organisatie' – onder aansturing van het Team Bevolkingszorg (TBZ) of het Gemeentelijk Beleidsteam (GBT). Het nadeel hiervan is dat de reguliere gemeentelijke crisisorganisatie 'van nature' op de buitenwereld gericht, terwijl het betreffende Actieteam een interne focus heeft.

Anderzijds kan een eigenstandig intern crisisteam opgericht worden, dat zelfstandig kan functioneren, los van de reguliere gemeentelijke crisisorganisatie. Het nadeel hiervan is dat het team té eigenstandig functioneert en in tijden van crisis als het ware loszingt van de reguliere lijnorganisatie én reguliere crisisorganisatie.



Berenschot

Bijlage: Model-Continuïteitsplan bij uitval ICT en/of elektriciteit

In 2013 begeleidde Berenschot in opdracht van het ministerie van Veiligheid en Justitie de 25 veiligheidsregio's bij het opstellen van hun continuïteitplan ICT en/of elektriciteit met behulp van een modelplan. De inzichten en best-practices die daarbij zijn opgedaan, zijn verwerkt in een een modelplan voor gemeenten. Zie ook https://www.nctv.nl/actueel/nieuws/magazine-nationale-veiligheid-en-crisisbeheersing-nummer-3-2014.aspx . Hieronder is een (deels) gevuld Model-Continuïteitsplan bij uitval van ICT en/of elektriciteit **voor gemeenten** opgenomen.

Inhoudsopgave

1. Inleiding

1.1. Wat is ons doel en onze doelgroep

Dit continuïteitsplan heeft betrekking op toekomstige situaties waarin sprake is van uitval van ICT en/of elektriciteit waardoor de organisatie van de gemeente *zelf* geraakt wordt. Als gevolg daarvan komt de dienstverlening van de gemeente in het geding. De aanleiding kan een stroomstoring zijn waardoor ICT, energievoorzieningen en huisvesting niet meer of maar gedeeltelijk functioneren. Maar ook zonder stroomstoring kan de ICT van de gemeente uitvallen (bijvoorbeeld als gevolg van een cyberattack) met allerlei mogelijke consequenties.

Doel van dit plan is om de effecten van een verstoring zoveel mogelijk te reduceren, de dienstverlening van de gemeente te continueren en het herstel te bespoedigen. Het beschrijft twee aspecten:

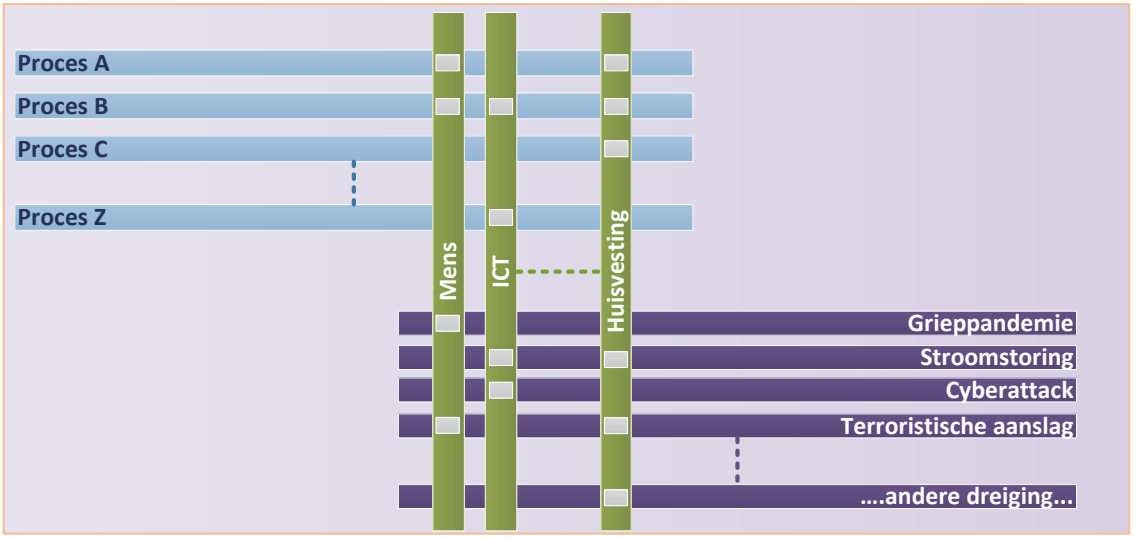
- Ter voorbereiding heeft de gemeente een aantal maatregelen getroffen om zodoende (nood)voorzieningen te organiseren. Deze noodvoorzieningen moeten het functioneren van de kritieke processen van de gemeente in geval van uitval van ICT en/of elektriciteit opvangen – althans voor een bepaalde periode. Zie hoofdstuk 3.
- Tijdens uitval ICT en/of elektriciteit onderneemt de gemeente een aantal activiteiten om de continuïteit van haar eigen dienstverlening in stand te houden of te herstellen en de effecten zo snel en effectief mogelijk te beperken. Zie hoofdstuk 4.

Doelgroep van dit plan zijn de functionarissen die bij uitval belast zijn met het zoveel mogelijk reduceren van de effecten van een verstoring, het continueren van de kernactiviteiten van de gemeente en de voorbereiding op uitval. Op bestuurlijk niveau is dat het college van burgemeester en wethouders, op tactisch/operationeel niveau is dat het managementteam onder leiding van de gemeentesecretaris, en functionarissen binnen de gemeente met expertise op het gebied van facilitaire zaken (zoals ICT inclusief telefonie/andere communicatiemiddelen, gebouwbeheer en beveiliging).

⇨ Kort dit desgewenst in/pas het desgewenst aan gegeven de gemeentelijke situatie.

1.2 Wat zijn onze uitgangspunten

Bij het opstellen van dit plan is de dienstverlening van de gemeente *zelf* het startpunt. De dienstverlening omvat een aantal kritieke en niet-kritieke processen. De uitvoerbaarheid daarvan is afhankelijk van beschikbare *middelen* (bijvoorbeeld menskracht, ICT of transportmiddelen en huisvesting). Deze middelen kunnen door externe factoren (ofwel *risico's*) geraakt worden (bijvoorbeeld een grieppandemie met uitval van menskracht tot gevolg, een stroomstoring met effect op ICT). De impact van de uitval van ICT en/of elektriciteit op de beschikbaarheid van middelen zal verschillen en daarmee ook op de uitvoering van de kritieke processen. Hieronder is de relatie tussen kritieke processen, middelen en risico's schematisch uitgebeeld.



Met andere woorden: de uitvoering van een kritiek proces van de gemeente (zoals het laten verstrekken van wekelijkse uitkeringen bij schuldhulpverlening of het verstrekken van reisdocumenten, rijbewijzen en uittreksels) is afhankelijk van 'de middelen' ICT en elektriciteit – die bij uitval wegvallen. In dit plan beschrijven we wat de gemeente organiseert om de impact van de uitval van ICT en/of elektriciteit zo veel mogelijk te verkleinen en de kritieke processen binnen de gemeente te continueren. Het gaat enerzijds om de noodvoorzieningen (ten behoeve van de ICT of elektriciteitsvoorziening). Anderzijds betreft het de inrichting van een crisisstructuur om snel en adequaat te kunnen reageren als de ICT en/of elektriciteit toch (deels) uitvalt.

⇨ Kort dit desgewenst in/ pas het desgewenst aan gegeven de gemeentelijke situatie.

1.3 Wat is de relatie met andere plannen

⇨ Som relevante (operationele) plannen op zoals een gemeentelijke crisisplan, een Fallback plan, afspraken met noodstroomleverancier enzovoorts.

2. Wat bedreigt ons

2.1 Wat kan er misgaan

Uitval van ICT en/of elektriciteit kan de gemeente op diverse manier raken. Voor de beeldvorming schetsen we een aantal voorbeelden.

- Bij uitval van elektriciteit, bijvoorbeeld door storing in een elektriciteitscentrale of problemen in elektriciteitskasten, valt geheel of gedeeltelijk ook ICT uit. Denk bijvoorbeeld aan de zendmasten in de regio, die zonder elektriciteit niet functioneren, met als gevolg dat mobiel communicatieverkeer (met mobieltjes, vaste telefoons) minder of niet mogelijk is. En zelfs als de zendmasten van noodstroom zijn voorzien, zal communicatieverkeer slechts ten dele én tijdelijk mogelijk zijn. Elektriciteitsuitval heeft ook een aantal praktische gevolgen (geen water meer uit de kraan, geen werkend toilet).
- Bij uitval van ICT kan het gaan om uitval van de hardware en/of van de software. Uitval van hardware is aan de orde als bijvoorbeeld het serverpark (waarop alle software draait) afbrandt of als het landelijk IP-verkeer wegvalt (waardoor er geen internet is en daarmee bijvoorbeeld geen LCMS). Uitval van software kan veroorzaakt worden door bijvoorbeeld een virus of cyberattack, waardoor applicaties in storing raken (delen of de gehele basisomgeving), met als gevolg dat bijvoorbeeld informatiesystemen niet meer operationeel zijn.

  Uitval van elektriciteit en hardware kan lokaal van aard zijn, maar uitval van software zal naar alle waarschijnlijkheid verschillende locaties van de gemeente raken. Grootschalige uitval van alleen de hardware is overigens niet waarschijnlijk.

De voorbeelden maken duidelijk dat uitval van ICT en/of elektriciteit op diverse manieren de gemeente kan raken, in het bijzonder de dienstverlening van de gemeente zelf.

⇨ Kort dit desgewenst in/ pas het desgewenst aan gegeven de gemeentelijke situatie.

2.2 Waar kan het misgaan

⇨ Specificeer de locaties van de gemeente die bij uitval van elektriciteit en of ICT niet mogen ‘omvallen’.
⇨ Benoem de situaties die tot opschaling noodzaken, waarbij een (al dan niet specifieke) crisisorganisatie wordt ingericht.
⇨ Benoem de situaties waarin verondersteld wordt dat de dienstverlening lokaal kan worden hersteld en geen crisisorganisatie wordt ingericht.

3. Wat doen we wel/niet

3.1 Wat zijn onze kritieke processen

De dienstverlening van de gemeente is omschreven in een aantal processen. Met het oog op de uitval van ICT en/of elektriciteit is binnen de processen een onderscheid te maken tussen kritieke en niet-kritieke processen. De kritieke processen van gemeente verdragen geen uitstel ("alles mag omvallen, behalve dat"). Niet-kritieke processen kunnen wel uitstel verdragen, denk bijvoorbeeld aan de salarisadministratie, het opstellen en actualiseren van beleid enzovoorts.

⇨ Benoem de kritieke processen die bij uitval van ICT en/of elektriciteit niet mogen 'omvallen' en waarvoor noodvoorzieningen nodig zijn (noodstroomvoorzieningen en noodvoorziening voor ICT, zoals back-upvoorzieningen voor servers en uitval-bestendige communicatieapparatuur).[8]
⇨ Een eerste voorbeeldlijst van kritieke processen

Aard proces	Proces	Toelichting
Bevolkingszorg processen	Informatievoorziening	Het voorzien van verbindingen en basisvoorzieningen om de benodigde/beschikbare informatie te kunnen verzenden/ontvangen/genereren (ten behoeve van besluitvormingsproces).
	Crisiscommunicatie	Het geven van pers – en publieksvoorlichting met als doel te voorzien in de maatschappelijke informatiebehoefte op basis van drie operationele doelen: informatie verstrekken; schade beperken en betekenis geven
	Publieke zorg	Het tijdelijk voorzien in de basisbehoeften van getroffenen (mensen en dieren) ten tijde van een (dreigende) ramp of crisis.

⇨ Een tweede voorbeeldlijst van kritieke processen, waarbij aansluiting gezocht is bij de naamgeving van KING GEMMA):

Aard proces	Bedrijfsproces	Specifiek onderdeel/product	Proceseigenaar
Primair	Beheren en onderhouden openbare	- Bedienen van bruggen	Afdelingshoofd Havens & Vaarwegen

[8] De gemeente is niet overal in de lead als het gaat om het treffen van noodvoorzieningen: bij sommige zaken is de gemeente afhankelijk van bijvoorbeeld landelijke organisaties die voor continuïteit van dienstverlening moeten zorgen.

	ruimte		
Primair	Beheren en onderhouden openbare ruimte	- Bedienen van sluizen en gemalen - Bedienen verkeerslichten	Afdelingshoofd Beheer
Primair	Verstrekken van publieke producten	- Verstrekken van reisdocumenten en rijbewijzen, uittreksels; - Huwelijksvoltrekkingen en registratie partnerschap	Afdelingshoofd KC Burgerzaken
		- …	
		- …	

⇨ Meld dat vooralsnog geen extra maatregelen of noodvoorzieningen getroffen worden om de uitvoering van niet-kritieke processen in geval van uitval van ICT en/of elektriciteit te continueren. Zie bijlage voor een overzicht van voorbeelden van 'minder kritieke processen'

3.2 Wat hebben we al geregeld als noodvoorzieningen voor ICT

De uitvoering van kritieke processen is afhankelijk van ICT software (applicaties / programma's) en hardware (systemen, computers, servers). De beschikbaarheid van de ICT bepaalt welke noodvoorzieningen nodig zijn om de kritieke processen draaiende te houden.

- **ICT – Hardware.** In hoeverre is ICT-hardware nog beschikbaar in geval van uitval van ICT en/of elektriciteit?

  ⇨ Breng in kaart welke hardware-onderdelen tegen uitval bestand zijn en dus beschikbaar zijn in geval van uitval van ICT en/of elektriciteit (dubbel uitgevoerd, op meerdere locaties beschikbaar, geen externe afhankelijkheden enzovoorts) met behulp van het excel- invulschema. Het schema begint bij de kritieke processen en helpt een inschatting te maken van de beschikbaarheid van hardware.

- **ICT – Software.** In hoeverre is ICT-software nog beschikbaar in geval van uitval van ICT en/of elektriciteit?

  ⇨ Breng in kaart welke software beschikbaar is en hoe zich dat verhoudt tot de kritieke processen met behulp van excel-invulschema. Het schema begint bij de kritieke processen en helpt een inschatting te maken van de beschikbaarheid van software.

3.3 Wat hebben we al geregeld als noodvoorziening voor elektriciteit

⇨ Benoem de noodstroomvoorzieningen / uitwijklocaties / andere oplossingen om de uitval van elektriciteit op te vangen. Het ligt voor de hand dat de locaties die genoemd zijn in 2.2 in deze paragraaf terug te zien zijn.

3.4 Welke kwetsbaarheden blijven

Ondanks de nood(stroom)voorzieningen blijft een ‘restrisico’ bestaan, met name rond de alarmering, opschaling en verlegde intake en de onderlinge informatievoorziening in het algemeen.

- **Alarmering.**

  ⇨ Licht toe hoe alarmering is geregeld bij uitval van ICT en/of elektriciteit en welke kwetsbaarheden eventueel blijven bestaan.

- **Opschaling en ondersteuning.**

  ⇨ Licht toe hoe opschaling is geregeld bij uitval van ICT en/of elektriciteit en welke kwetsbaarheden eventueel blijven bestaan.

- **Informatievoorziening onderling.**

  ⇨ Licht toe hoe informatievoorziening is geregeld bij uitval van ICT en/of elektriciteit en welke kwetsbaarheden eventueel blijven bestaan.

  Enkele algemene kwetsbaarheden met betrekking tot de onderlinge informatievoorziening:

  - Noodvoorziening communicatie (NCV), het vroegere nationaal noodnet. Locaties binnen de gemeente en een aantal partners van de gemeente zijn aangesloten op dit net. Degenen die niet op de lijst staan, zijn bij uitval van elektriciteit waarschijnlijk niet bereikbaar. Overigens is ook het NCV afhankelijk van spanningsvoorziening op betreffende locaties. Zonder elektriciteit bij ofwel de zendende ofwel de ontvangende partij zal NCV niet werken.
  - Mobiele telefoons. Via mobiele telefoons zijn mensen en kazernes bereikbaar zolang de zendmasten van telefoonproviders en de servers van telefoonproviders elektriciteit hebben. Zodra spanning op deze zaken wegvalt, zal geen communicatie met mobiele telefoons mogelijk zijn (en dus ook geen twitter, facebook, sms of whatsapp).

4. Hoe gaan we er mee om

4.1 Welke crisisorganisatie gebruiken we

⇨ Licht toe welke (al dan niet specifieke) crisisorganisatie wordt ingericht bij uitval van ICT en/of elektriciteit.

4.2 Welke taken worden uitgevoerd

⇨ Noem de functionarissen die verantwoordelijk zijn voor uitvoering van (één of meerdere) taken.

Expertise	Functionaris binnen de gemeente	Taken
Facilitair/ bedrijfsvoering	• …… • ……	• Leiding en coördinatie op het gebied van Facilitair/Bedrijfsvoering, ICT, Telecom, Gebouwbeheer, Beveiliging.
Gebouwbeheer Beveiliging	• …… • ……	• Het waar mogelijk verhelpen van de stroomstoring • Het op gang brengen van de noodvoorzieningen • Het verzorgen van de technische ondersteuning • Het verzorgen van ondersteuning ten aanzien van het gebouw (bijvoorbeeld luchtzuivering, klimaatbeheersing, drinkwatervoorziening, beveiligingssystemen) • Het organiseren van toegangsbeveiliging • Het onderhouden van contacten met de relevante externe partners.
ICT (inclusief verbindingen/ telecom/ communicatiemiddelen)	• …… • …… • ……	• Het opstarten van de noodvoorziening van ICT • Het beschikbaar maken van de minimale ICT behoeften • Het tot stand brengen en verzorgen van voldoende communicatiemiddelen. • Het organiseren van herstelwerkzaamheden op het gebied van telecom of andere verbindingen • Onderhouden van contacten met de relevante externe partners.

4.3 Wie zijn onze partners

⇨ Benoem de partners en meld of er reeds afspraken vastliggen over het alarmeren/ informeren van de partners en gemeente:

Partner	Reeds afspraken gemaakt?	Samenvatting van afspraken of verwijzing naar onderliggend (operationeel) document
Leverancier elektriciteitsvoorziening / netbeheerder	….	….
Leverancier noodstroom / brandstoffen	….	….
Beheerder communicatiesysteem	….	….
Beheerder externe servers	….	….
Outsourcepartner ICT	….	….
Hard- en software leverancier	….	….
Beheerder Nood Communicatie Voorziening (NCV)	….	….
Organisatie backup locatie	….	….
….	….	….
….	….	….

4.4 Wat gebeurt er stap voor stap (procesbeschrijving)

⇨ Beschrijf stap voor stap het proces dat zich op hoofdlijnen zal voltrekken bij uitval van ICT en/of elektriciteit.

	Locatie X
Uitval elektriciteit	Hoe wordt de uitval van elektriciteit opgemerkt?
	Wie krijgt melding en hoe van de uitval van elektriciteit?
Uitval ICT	Hoe wordt de ICT-uitval opgemerkt?
	Wie krijgt melding en hoe van ICT-uitval?
Beeldvorming	Hoe en door wie vindt beeldvorming van de lokale situatie plaats?
	Hoe en door wie wordt met netbeheerder / andere partners overlegd?
	Hoe wordt de afweging gemaakt ten aanzien van aard en omvang?
Alarmering	Hoe en door wie wordt gealarmeerd?

Opschaling	Hoe en door wie wordt opgeschaald?
Crisisbeheersing	Welke crisisorganisatie wordt ingericht?
	Wat is de werkwijze?
Herstel	Op welke manier wordt gewerkt aan herstel en normalisatie van de organisatie? Hoe worden de processen op gang gebracht die stil kwamen te liggen?

Berenschot

Bijlage met voorbeelden van 'minder kritieke processen'

Minder kritieke processen – die na circa 1 week wel kritisch worden vanwege mogelijke ontwrichting van situaties en/of systemen, financiële en/of juridische schade

Aard proces	Bedrijfsproces	Specifiek onderdeel/product	Proceseigenaar
Primair	Verstrekken van inkomens en maatschappelijke ondersteuning	- Verstrekken van uitkeringen - Schulddienstverlening, maatschappelijke ondersteuning	Sectorhoofd Werk&Inkomen
Primair	Aangiften burgerlijke stand	- Aangiften van geboorte, overlijden, adreswijziging, inschrijving, erkenning kind	Afdelingshoofd KC Burgerzaken
Primair	Vragen beantwoorden	- Behandelen WOB-verzoeken	Sectorhoofd Middelen
Primair	Afhandelen bezwaren	- Afhandelen bezwaarschriften, civiel/hoger beroep.ingebrekestelling,verzetsprocedure	Afdelingshoofd Juridische Zaken
Ondersteunend	Betalen en innen	- Beheren debiteuren, beheren crediteuren, aangeven belastingen	Afdelingshoofd Inkoop & Financiën
Ondersteunend	Faciliteren	- Termijngebonden post	Afdelingshoofd Facilitaire Zaken
		- verlenen vergunningen en ontheffingen	

Berenschot

Bijlage: Tool afhankelijkheden en beschikbaarheid ICT

Kritieke processen en de software (applicaties)								
Deze tabel maakt inzichtelijk wat de kritieke processen zijn en van welke applicaties (software) de kritieke processen afhankelijk zijn. Dat wil zeggen de applicaties die nodig zijn om een kritiek proces uit te voeren.								
Stap 1: Vul horizontaal de kritieke processen in (het 'stukje' dienstverlening dat niet mag omvallen). Hieronder zijn voorbeelden opgenomen (in rood).								
Stap 2: Vul verticaal de applicaties (de software) in die je nodig hebt om het kritieke proces uit te voeren. Hieronder zijn voorbeelden opgenomen (in rood) Benodigde applicaties zijn per proces gemarkeerd met een "x"								
	Kritieke processen							
SOFTWARE (applicaties)	**Proces A**	**Proces B**	**Proces C**	**Proces D**	**...**	**...**	**...**	**...**
GMS	x							
VNET 3.0	x	x	x					
vCenter			x	x				
CityGis								
Werkplek MK		x						
WAS			x					
NCV								
Mail Intern (veiligheidsregio/ MK)								
Mail Extern (veiligheidsregio / MK)			x					
LCMS 1.4								
LAN / WAN toegang								
WLAN toegang								
etc. etc.	x							

Berenschot

Software (applicaties) en Hardware (systemen)											
Deze tabel geeft aan welke hardware-onderdelen nodig zijn om de software (applicaties) te kunnen draaien én de beschikbaarheid van zowel software als hardware.											
Stap 3: Score verticaal de software (applicaties) op hun beschikbaarheid met een 1, 2 of 3 (zie legenda). Hieronder zijn voorbeelden opgenomen (in rood).											
Stap 4: Vul horizontaal de hardware in die je nodig hebt om de applicaties te kunnen draaien. Hieronder zijn voorbeelden opgenomen (in rood).											
Stap 5: Score de hardware (systemen) op hun beschikbaarheid met 1, 2 of 3 (zie legenda). Hieronder zijn voorbeelden opgenomen (in rood).											
Legenda	*nvt*	*Niet van toepassing (niet nodig voor de betreffende applicatie)*									
	1	1 = Niet bestand tegen uitval van onderdelen en uitval bij onderhoud: onderdelen zijn niet dubbel uitgevoerd en er zijn geen dubbele aanvoerlijnen, hardware zit niet op noodstroom (en dus niet beschikbaar bij uitval of onderhoud).									
	2	2 = Meer bestand tegen uitval van onderdelen. Dubbel uitgevoerde onderdelen en dubbele aanvoerlijnen. Niet altijd bestand tegen onderhoud (waarschijnlijk wel beschikbaar bij uitval stroom, niet beschikbaar bij onderhoud).									
	3	3 = Meest bestand tegen uitval van onderdelen. Alle onderdelen dubbel uitgevoerd, aanvoerlijnen dubbel en achter noodstroom. Ieder onderdeel is te onderhouden zonder uitval. Hardware kan verdeeld zijn over meerdere locaties (deze componenten zijn beschikbaar bij uitval).									
	Beschikbaarheid	**Beschikbaarheid HARDWARE (systemen)**									
	SOFTWARE (applicaties) ↓	DC-SRV01	DC-SRV02	SRV2	TSSRV01	TSSRV02	...	...	...	....	....
GMS	1	2	2		2					2	2
VNET 3.0	2	3		3	3	3				3	3
vCenter	3	3	3	3							
CityGis	2			3						nvt	
Werkplek MK	2			3				2			
WAS	2			3							
NCV	3			3							
Mail Intern (veiligheidsregio/ MK)	3			3			1		nvt		
Mail Extern (veiligheidsregio / MK)	3		3	nvt	3	3				3	
LCMS 1.4	2	3	1		3					3	3
LAN / WAN toegang	2			3		3				3	3
WLAN toegang	1	3	3	3	3						3
etc. etc.											

Beschikbaarheid van ICT bij uitval en de consequenties daarvan voor de kritieke processen

Deze tabel geeft de overall scores weer op basis van de inventarisaties (vorige twee tabbladen).

	Totaalscore van de beschikbaarheid van de ICT bij uitval	Beschikbaarheid van ICT ten opzichte van kritieke processen							
SOFTWARE (applicaties)		Proces A	Proces B	Proces C	Proces D	…	…	…	…
GMS	1	1	nvt	nvt	nvt	nvt	nvt	nvt	nvt
VNET 3.0	2	2	2	2	nvt	nvt	nvt	nvt	nvt
vCenter	3	nvt	nvt	3	3	nvt	nvt	nvt	nvt
CityGis	2	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt
Werkplek MK	2	nvt	2	nvt	nvt	nvt	nvt	nvt	nvt
WAS	2	nvt	nvt	2	nvt	nvt	nvt	nvt	nvt
NCV	3	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt
Mail Intern (veiligheidsregio/ MK)	1	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt
Mail Extern (veiligheidsregio / MK)	3	nvt	nvt	3	nvt	nvt	nvt	nvt	nvt
LCMS 1.4	1	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt
LAN / WAN toegang	2	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt
WLAN toegang	1	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt
etc. etc.	0		nvt	nvt	nvt	nvt	nvt	nvt	nvt
	0	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt
	0	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt
	0	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt
	0	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt
	0	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt
	0	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt
	0	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt
	0	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt
	0	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt
	0	nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt
Totaalscore beschikbaarheid ICT per kritiek proces		**1**	**2**	**2**	**3**				

Uitkomst van de inventarisatie

De ICT die nodig is bij	**Proces A**	is in geval van uitval	**niet beschikbaar**
De ICT die nodig is bij	**Proces B**	is in geval van uitval	**misschien wel/ misschien niet beschikbaar**
De ICT die nodig is bij	**Proces C**	is in geval van uitval	**misschien wel/ misschien niet beschikbaar**
De ICT die nodig is bij	**Proces D**	is in geval van uitval	**waarschijnlijk wel beschikbaar**
De ICT die nodig is bij	…	is in geval van uitval	
De ICT die nodig is bij	…	is in geval van uitval	
De ICT die nodig is bij	…	is in geval van uitval	
De ICT die nodig is bij	…	is in geval van uitval	