beek
uw gemeente.

GEMEENTEBLAD

Officiële uitgave van de gemeente Beek

Nr. 218870
19 mei
2023

Gemeente Beek Beleid bedrijfscontinuïteit 2023 – 2026

Inhoudsopgave

Besluit van het college van B&W van de gemeente Beek tot vaststelling van de beleidsregel voor de uitvoering van het bedrijfscontinuïteitsbeleid van de gemeente Beek

Het college van burgemeester en wethouders van de gemeente Beek:

gelezen het voorstel van het college van B&W van 25 april 2023 met nummer 23bbw00135.

overwegende dat,

het gewenst is om een beleidsregel vast te stellen omtrent de vaststelling van het bedrijfscontinuïteits-beleid omdat deze afspraken zijn nodig om bedrijfscontinuïteit structureel vorm te geven en te borgen binnen de organisatie;

gelet op de artikelen 4:81, eerste lid, 4:83 en 1:3, vierde lid, van de Algemene wet bestuursrecht en de wet beveiliging netwerk- en informatiesystemen;

besluit vast te stellen de volgende beleidsregel:

Beleid bedrijfscontinuïteit 2023 – 2026 van de gemeente Beek

Inwerkingtreding en citeertitel:
1. Deze beleidsregel treedt in werking, zie hoofdstuk 4;
2. Deze beleidsregel wordt aangehaald als: Beleid bedrijfscontinuïteit 2023 – 2026 van de gemeente Beek.

Aldus vastgesteld door het college van burgemeester en wethouders van de gemeente Beek in de vergadering van 25 april 2023.

1. INLEIDING

1.1. VOOR WIE

Dit beleid stelt algehele kaders vast waarbinnen de gemeente Beek haar bedrijfscontinuïteit regelt. Dit beleidsdocument geeft daarnaast richting voor nader vast te stellen continuïteits- en herstelplannen en bevat managementafspraken tussen het college, de directie, leidinggevenden van primaire (BMO, Ruimte en Samenleving) en ondersteunende bedrijfsprocessen (denk aan facilitair HRM, ICT en archief). Deze afspraken zijn nodig om bedrijfscontinuïteit structureel vorm te geven en te borgen in de gemeen-

telijke organisatie en daarbij hoort ook bewustwording, kennisoverdracht en een open en kritische bedrijfscultuur.

1.2. WAAROM AANDACHT VOOR BEDRIJFSCONTINUÏTEIT?

Als gemeente zijn we in de kern een informatiehuishouding en sterk afhankelijk van en kwetsbaar op onze gedigitaliseerde informatievoorziening die verbonden is met het internet. En een digitale overheid is vitaal voor maatschappelijke en economische activiteiten. Helaas is de digitale wereld waarin we ons begeven omgeven met diverse dreigingen die kunnen leiden tot gedeeltelijke of totale uitval van onze informatievoorziening en daaraan gerelateerde bedrijfsprocessen. Dat dreigingsbeeld wordt vooral veroorzaakt door cybercriminaliteit die steeds intensiever en geavanceerder wordt en inmiddels gegroeid is tot een professionele bedrijfstak met een verdienmodel voor criminelen. 'Visitekaartjes' hiervan vinden we volop terug in de vorm van malware, hacking of phisingmail. De meest herkenbare uiting hiervan is ransomware ofwel kwaadaardige gijzelsoftware waarbij aanvallers de gegevens van een organisatie versleutelen en betaling eisen om de toegang te herstellen, maar ook het digitaal stelen van gevoelige data valt hieronder. Cybercriminaliteit kan leiden tot forse financiële en reputatieschade en het vertrouwen van gebruikers ondermijnen en een organisatie helemaal platleggen voor lange duur. Paraatheid en doeltreffendheid op het gebied van cyberbeveiliging is daarom nu meer dan ooit van essentieel belang. Dat is ook op Europees niveau onderkend. Zo is zeer recentelijk de Europese richtlijn NIS2 (NIS2 staat voor Netwerk- en Informatiesystemen en is een Europese richtlijn die op 27 december 2022 is gepubliceerd en van toepassing is op diverse sectoren binnen de lidstaten die belangrijk zijn voor de economie en samenleving. Daaronder vallen in de nieuwe richtlijn ook overheidsdiensten. De richtlijn verplicht organisaties meer maatregelen te treffen om cyberrisico's te beheersen en stelt dat nationale autoriteiten strenger moeten handhaven op naleving van deze regels. Deze richtlijn moet nog worden omgezet naar Nederlands recht ter vervanging van de huidige Wet beveiliging netwerk- en informatiesystemen. Verwachting is dat de huidige wet in 2024 vervangen wordt in een nieuwe wet gebaseerd op NIS2.) gepubliceerd om weerstand te bieden aan elke gebeurtenis die de beschikbaarheid, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van diensten die door of via netwerk- en informatiesystemen worden aangeboden. Aandacht voor bedrijfscontinuïteit is daardoor vanuit de digitale wereld nadrukkelijk in beeld gekomen. Het is dus niet zozeer de vraag of een ramp of crisis zich zal voordoen maar wanneer en dat we daarop voorbereid zijn.
Daarnaast kunnen ook andere bedrijfsmiddelen uitvallen en leiden tot uitval van bedrijfsprocessen. Denk bijvoorbeeld aan stroomuitval, uitval personeel als gevolg van pandemie en huisvesting als gevolg van brand. Ook dit soort bedrijfsmiddelen valt onder het toepassingsgebied van dit beleid.
In het derde kwartaal 2022 is een rapport nulmeting bedrijfscontinuïteit uitgebracht. Uit dat rapport blijkt dat kennis over bedrijfscontinuïteit is versnipperd in de organisatie en niemand een volledig beeld heeft over dit onderwerp. Voorts geeft het rapport aan dat op het gebied van bedrijfscontinuïteit geen directe sturing en onderlinge afstemming is tussen de diverse disciplines en afdelingen. Dat beeld wordt onderkend door de directie en het bestuur.

1.3. DOEL

Doel van dit beleid is enerzijds gericht om meer draagvlak en bewustwording te creëren bij alle belanghebbenden voor bedrijfscontinuïteit, anderzijds om onze weerbaarheid te vergroten bij een ramp of calamiteit die een crisis tot gevolg kan hebben. Een crisis is in deze context een aanduiding van een situatie die levensbedreigend is voor een organisatie. In zo'n situatie stopt de normale gang van zaken en treedt een crisisaanpak in werking. Als niet goed gereageerd wordt op een crisis dan zijn de nadelige gevolgen niet te overzien in termen van financiële en reputatieschade. In de private sector zou dit doorgaans leiden tot faillissement.

1.4. MISSIE

- De gemeente Beek heeft een zorgplicht naar haar inwoners, organisaties en ketenpartners en daarbij behoort een betrouwbare dienstverlening.
- Inwoners, organisaties en ketenpartners van de gemeente Beek mogen erop kunnen vertrouwen dat de gemeentelijke dienstverlening die kritisch is onder alle omstandigheden betrouwbaar en beschikbaar is.
- Bedrijfscontinuïteit moet onderdeel worden van de bedrijfscultuur en geen opgelegde verplichting zijn vanuit de organisatie.
- Focus op bedrijfscontinuïteit zorgt voor meer weerbaarheid in tijden van onvoorziene, complexe en onstabiele omstandigheden. Die eigenschap maakt een organisatie ook onder normale omstandigheden sterker in termen van ethiek, overlevingsdrang en in geloofwaardigheid en vertrouwen om succesvol te zijn als organisatie.
- Het college stuurt daarom actief op bedrijfscontinuïteit gericht op de kritische dienstverlening door te voorzien in praktische waarborgen ter voorkoming van een ramp of calamiteit en ter voorbereiding op het bestrijden van een ramp of calamiteit om daaruit voortkomende schade zo beperkt mogelijk te houden.

De directie en het college van de gemeente Beek heeft zich daarom ten doel gesteld om bedrijfscontinuïteit structureel te borgen in de organisatie.

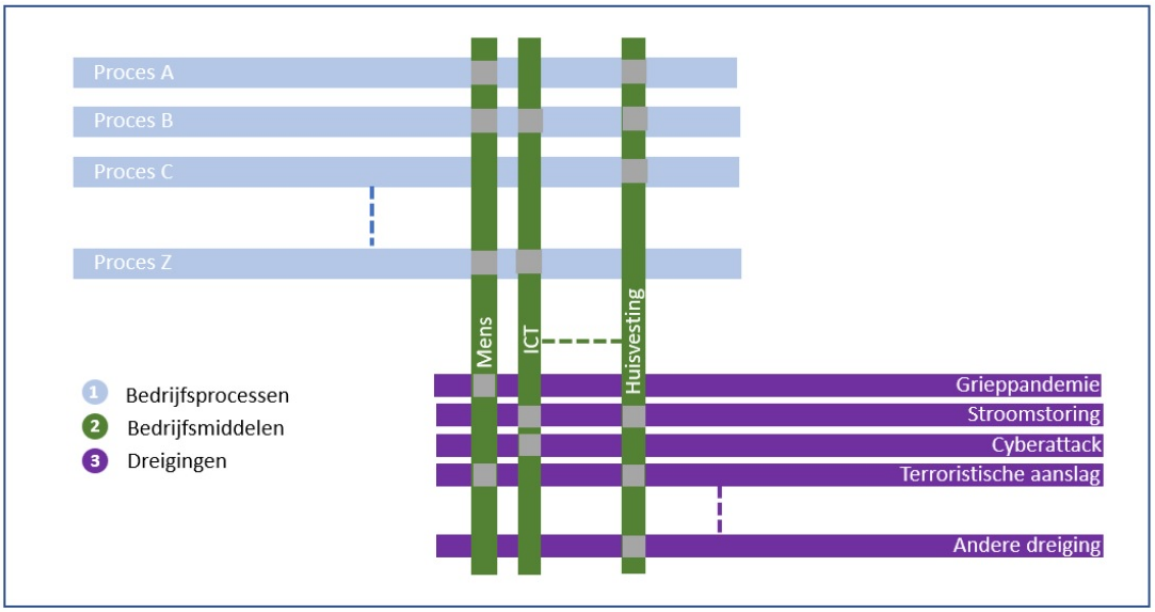
2. REIKWIJDTE

2.1. DEFINITIE BEDRIJFSCONTINUÏTEITSMANAGEMENT (BCM)

Bedrijfscontinuïteitsmanagement (BCM) is het proces dat gericht is op continu verbeteren van het vermogen van een organisatie om potentiële gevaren en de gevolgen van deze gevaren te identificeren, het hoofd te bieden en daarmee de continuïteit en het voortbestaan van onze organisatie te waarborgen onder alle omstandigheden.
Enerzijds gaat het om maatregelen ter voorkoming van een calamiteit of ramp die een crisis tot gevolg kan hebben, anderzijds om ons voor te bereiden om onder buitengewone onstabiele en complexe situaties te blijven presteren. Dat vereist andere competenties dan onder normale omstandigheden.
Belangrijk is te constateren dat BCM vooral gaat om een beheersingsproces dat de hele organisatie raakt en gericht is op continu verbeteren waar dat nodig is. Dat vereist een brede samenwerking en afstemming met alle belanghebbenden van bestuur, directie tot leidinggevenden van primaire bedrijfsprocessen en alle ondersteunende afdelingen die noodzakelijk zijn om bedrijfskritische bedrijfsprocessen operationeel te houden onder alle omstandigheden.

2.2. AFBAKENING

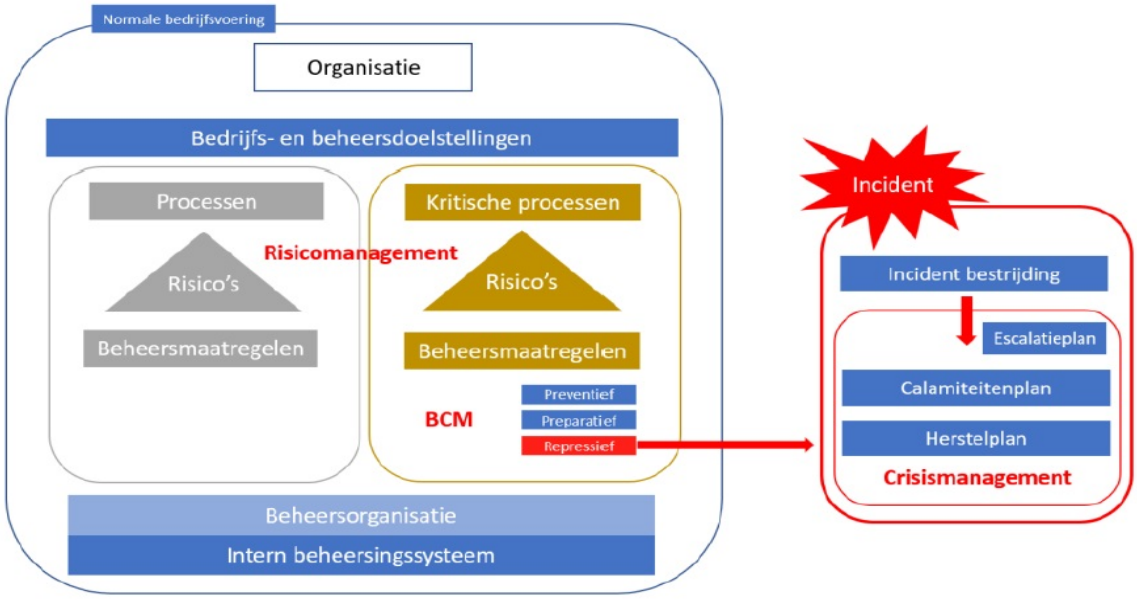
Bedrijfscontinuïteit richt zich op alle bedrijfskritische bedrijfsprocessen die onder alle omstandigheden beschikbaar moeten blijven. Niet-kritische bedrijfsprocessen vallen buiten dit kader. Welke bedrijfsprocessen onder de categorie kritisch of niet-kritisch vallen, wordt vastgelegd in een continuïteitsstrategie en formeel vastgesteld (zie ook $ 3.3).
Kritische bedrijfsprocessen vallen overigens niet rechtstreeks uit door een dreiging. Het zijn bedrijfsmiddelen zoals ICT, personeel en huisvesting die kwetsbaar zijn en kunnen uitvallen en als gevolg daarvan de bedrijfsprocessen die afhankelijk zijn van de beschikbaarheid van deze bedrijfsmiddelen.
Schematisch ziet deze samenhang er als volgt uit:



Het is daarom van belang dat van elk kritisch bedrijfsproces inzicht is in de mate van afhankelijkheid van bedrijfsmiddelen. Zo kan een dreiging impact hebben op het middel ICT waardoor ICT-gerelateerde bedrijfsprocessen kunnen uitvallen. Hetzelfde geldt voor langdurige uitval van huisvesting en personeel.

2.3. POSITIONERING BCM IN DE BEDRIJFSVOERING

BCM maakt standaard onderdeel uit van de normale bedrijfsvoering van de gemeente, alleen is deze gericht op de kritische bedrijfsprocessen. Dat onderscheid tussen kritische en niet-kritische bedrijfsprocessen wordt bepaald door de inzet van risicomanagement zoals hieronder visueel is weergegeven.



De relatie tussen risicomanagement, BCM en crisismanagement is in bovenstaand overzicht zichtbaar gemaakt. Risicomanagement is geschikt om onder normale omstandigheden te wijzen op mogelijke dreigingen die de bedrijfscontinuïteit in gevaar kan brengen met als mitigerende maatregel daarvoor BCM te implementeren dat zich ook richt op de inrichting van crisismanagement. In die zin is BCM een op maat gemaakte interne 'verzekeringspolis' die de schade als gevolg van een ramp of calamiteit zo beperkt mogelijk houdt en niet kan worden afgedekt door een normale verzekering.

2.4. RAAKVLAKKEN MET ANDERE THEMA'S

Bedrijfscontinuïteit is nauw verweven met informatie- en cyberbeveiliging (Baseline Informatiebeveiliging Overheid, NIS2) als het gaat om de beschikbaarheid, integriteit en vertrouwelijkheid van digitale informatie. Er zijn dan ook concrete raakvlakken gericht op het voorkomen van beveiligingsincidenten die kunnen escaleren naar een ramp of calamiteit. Maar ook het borgen van de beveiliging van informatie is essentieel bij een calamiteit of ramp waarbij geen sprake meer is van een normale bedrijfsvoering. Dan is vertrouwelijke informatie doorgaans kwetsbaar. Bedrijfscontinuïteit raakt het weerstandsvermogen en liquiditeiten van de gemeente om een calamiteit of ramp financieel op te kunnen vangen. Bedenk dat een calamiteit of ramp financieel al gauw in de miljoenen kan lopen. Voorts is er een raakvlak met BHV'ers als het gaat om de veiligheid van personeel en bezoekers bij bijvoorbeeld een ontruiming en met archiefbeheer (beschermen fysiek en digitaal archief) voortkomend uit de Archiefwet.

2.5. UITGANGSPUNTEN

De gemeente Beek hanteert in het kader van bedrijfscontinuïteit de volgende uitgangspunten:

2.5.1. Governance

1. Het college is bestuurlijk eindverantwoordelijk voor de bedrijfscontinuïteit van de dienstverlening van de gemeente.
2. De directie is ambtelijk verantwoordelijk voor de inrichting en effectieve werking van de beheerorganisatie rond bedrijfscontinuïteit en legt periodiek op een aantoonbare wijze verantwoording af aan het college.
3. De directie zorgt dat voor elk kritisch bedrijfsproces een proceseigenaar is benoemd. Een proceseigenaar is een (lijn/staf)manager of leidinggevende.
4. Een proceseigenaar is verantwoordelijk voor de continuïteit van zijn bedrijfsproces inclusief de daaraan gerelateerde informatiesystemen.
5. De directie heeft een coördinator bedrijfscontinuïteit (BC) benoemd die de organisatie ondersteunt met het realiseren van haar doelstellingen op het gebied van bedrijfscontinuïteit, onderhoudt de contacten met alle belanghebbenden en zorgt voor onderlinge afstemming van uit te voeren taken.

2.5.2. Beheerorganisatie

1. De directie stelt toereikende middelen beschikbaar voor het structureel borgen van bedrijfscontinuïteit in de organisatie.
2. De directie zorgt voor een managementsysteem voor bedrijfscontinuïteit (BCMS) dat gericht is op continu verbeteren en het jaarlijks verantwoordingsproces voor de BCM ondersteunt.
3. De coördinator BC onderhoudt het BCMS en is belast met het verstrekken van periodieke managementrapportages aan alle belanghebbenden voortkomend uit het BCMS.

4. De directie bevordert de integratie van en onderlinge afstemming tussen de verschillende beheeractiviteiten verdeeld over de organisatie die nodig is voor het borgen van bedrijfscontinuïteit.
5. De directie stelt een continuïteitsstrategie (plan op hoofdlijnen om uit een crisissituatie te raken) vast als basis voor het nader uitwerken van de vereiste deelplannen gericht op bedrijfscontinuïteit.
6. De directie zorgt voor continue aandacht voor bewustwording onder het personeel over het belang en de noodzaak van bedrijfscontinuïteit en wat in dat kader van het personeel verwacht wordt.
7. De directie zorgt dat het beleidsdocument bedrijfscontinuïteit om de 3 jaar wordt herijkt of eerder als significante veranderingen zich voordoen.
8. De coördinator BC bewaakt de actualiteit en uitvoerbaarheid van alle opgeleverde en vereiste continuïteits- en herstelplannen.

2.5.3. Continuïteits- en herstelplannen

1. Een proceseigenaar stelt voor zijn bedrijfsproces op basis van een expliciete risicoafweging de maximale uitvalsduur (de termijn waarbinnen het bedrijfsproces na het optreden van een calamiteit weer operationeel dient te zijn) en gegevensverlies(de termijn waarbinnen het bedrijfsproces na het optreden van een calamiteit weer operationeel dient te zijn) vast rekening houdend met vigerende wet- en regelgeving.
2. Een proceseigenaar geeft voor zijn kritisch bedrijfsproces inzicht in de bedrijfsmiddelen die nodig zijn voor een normale bedrijfsvoering en in de interne en externe afhankelijkheden (denk aan ketenpartners).
3. De directie draagt zorg voor een crisisbeheerplan inclusief crisiscommunicatieplan dat zich met name richt op de bestuurlijke, organisatorische en coördinerende aspecten van crisismanagement.
4. Proceseigenaren dragen zorg voor de beschikbaarheid en veiligheid van hun kritische bedrijfsprocessen onder alle omstandigheden en stemmen hun eisen af op de daarvoor benodigde bedrijfsmiddelen.
5. Facilitair beheer draagt zorg voor de beschikbaarheid en veiligheid van de huisvesting, nutsvoorzieningen en telefonie die nodig zijn voor het beschikbaar houden van de kritische bedrijfsprocessen die daarvan afhankelijk zijn onder alle omstandigheden.
6. ICT-beheer draagt zorg voor de beschikbaarheid en veiligheid van de digitale netwerk- en informatiesystemen die nodig zijn voor het beschikbaar houden van de kritische bedrijfsprocessen die daarvan afhankelijk zijn, rekening houdend met de daarvoor vereiste hersteltijden.
7. Archiefbeheer draagt zorg voor het beschikbaar houden van het fysiek en digitaal archief onder alle omstandigheden.
8. De directie zorgt dat is voorzien in periodieke beoordeling van de kwaliteit en onderlinge afstemming / aansluiting van opgeleverde continuïteits- en herstelplannen waarbij rekening wordt gehouden met dezelfde spreektaal en terminologie om misverstanden in de communicatie zoveel mogelijk te voorkomen.

2.5.4. Periodieke beoordeling en testen

1. Alle continuïteits- en herstelplannen worden minimaal één maal per jaar beoordeeld op volledigheid, juistheid en actualiteit.
2. De directie zorgt ervoor dat structureel voldoende middelen beschikbaar zijn voor het periodiek oefenen en testen van continuïteits- en herstelplannen.
3. De directie zorgt ervoor dat de opgeleverde en vastgestelde continuïteits- en herstelplannen periodiek worden getest op uitvoerbaarheid binnen de gestelde uitvaltermijnen en waar nodig worden aangepast als niet voldaan wordt aan de vereiste hersteltijden.

2.6. WIE ZIJN INTERN BELANGHEBBENDEN?

Zoals al is aangegeven raakt BCM de hele organisatie. Naast het college en de directie gaat het ook om de proceseigenaren in de 1e lijn, en leidinggevenden van facilitair beheer, ICT-beheer, contractenbeheer, archiefbeheer, juridische zaken, HRM en communicatie. Daarnaast zijn de concerncontroller, CISO, privacyfunctionaris en de coördinator bedrijfscontinuïteit (BC) belangrijke spelers in het kader van BCM als het gaat om coördinatie van beheertaken en het delen van informatie over BCM.

3. MANAGEMENTSYSTEEM VOOR BEDRIJFSCONTINUÏTEIT (BCMS)

Het doel van een BCMS is gericht op het voorbereiden, voorzien in en onderhouden van effectieve beheersmaatregelen en bekwaamheden voor het managen van het algehele vermogen van de gemeentelijke organisatie om de kritische bedrijfsactiviteiten tijdens verstoringen voort te zetten. Het BCMS behoort te worden ingericht, onderhouden en te voorzien in managementrapportages om tijdig te kunnen sturen en op een gecontroleerde wijze verantwoording af te leggen. Het BCMS is voorzien van een samenhangende set van toetsbare normen waaraan moet worden voldaan volgens het principe ‘pas toe of leg uit’.

Belangrijk is dat het BCMS bijdraagt tot
- het structureren en standaardiseren van het beheersingsproces rondom bedrijfscontinuïteit;
- bevorderen van onderlinge samenwerking tussen verschillende afdelingen en disciplines;
- creëren van een stabiele beheersorganisatie rondom bedrijfscontinuïteit;
- makkelijker uitwisselen van informatie aan belanghebbenden.

Het BCMS ondersteunt en draagt bij tot een betere grip op bedrijfscontinuïteit voor alle relevante organisatieonderdelen. Daarnaast versterkt het BCMS de collectieve bewustwording en onderlinge samenwerking met alle verschillende disciplines en afdelingen die een bijdrage leveren aan bedrijfscontinuïteit.

3.1. BEHEERSINGSPROCES

Het BCMS is ingebed in een jaarlijks doorlopende plan-do-check-act cyclus (PDCA-cyclus) gericht op continu verbeteren met als uitgangspunt dat dit beheersingsproces de 'inhoud' borgt. Uiteraard heeft het vormen van dit proces tijd nodig, maar als dat eenmaal staat dan komt de inhoud als ware naar je toe. Er wordt dan volgens gangbare beheersingsprincipes (waaronder het drielijnenmodel) op een constructieve wijze gebouwd aan het borgen van bedrijfscontinuïteit. Geen los zand meer, maar cement om muren te bouwen volgens een bouwplan in het tempo dat past bij de ambitie van de organisatie. Belangrijke aspecten hierbij zijn samenwerken, afstemmen, structureren en standaardiseren.

3.2. RISICOGEBASEERDE AANPAK

Het opzetten en implementeren van een BCMS geschiedt vanuit een risicogebaseerde benadering. Dat is een samenspel van verantwoordelijkheden en bevoegdheden volgens het drielijnenmodel verdeeld over verschillende afdelingen en disciplines waarbij bewuste en onderbouwde keuzes worden gemaakt om bepaalde risico's als zodanig te accepteren. Dat uit zich onder andere door het bepalen welke bedrijfsprocessen wel of niet als bedrijfskritisch te waarmerken zijn en onder het BCMS vallen. Bij deze afweging houden we rekening met eisen omtrent de beschikbaarheid van onze dienstverlening voortvloeiend uit wet- en regelgeving zoals de Basisregistratie Personen (BRP) en paspoorten en Nederlandse identiteitskaarten (PNIK). BCMS richt zich nadrukkelijk op de kritische bedrijfsprocessen en daarbij accepteren we dat niet-kritische bedrijfsprocessen bij een calamiteit of crisis mogen uitvallen.

Vanuit het dreigingsbeeld richt de risicogebaseerde aanpak zich vooral op de meest voorkomende dreigingen met de grootste impact zoals cyberaanvallen, stroomuitval en brand. Het is namelijk ondoenlijk en onpraktisch om alle dreigingen in beeld te brengen, te relateren aan bedrijfsmiddelen en bedrijfsprocessen en daarvoor continuïteitsscenario's te bedenken. In die zin is er altijd sprake van een voor de organisatie acceptabel restrisico.

3.3. CONTINUÏTEITSSTRATEGIE

Het hoofddoel van een continuïteitsstrategie is om te verduidelijken hoe de gemeente de bedrijfscontinuïteit van haar kritische bedrijfsprocessen zal waarborgen. Een continuïteitsstrategie is een resultante van een risicogebaseerde aanpak en draagt bij tot inzicht in:
- bedrijfsprocessen die als kritisch zijn gewaarmerkt met vermelding van maximale uitvalsduur en maximale gegevensverlies;
- de prioriteitsvolgorde van kritische bedrijfsprocessen die gecontinueerd dient te worden;
- bedrijfsprocessen die als niet-kritisch zijn gewaarmerkt;
- proceseigenaren van kritische bedrijfsprocessen;
- afhankelijkheden van kritische bedrijfsprocessen in relatie tot de bedrijfsmiddelen als ICT, stroomvoorziening, personeel, huisvesting en eventueel derde partijen;
- de vereiste continuïteits- en herstelplannen.

Een continuïteitsstrategie is een formeel en vertrouwelijk document en behoort periodiek te worden geëvalueerd en ligt aan de basis voor het nader uitwerken van continuïteits- en herstelplannen.

4. FORMELE VASTSTELLING

Dit beleid bedrijfscontinuiteit 2023-2026 wordt door het college van burgemeesters en wethouders vastgesteld voor een periode van drie jaar. Het beleid wordt periodiek geëvalueerd en indien nodig herzien. Dit beleid treedt in werking een dag na bekendmaking.