Gemeente Amsterdam

Auditrapport

Business Continuity Management (BCM)

Opdrachtgever: Concerncontroller

Auteur: Interne Audit & Beleidsonderzoek

Ontvanger rapportage: Directie Digitale Strategie & Informatie

14-08-23 (Definitieve versie 1.0)

1 Inleiding

Op basis van het auditjaarplan 2023 heeft de afdeling Interne Audit & Beleidsonderzoek een audit uitgevoerd naar het proces Business Continuity Management (Hierna: BCM) binnen de gemeente.

1.1 Aanleiding

BCM gaat over het beheersen van de bedrijfscontinuïteit. BCM is een beheerproces waarbij de gemeente maatregelen treft om de continuïteit van de meest kritische bedrijfsprocessen te garanderen. Dit is van belang om de dienstverlening richting de Amsterdammers te kunnen blijven continueren. Binnen de gemeente gaat het dan bijvoorbeeld om processen als beheer van de basisregistratie personen (BRP), het verstrekken van identiteitsdocumenten of het toekennen en betalen van uitkeringen. Mochten deze kritische bedrijfsprocessen verstoord worden, dan heeft dit direct negatieve gevolgen voor de Amsterdammer. Zo kan het niet tijdig verstrekken van uitkeringen Amsterdammers direct financieel in de problemen brengen. Op de lange termijn kan het niet op orde hebben van BCM binnen de gemeente ook het vertrouwen van de Amsterdammer in de gemeente schaden. Zo moeten we goed voorbereid zijn op incidenten zoals brand, overstromingen en stroomuitval zodat we een betrouwbare dienstverlening kunnen blijven garanderen. Een betrouwbare gemeente draagt daarin bij aan vertrouwen door de Amsterdammer.

Vanuit de directie Digitale Strategie en Informatie (DS&I) is de externe partij Verdonck, Klooster & Associates (VKA) gevraagd om een aanpak voor BCM uit te werken en hier een startnotitie voor te schrijven. Het doel van de startnotitie is de gemeente Amsterdam in staat te stellen om met voldoende draagvlak bij alle relevante stakeholders en met een gestructureerde aanpak een BCM-project op te starten (Zie VKA-offerte startnotitie BCM).

Vanuit DS&I is IA&BO gevraagd om na te gaan of de geschetste aanpak in de startnotitie door VKA past binnen de context van de gemeente Amsterdam.

1.2 Doelstelling en Centrale Vraag

De doelstelling van deze audit is het bieden van aanvullend inzicht op de VKA-startnotitie BCM. Dit doen we door onderzoek te doen naar het voorgestelde implementatietraject van BCM binnen de gemeente, de voorgestelde inrichting van de governance omtrent BCM en de bijbehorende uitgangspunten. De audit resulteert in aandachtspunten die meegenomen kunnen worden in de verdere inrichting van BCM binnen de gemeente.

De centrale vraag van de audit luidt: ‘’Welke aandachtspunten zijn er naar aanleiding van de startnotitie BCM te geven voor de inrichting en invoering van BCM binnen de gemeente, gegeven de Amsterdamse gemeentelijke context?’’.

Onze centrale vraag valt uiteen in onderstaande deelvragen:

1. Wat is de huidige status van de implementatie van BCM binnen de gemeente?
2. Welke aandachtspunten zijn er met betrekking tot het creëren van bewustwording en draagvlak bij de business?
3. Welke aandachtspunten zijn er met betrekking tot de voorgestelde inrichting van de governance van BCM in de gemeente?
4. Welke aandachtspunten zijn er voor een Lean implementatie van BCM binnen de gemeente?

1.3 Leeswijzer

In hoofdstuk 2 hebben wij de samenvatting en conclusies opgenomen. In hoofdstuk 3 beantwoorden we deelvraag 1; dit betreft de schets van de huidige status van de implementatie van BCM binnen de gemeente. In hoofdstuk 4 beantwoorden we deelvraag 2 t/m 4. Hierin zijn de aandachtspunten opgenomen die wij zien ten aanzien van de startnotitie. In bijlage 1 hebben we onze werkzaamheden vermeld en is aandacht voor de gemaakte afspraken met betrekking tot deze audit. Voor deze afspraken verwijzen wij ook naar onze auditbrief. Tot slot hebben we in bijlage 2 enkele standaarden vanuit ISO-22301 opgenomen, waarvan wij denken dat deze ondersteunen bij de nadere uitwerking van BCM.

1.4 Dankwoord

Wij bedanken de medewerkers die bij dit onderzoek betrokken zijn geweest voor de open en constructieve samenwerking bij het verrichten van onze werkzaamheden. Tot het verstrekken van nadere toelichting zijn wij uiteraard bereid.

2 Samenvatting en conclusies

Wij hebben onderzocht welke aandachtspunten er zijn inzake de startnotitie BCM met betrekking tot de inrichting en invoering van BCM binnen de Gemeente Amsterdam.

2.1 Conclusie

De startnotitie BCM moet de gemeente in staat stellen om met voldoende draagvlak bij alle relevante stakeholders en met een gestructureerde aanpak een BCM-project op te starten. De startnotitie slaagt hier wat ons betreft ten dele in. Zo vinden wij het positief dat er: aandacht is voor bewustwording en draagvlak, een aanzet gedaan wordt voor de uitwerking van de governance omtrent BCM en dat er aandacht is voor de aansluiting op de bestaande crisismanagementorganisatie. Wel zien we op onderdelen ruimte voor verbetering. We constateren dat:

- De gemeente al langere tijd het voornemen heeft om een BCM-strategie te implementeren. De voortgang hierop is de afgelopen jaren beperkt;
- Aanvullende aandacht voor bewustwording en draagvlak omtrent BCM gewenst is;
- Verantwoordelijkheden voor BCM niet overal expliciet belegd zijn. Daarnaast is de inrichting van de governance voor BCM in crisissituaties niet uitgewerkt;
- Het BCM-implementatietraject efficiënter kan;
- Het onduidelijk is of crisismanagement breed en afdoende is ingericht in de gemeente. Wanneer dit niet afdoende is ingericht, heeft dit gevolgen voor de doorlooptijd en aanpak (routekaart) van het BCM-implementatietraject.

2.2 Aanbevelingen

De belangrijkste aandachtspunten die wij zien met betrekking tot de startnotitie zijn:

Bewustwording en draagvlak

- Betrek directies, ketenpartners en leveranciers (stakeholders) nauw in het vervolg van het BCM-implementatietraject. Maak daarbij duidelijk wat het doel en belang van BCM is, wat het doel van de voorgestelde aanpak is en wat verwacht wordt van de stakeholders. Laat hierbij ook ruimte voor stakeholders voor eigen inbreng.
- We bevelen aan om bij de start van het implementatietraject BCM het GMT hier op een formele wijze over te laten communiceren en het belang van BCM verder uit te dragen. Dit benadrukt het belang dat het GMT aan BCM hecht en is ook meteen één van de belangrijkste randvoorwaarden voor een succesvolle implementatie (Informatiebeveiligingsdienst VNG: BCM agenderen binnen de organisatie).

Governance

- Besteedt expliciet aandacht aan het eigenaarschap voor BCM bij ketenprocessen en laat dit door het GMT vaststellen.
- Werk op korte termijn uit hoe de governance van BCM in een crisissituatie eruit zou moeten zien en laat dit vaststellen door het GMT.

Aanpak implementatietraject

- Wij bevelen aan om nadat de workshops op GMT-niveau, clusterniveau en bij de kritieke directies hebben plaatsgevonden, niet direct de workshops te organiseren bij alle directies, maar juist eerst te focussen op de processen die door het GMT al als cruciaal zijn bestempeld met betrekking tot continuïteit (kernprocessen). Op basis

van de uitkomsten van een risicoanalyse van de overige processen kan vervolgens besloten worden of het noodzakelijk is om ook workshops te organiseren bij overige directies of dat risico's bewust geaccepteerd worden. Hiermee kan een efficiencyslag worden gerealiseerd.

Uitgangspunten (crisismanagement)

- Wij bevelen aan om in kaart te brengen in hoeverre crisismanagement breed is ingericht in de organisatie en hiernaar te verwijzen in verdere communicatie. Mocht crisismanagement niet breed zijn ingericht binnen de gemeente, dan is het effectiever om eerst generieke maatregelen te nemen, voordat er naar de bedrijfsprocessen wordt gekeken.

Vertrouwen

We zijn positief over de voorgestelde lean aanpak van BCM binnen de gemeente in plaats van een traditionele implementatie van BCM. Het uitgangspunt hierbij is eerst oefenen en het opstellen van plannen komt later. Dit vereist vertrouwen. Vertrouwen dat we ook zonder gedetailleerde plannen als gemeente voldoende weerbaar zijn tegen crisissen en continuïteitsverstoringen. Incidenten uit het verleden zoals het Log4j-incident hebben aangetoond dat we als gemeente wendbaar zijn. Maar ook vertrouwen in elkaar; vertrouwen in onze (directe) collega's. Samenwerking en communicatie worden hierbij in de Lean BCM-aanpak als essentiële competenties gezien. Wij vertrouwen in principe in de opzet van de geschetste aanpak. Wel benoemen we in de rapportage aandachtspunten ter verbetering en nadere uitwerking.

In de rapportage geven we aan welke prioriteit we aan de bevindingen toekennen. Bevindingen met prioriteit 1 worden in de voortgangsrapportages aan het GMT opgenomen. Prioriteit 2 bevindingen worden alleen aan het GMT gemeld als er geen opvolging aan wordt gegeven en prioriteit 3 bevindingen (opvolging niet noodzakelijk) worden enkel aan de directie en het management gerapporteerd. Standaardrisico`s, beheersmaatregelen, bevindingen en aanbevelingen worden opgenomen in het gemeentebrede risicomanagementsysteem FullyInControl.

Bevindingen	Beoordeling
Aanvullende aandacht voor bewustwording en draagvlak omtrent BCM is gewenst.	
Het breed beleggen van verantwoordelijk-heden voor BCM en het uitwerken van de inrichting van de governance voor BCM in crisissituaties ontbreekt.	
Het BCM-implementatietraject kan efficiënter.	
Het is onduidelijk of crisismanagement breed en afdoende is ingericht in de gemeente. Dit heeft mogelijk gevolgen voor de doorlooptijd van het BCM-implementatietraject.	

Figuur 1:
Prioriteit 1: Zeer belangrijk, grote impact, urgent, opvolging direct vereist
Prioriteit 2: Belangrijk, gemiddelde impact, minder urgent, opvolging nodig
Prioriteit 3: Aandacht nodig, beperkte impact, niet urgent, opvolging niet noodzakelijk.

2.3 Managementreactie Digitale Strategie en Informatie

Directie Digitale Strategie en Informatie heeft op 9-8-2023 een managementreactie gegeven op dit rapport. Samengevat heeft directie als reactie aangegeven:

Directie Digitale Strategie en Informatie stemt in met de inhoud van het rapport en de daarin gedane aanbevelingen.

De aanbevelingen die gericht zijn op de coördinatie door het GMT, creëren van een breed draagvlak in de gemeentelijke organisatie en de samenhang met crisismanagement zullen worden verwerkt in de aanpak.

De aanbeveling om eerst te focussen op de gemeentelijke kernprocessen is een waardevolle toevoeging en helpt om keuzes te maken en prioriteiten te stellen.

3 Werkzaamheden en bevindingen

In dit hoofdstuk schetsen we kort de huidige status van de gemeentebrede implementatie van BCM. Dit vormt het startpunt voor het BCM-implementatietraject zoals voorgesteld in de startnotitie van VKA.

BCM is momenteel nog onvoldoende structureel geborgd in de organisatie

De gemeente heeft al langere tijd het voornemen om een BCM-strategie te implementeren. De startnotitie biedt hier een goed uitgangspunt voor. Tegelijkertijd is de voortgang op de implementatie van BCM binnen de gemeente de afgelopen jaren beperkt. Sturing op de voortgang van het BCM-implementatietraject is een aandachtspunt.

Bij voorgaande crisissen heeft de gemeente Amsterdam laten zien dat het in staat is om snel en flexibel in te spelen op crisissen. Een voorbeeld hiervan is het log4j-incident dat wereldwijd gezorgd heeft voor bedreiging van de veiligheid en continuïteit bij organisaties. In januari 2023 is uit een evaluatieverslag van dit incident naar voren gekomen dat in grote lijnen met succes op dit incident is ingespeeld. Ook leeft bij directies die wij gesproken hebben in het kader van dit onderzoek het gevoel dat adequaat is ingespeeld op de coronacrisis. Het is goed dat we als gemeente in staat blijken om flexibel en wendbaar te opereren wanneer dat nodig is.

Ondanks deze positieve signalen zien we ruimte voor verbetering. Zo ontbreekt het momenteel aan regie, beleid en aansturing op het gebied van BCM (ACAM-accountantsverslag 2022). BCM is op dit moment nog niet structureel geborgd in de organisatie. Dit maakt de gemeente kwetsbaar. Zo maakt het ontbreken van BCM-beleid het onduidelijk binnen welke kaders geopereerd dient te worden. De gemeente heeft hierbij al langere tijd het voornemen om een BCM-strategie te implementeren. De voortgang met betrekking tot de implementatie van BCM is tot nog toe echter beperkt; er moet nog steeds veel gebeuren. Er is nog geen Business Continuity Officer aangesteld (BCO'er), het ontbreekt bij veel directies aan Business continuity plannen en de governance voor BCM is nog niet ingericht. Ook hebben in 2022 geen oefeningen plaatsgevonden op het gebied van BCM. Wel is aangegeven dat in 2023 een aantal crisisoefeningen staan gepland, specifiek gericht op cyberaanvallen en hacks (ACAM-accountantsverslag 2022). Ook zullen er op diverse niveaus workshops georganiseerd worden waarin geoefend zal worden met verschillende (ramp)scenario's. De oefeningen en workshops zullen bijdragen aan de weerbaarheid van de gemeente tegen continuïteitsverstoringen.

De startnotitie BCM biedt een aanzet voor de implementatie van BCM binnen de gemeente. De startnotitie schetst randvoorwaarden voor een geslaagde invulling van BCM binnen de gemeente. De exacte invulling van BCM moet nog wel nader uitgewerkt worden. Denk bijvoorbeeld aan de invulling van de workshops, de inhoud van de business continuity plannen en beleid, hoe ketenpartners en leveranciers betrokken worden en de governance voor tijdens crisissituaties.

4 Aandachtspunten BCM-startnotitie

In dit hoofdstuk behandelen we onze aandachtspunten naar aanleiding van de BCM-startnotitie. Deze aandachtspunten verdelen we onder in de volgende onderwerpen: 4.1 bewustwording en draagvlak (deelvraag 2), 4.2 inrichting van de governance BCM (deelvraag 3), 4.3 het BCM-implementatietraject (deelvraag 4) en 4.4 crisismanagement.

4.1 Aanvullende aandacht voor bewustwording en draagvlak omtrent BCM is gewenst.

Voor het opstellen van de startnotitie BCM is input opgehaald bij verschillende directies. Wij constateren dat niet alle directies waarvoor in de geschetste opzet van BCM een cruciale rol weggelegd is, meegenomen zijn in het leveren van input op de startnotitie. Daarnaast zijn niet alle directies op de hoogte van het belang van alle onderdelen van BCM en wordt uit de startnotitie niet duidelijk hoe leveranciers en ketenpartners in het implementatietraject betrokken zullen worden.

Aanbeveling

Naast de aandachtspunten die wij in deze rapportage benoemen voor de implementatie van BCM binnen de Amsterdamse context, bevelen wij ook aan om het gesprek aan te gaan met andere (G4-) gemeenten. Er kan lering getrokken worden uit hoe zij BCM geïmplementeerd hebben in de gemeente met betrekking tot de nadere uitwerking en invulling van BCM.

In de startnotitie is aandacht voor bewustwording en draagvlak van BCM. In de startnotitie staat als uitgangspunt/wens voor de implementatie van BCM binnen Amsterdam:

"Bewustwording op (cluster-) directieniveau waarom BCM belangrijk is, is een randvoorwaarde voor succes."

Bevindingen

1. Uit de interviews blijkt dat bewustzijn bij de directies waar de interviews zijn afgenomen (zie hiervoor bijlage 1) over het belang van zekere onderdelen van BCM ontbreekt. Dit heeft zowel betrekking op wat het nut en de noodzaak van BCM op directieniveau is, maar ook op deelaspecten. Zo wordt in de interviews door directeuren aan ons gevraagd wat het doel is van (gedetailleerde) Business continuity plannen. Duidelijk is dat de noodzaak van BCM beperkt leeft. Hierin ligt een belangrijke communicatieve rol weggelegd voor het team kwartiermakers BCM in het vervolg van het traject.

2. Een aanzienlijk aantal directies dat in de geschetste opzet van BCM binnen de gemeente straks een cruciale rol zal gaan spelen, is niet meegenomen in het meedenken over de startnotitie. We vinden dit opvallend, omdat vanuit het I-domein het verbredingsvraagstuk omtrent BCM heel erg leeft. BCM moet geen IT-'feestje' worden, maar breed in de organisatie landen. BCM gaat ook over de duurzame inzet van collega's, bedrijfsmiddelen en gebouwen. Met betrekking tot deze aspecten ligt een belangrijke verantwoordelijkheid bij directies als Facilitair Bureau en Personeel & Organisatie.

   Daarbij valt ons ook op dat in de startnotitie weinig aandacht is, voor de wijze waarop draagvlak en bewustwording omtrent BCM gecreëerd zal worden. Dit zou in de huidige opzet bereikt moeten worden via de workshops. Hoewel de workshops daar ook zeker aan zullen bijdragen, is het de vraag of workshops alleen voldoende zijn. Wij achtten het van belang dat er in bredere zin aandacht voor het creëren van draagvlak is. Zo is het van belang dat ook ruim voordat de workshops plaatsvinden, het belang van BCM gecommuniceerd wordt. Ook zou het goed zijn om de kritieke directies mee te nemen

in de verdere besluitvorming, gezien hun cruciale rol met betrekking tot BCM. Zie voor nadere uitwerking van deze punten de aanbevelingen.

3. Het is onduidelijk hoe leveranciers en ketenpartners in het implementatietraject betrokken zullen worden. We vinden dit opvallend omdat in eerdere interviews die zijn afgenomen door VKA aangegeven is, dat het essentieel is dat afhankelijkheden van ketenpartners en leveranciers meegenomen dienen te worden in de continuïteitsplannen. Ook is in interviews het belang benadrukt van het nauw betrekken van ketenpartners en leveranciers in het BCM-implementatietraject. Hoe hierop ingespeeld zal worden, is nu onduidelijk.

Risico

BCM is een gemeentebrede aangelegenheid. Wanneer er onvoldoende draagvlak en bewustzijn is voor BCM binnen de gemeente, is het risico dat BCM onterecht vooral een IT-issue is. Dit maakt de gemeente kwetsbaar op andere (niet-IT-)aspecten van BCM, bijvoorbeeld hoe we als gemeente omgaan met ketenpartners (leveranciers), bedrijfsmiddelen en gebouwen. Ook is het risico dat de verantwoordelijkheid voor de implementatie voor BCM onvoldoende voelt als een verantwoordelijkheid van de business, maar meer als een opgave die centraal vanuit de gemeente is opgelegd, zonder dat hier vanuit de business invloed op uit te oefenen valt.

Aanbeveling

- Aanvullende aandacht voor bewustwording en draagvlak omtrent BCM is gewenst.

- Betrek directies, ketenpartners en leveranciers (stakeholders) nauw in het vervolg van het BCM-implementatietraject. Maak daarbij duidelijk wat het doel en belang van BCM is, wat het doel van de voorgestelde aanpak is en wat verwacht wordt van de stakeholders. Laat hierbij ook ruimte voor stakeholders voor eigen inbreng.

- We bevelen aan om bij de start van het implementatietraject BCM het GMT hier op een formele wijze over te laten communiceren en het belang van BCM verder uit te dragen. Dit benadrukt het belang dat het GMT aan BCM hecht en is ook meteen één van de belangrijkste randvoorwaarden voor een succesvolle implementatie (Informatiebeveiligingsdienst VNG: BCM agenderen binnen de organisatie).

4.2 Beleg verantwoordelijkheden voor BCM breed en werk de inrichting van de governance voor BCM in de crisissituatie uit.

Er wordt in de startnotitie geen aandacht besteed aan het breder beleggen van de bestuurlijke en ambtelijke verantwoordelijkheid. Daarnaast is de governance voor BCM in een crisissituatie nog niet uitgewerkt en uitgedacht.

In de startnotitie is de inrichting van de governance van BCM beschreven. In de notitie staat:

"De eerste aanzet voor de inrichting gaat over de 'koude' fase, oftewel er is geen crisis of uitwijk aan de orde. De inrichting in de 'warme' fase is een resultaat van het BCM-traject."

"De governance van de BCM-situatie (warme fase) wordt ontwikkeld aan de hand van competenties in plaats van functie. Niet de hiërarchische plek van een persoon, maar diens kennis en kunde bepalen welke plek diegene binnen de BCM-organisatie inneemt."

Bevindingen

1. In de startnotitie wordt beperkt aandacht besteed aan de bestuurlijke verantwoordelijkheid voor BCM in het college en de ambtelijke verantwoordelijkheid in het GMT. De Rekeningencommissie van de

gemeenteraad constateert dat momenteel in de gemeente nog onvoldoende voortgang geboekt wordt in het organisatorisch inbedden en bemensen van BCM. De verantwoordelijkheid voor dit onderwerp zou breed in de organisatie gevoeld en genomen moeten worden. Wij onderschrijven dit belang. De gemeentebrede implementatie van BCM vraagt breed gevoelde en genomen verantwoordelijkheid zowel bestuurlijk als ambtelijk en op verschillende niveaus in de organisatie. Hoewel de stelselverantwoordelijkheid voor BCM uiteindelijk in de portefeuille valt van één stedelijk directeur, zijn alle stedelijk directeuren inhoudelijk verantwoordelijk voor BCM. De proceseigenaren zijn uiteindelijk verantwoordelijk voor de beheersing op strategisch, tactisch en operationeel niveau van hun processen (conform Amsterdam Doelgericht). BCM is hier een onderdeel van.

2. In de startnotitie wordt gesteld dat de inrichting van de governance voor BCM in de 'warme' fase (op het moment van een crisis) het resultaat is van het BCM-implementatietraject. De BCM-governance voor in crisissituaties is nog niet uitgewerkt. Daarbij kent het totale BCM-implementatietraject een looptijd van twee jaren. Het is onduidelijk wanneer de inrichting van de governance in de 'warme' fase nader wordt uitgewerkt. Wij vinden dat hier op korte termijn invulling aan moet worden gegeven. Het risico is dat zich in de tussenliggende periode een crisis voordoet. De gemeente is hier mogelijk dan niet goed op voorbereid.

3. Veel kernprocessen die door het GMT als cruciaal worden gezien met betrekking tot de continuïteit betreffen ketenprocessen. Juist bij deze directie overstijgende processen is het extra van belang dat duidelijk is waar eigenaarschap ligt. Wij zien hierin grote continuïteitsrisico's. Voor eigenaarschap van BCM bij ketenprocessen is geen aandacht in de startnotitie. Ook zien we geen aandacht voor de rol van control. Zij hebben een belangrijke rol in de advisering en monitoring van BCM-risico's.

<u>Risico</u>

Het risico is dat er op het gemeentelijk managementniveau (zowel ambtelijk als bestuurlijk) de verantwoordelijkheden voor BCM niet goed zijn belegd, dan wel dat deze verantwoordelijkheden onvoldoende worden gevoeld, waardoor BCM niet van de grond komt. Het college en het GMT hebben hierbij een belangrijke voorbeeldfunctie. Als het belang op dit niveau niet voldoende wordt gevoeld en uitgedragen, dan gaat dit ten kostte van het draagvlak voor de implementatie van BCM in de hele gemeente. Ook zien we er een risico in, dat de governancestructuur voor tijdens crisissituaties nog niet is uitgewerkt. Mocht zich op korte termijn een crisis voordoen dan is de vraag of de gemeente hier in voldoende mate op is voorbereid.

Aanbeveling

- Beleg verantwoordelijkheden voor BCM en werk de inrichting van governance voor BCM in de crisissituatie uit.

- Besteedt expliciet aandacht aan het eigenaarschap voor BCM bij ketenprocessen en laat dit door het GMT vaststellen.

- Werk op korte termijn uit hoe de governance van BCM in een crisissituatie eruit zou moeten zien en laat dit vaststellen door het GMT.

4.3 BCM-implementatietraject kan mogelijk efficiënter

Binnen de gemeente zijn bedrijfsprocessen geïdentificeerd die cruciaal zijn met betrekking tot de continuïteit van de bedrijfsvoering. Deze zogenaamde kernprocessen zijn een goed uitgangspunt voor de voorgestelde inventarisatie van bedrijfsprocessen zoals opgenomen in de startnotitie. De gemeente begint hiermee niet blanco. Daarnaast wijzen we erop dat het huidige voorstel voor het BCM-implementatietraject in de startnotitie meer risicogestuurd zou kunnen worden aangevlogen omwille van efficiëntie.

Een belangrijke stap in BCM is het identificeren van de bedrijfsprocessen die cruciaal zijn binnen de organisatie. Hier ligt een rol weggelegd voor het GMT. In de startnotitie is beschreven hoe deze bedrijfsprocessen worden geïdentificeerd:

"Workshop Red de gemeente voor het GMT: Leden GMT gaan met elkaar in discussie welke kroonjuwelen de gemeente heeft door een situatie te simuleren waarin de gemeente gered moet worden."

"De workshop is een impliciete business impact analyse (BIA): In deze workshop gaan we in gesprek over welke processen en producten de belangrijkste zijn voor de gemeente en hoe lang deze mogen uitvallen."

Bevindingen

1. In februari 2023 is door het GMT een lijst met 86 kernprocessen vastgesteld. Dit is een lijst van processen waarvan het GMT vindt dat die altijd goed beheerst moeten worden. Binnen deze lijst is ook aangegeven welke processen hiervan cruciaal zijn met betrekking tot continuïteit. Hoewel het zeker goed is om deze lijst periodiek te herijken, willen wij er tegelijkertijd op wijzen dat de gemeente in dit opzicht niet op nul begint. Hier lijkt nu geen aandacht voor te zijn in de startnotitie.

2. De workshops die georganiseerd worden zijn impliciete BIA's. Het kan zijn dat het GMT, college, directie-directeuren en/of verantwoordelijke proceseigenaren (bij een beperkte impact) bepaalde risico's willen accepteren. Middels het besluitvormingsproces zal dit helder moeten worden. Voor geaccepteerde risico's hoeft geen calamiteitenscenario te worden gemaakt. Het is niet zinvol om mitigerende maatregelen te treffen en kosten te maken voor bedrijfsprocessen waarvan uitval wordt geaccepteerd (zie ook HS4 in het plan van aanpak bedrijfscontinuïteit IBD van de VNG). Ook kan het helpen om expliciet te bepalen wat de maximale geaccepteerde uitval of schade van een proces is. Dit sluit ook aan bij de aanbeveling vanuit de rekeningencommissie om BCM voor de organisatie in te richten op basis van een risicoanalyse.

3. In de startnotitie wordt niet expliciet ingegaan op de inhoud van de workshops. Wel wordt aangegeven dat het impliciete BIA's zijn. Wij achten het van belang dat in de worshops op directieniveau in ieder geval aandacht is voor (standaard)risico's BCM en beheersmaatregelen. Dit is voorwaardelijk voor de inrichting van de monitoring op de risico's. Op termijn zal ook een onafhankelijke partij aangewezen moeten worden voor beoordeling van de effectiviteit van BCM. Hier kan interne audit een rol spelen (FFIEC; business continuity management). Daarnaast zou het goed zijn om aandacht te besteden aan de herhaalbaarheid van de BIA's/ workshops zodat makkelijk updates kunnen worden uitgevoerd. Dit stelt management in staat om informatie te herevalueren indien significante wijzigingen zich hebben voorgedaan. (FFIEC; business continuity management). Bijvoorbeeld in het geval dat de kernprocessen binnen de gemeente wijzigen.

Risico

Het risico is een verlies aan efficiëntie. Er is een efficiëntieslag te behalen in de voorgestelde opzet.

Aanbeveling

- Richt de workshops binnen het BCM-implementatietraject efficiënter in en werk de inhoud van de workshops nader uit.

- Neem bij de inventarisatie van de 'kroonjuwelen' in de workshop 'Red de gemeente' de al bestaande lijst met vastgestelde kernprocessen (specifiek m.b.t. tot continuïteit) als uitgangspunt. Dit voorkomt dubbel werk. Daarnaast wijzen wij erop, dat de informatiebeveiligingsdienst (IBD) van de Vereniging Nederlandse Gemeenten (VNG) een lijst heeft opgesteld met 13 top-kritische bedrijfsprocessen binnen gemeenten. Neem ook deze lijst mee in het proces.

- Besteed in de workshop op GMT-niveau vooral aandacht aan de impactclassificatie van de reeds geïnventariseerde kernprocessen en aan risicobereidheid en risicoacceptatie.

- Wij bevelen aan om nadat de workshops op GMT-niveau, clusterniveau en bij de kritieke directies hebben plaatsgevonden, niet direct de workshops te organiseren bij alle directies, maar juist eerst te focussen op de processen bij de directies die door het GMT al als cruciaal zijn bestempeld met betrekking tot continuïteit (kernprocessen). Op basis van de uitkomsten van een risicoanalyse van de overige directies kan vervolgens besloten worden of het noodzakelijk is om ook workshops te organiseren bij overige directies of dat risico's bewust geaccepteerd worden.

- Besteed in de workshops op directieniveau expliciet aandacht aan (standaard)risico's en beheersmaatregelen. Dit is voorwaardelijk voor de inrichting van de monitoring op BCM-risico's. Let ook op de herhaalbaarheid van de workshops.

4.4. Het is onduidelijk of crisismanagement breed en afdoende is ingericht in de gemeente.

De mate waarin crisismanagement breed en afdoende is ingericht binnen de gemeente Amsterdam is van invloed op de doorlooptijd van het BCM-implementatietraject. Het is momenteel onduidelijk of crisismanagement breed en afdoende is ingericht.

In de startnotitie is de verhouding tussen BCM en crisismanagement beschreven. In de notitie staat het volgende:

“Uit de interviews blijkt dat er verschillende beelden zijn van de huidige status van het gemeentelijke brede crisismanagement. We gaan er nu vanuit dat crisismanagement breed is ingericht (voor een crisis binnen de gemeentelijke organisatie). Mocht tijdens de uitvoering blijken dat dat niet het geval is dan verandert de opbouw van de routekaart.”

“crisismanagement is reactief en is een onmiddellijke reactie op een ontstane situatie, BCM is proactief je zorgt er voor dat er voor een aantal te verwachten scenario’s alternatieve oplossingen voorbereid zijn waarop je in geval van een crisis terug kunt vallen om een deel van je bedrijfsprocessen functioneel te houden.”

Aanbevelingen

Wij bevelen aan om in kaart te brengen in hoeverre crisismanagement breed is ingericht in de organisatie en hiernaar te verwijzen in verdere communicatie. Mocht crisismanagement niet breed zijn ingericht binnen de gemeente, dan is het effectiever om eerst generieke maatregelen te nemen, voordat er naar de bedrijfsprocessen wordt gekeken. Denk aan maatregelen tegen: brand en bliksemschade, grootschalige stroomuitval, overstromingen en verlies van communicatiemiddelen.

Bevindingen

De startnotitie geeft aan ervanuit te gaan dat crisismanagement binnen Amsterdam breed is ingericht en dat, als dat niet het geval is, de opbouw van de routekaart moet worden aangepast. Daarnaast heeft VKA in interviews opgehaald dat ‘er verschillende beelden zijn van de huidige status van het gemeentelijke brede crisismanagement’. Wij constateren, dat door VKA niet is vastgesteld dat crisismanagement daadwerkelijk breed en afdoende is ingericht in de gemeente. Crisismanagement is echter een belangrijk voorportaal van BCM. Het is niet effectief om aandacht te besteden aan BCM, wanneer generieke maatregelen zoals maatregelen tegen brand, stroomuitval en overstroming niet op orde zijn. Het IBD van de VNG zegt hierover in hun plan van aanpak op bedrijfscontinuïteit, het volgende:

“Voordat naar de bedrijfsprocessen wordt gekeken moet eerst worden nagegaan of er voldoende generieke maatregelen zijn getroffen om calamiteiten te voorkomen (“huidige beschikbare middelen”). Het is effectiever om eerst deze generieke maatregelen te nemen voordat er naar de bedrijfsprocessen wordt gekeken. Als mocht blijken dat de genomen maatregelen niet toereikend zijn, geef hier dan eerst prioriteit aan.”

Risico

Het risico van een niet breed ingericht crisismanagement binnen de gemeente is dat de opbouw van de routekaart in de startnotitie moet worden aangepast en daarmee ook de doorlooptijd van het BCM-implementatietraject langer wordt. In de startnotitie staat, dat er met betrekking tot de implementatie van BCM op korte termijn resultaten moeten worden geboekt om aantoonbaar in control te komen en te blijven. Het risico bestaat, dat dit op zich laat wachten.

Bijlage 1: Werkzaamheden en afspraken

1.1 Werkzaamheden

Op basis van de doelstelling van de audit heeft het auditteam de volgende werkzaamheden uitgevoerd. De startnotitie is vergeleken met ISO-norm 22301 voor bedrijfscontinuïteitsbeheer en met het plan van aanpak en de handreiking voor bedrijfscontinuïteit van de informatiebeveiligingsdienst van de vereniging Nederlandse gemeenten. Daarnaast zijn interviews afgenomen met directies die een cruciale rol hebben met betrekking tot de continuïteit van kritische bedrijfsprocessen. Hiervoor zijn de kernprocessen van de gemeente Amsterdam als uitgangpunt genomen.

De interviews zijn afgenomen bij de directies: Belastingen, Dienstverlening, Facilitair Bureau en Inkomen. Daarnaast is een interview afgenomen met crisismanagement bij Openbare Orde en Veiligheid. Ook is gesproken met een van de G-4 gemeenten over hun lessen voor BCM.

Verantwoording werkzaamheden

Wij hebben deze audit uitgevoerd conform het Audit Charter 2023, welke is ondertekend door onze opdrachtgever, de Gemeentesecretaris. Hierin staat de reikwijdte van onze werkzaamheden en bevoegdheden beschreven en is te vinden op onze intranetpagina van IA&BO. Onze werkzaamheden worden uitgevoerd in overeenstemming met de normen van de beroepsgroep voor interne auditors. Dit is het Instituut voor Interne Auditors (IIA). Sinds september 2022 is IA&BO gecertificeerd.

1.2 Afspraken

Voor de audit gelden onderstaande afspraken:

Verspreidingskring

Naast dat de definitieve rapportage gedeeld zal worden met DS&I zullen we het definitieve auditrapport ook toesturen aan de concerncontroller, de stedelijk directeur, de manager Control, de (proces)controller en ACAM. Wanneer ACAM erom verzoekt, verstrekken wij hen ook toegang tot ons dossier. De conclusies en belangrijkste bevindingen worden opgenomen in onze voortgangsrapportage die aan het GMT wordt toegestuurd.

Fully in Control

De bevindingen en aanbevelingen door IA&BO worden overgenomen in de Goverance, Risk en Compliance Tool van Gemeente Amsterdam genaamd FullyInControl. Vervolgens dient de auditee de nadere opvolging hiervan in dit systeem vast te leggen.

Openbaar maken van rapporten

Definitieve auditrapporten worden 6 maanden na bespreking in het Risk & Audit Comité openbaar gemaakt.

Bijlage 2: Aanknopingspunten ISO-22301 voor verdere inrichting BCM

De startnotitie BCM biedt een goede aanzet voor de implementatie van BCM binnen de gemeente. De verdere uitwerking van de opzet van het implementatietraject is aan het team kwartiermakers BCM.

Hoewel de voorgestelde lean BCM-implementatiemethodiek andere uitgangspunten kent dan de traditionele implementatie van BCM, maakt dit het ISO-22301 normenkader niet per se minder geschikt. Onderstaand hebben wij enkele standaarden uit ISO-22301 opgesomd, waarvan wij denken, dat ze uitwerking behoeven door de gemeente ten behoeve van een verdere inrichting van BCM. De standaarden zijn:

- **Bepalen van de reikwijdte van het BCM-systeem (4.3.1):** De organisatie moet bepalen welke delen en producten/diensten worden opgenomen in het BCMS, met documentatie van eventuele uitsluitingen die geen invloed hebben op de bedrijfscontinuïteit, rekening houdend met de locatie, grootte, aard en complexiteit van organisatieonderdelen.
- **Leiderschap en toewijding (5.1 en 5.2.1):** Het topmanagement zorgt ervoor dat beleid voor bedrijfscontinuïteit en de doelstellingen van bedrijfscontinuïteit worden vastgesteld en compatibel zijn met de strategische richting van de organisatie.
- **Communiceren van BCM-beleid (5.2.2):** Het bedrijfscontinuïteitsbeleid moet beschikbaar zijn als gedocumenteerde informatie, gecommuniceerd worden binnen de organisatie en beschikbaar zijn voor betrokken partijen.
- **Business continuity doelstellingen en hoe deze te bereiken (6.2.2):** Bij het plannen van het behalen van de bedrijfscontinuïteitsdoelstellingen moet de organisatie bepalen wat er gedaan moet worden, welke middelen nodig zijn, wie verantwoordelijk is, wanneer het voltooid zal zijn, en hoe de resultaten geëvalueerd zullen worden.
- **Middelen (7.1):** De organisatie moet de benodigde middelen bepalen en beschikbaar stellen voor het opzetten, implementeren, onderhouden en continu verbeteren van het BCMS.
- **Bewustzijn (7.3):** Werknemers moeten op de hoogte zijn van het bedrijfscontinuïteitsbeleid, hun bijdrage aan de effectiviteit van het BCMS, de consequenties van niet naleven en hun rol bij verstoringen;
- **Business impactanalyse en risicoanalyse (8.2.2):** De organisatie moet het proces voor het analyseren van bedrijfsimpact gebruiken om prioriteiten en vereisten voor bedrijfscontinuïteit vast te stellen. Het proces moet impacttypes en -criteria definiëren, activiteiten identificeren, impact beoordelen, tijdframes bepalen, en afhankelijkheden vaststellen.
- **Business continuity plannen en procedures (8.4.4):** De organisatie moet gedocumenteerde en onderhouden bedrijfscontinuïteitsplannen en -procedures hebben die teams begeleiden bij het reageren op verstoringen en het herstellen van activiteiten binnen vastgestelde tijdframes. Deze plannen bevatten ook maatregelen voor activering, capaciteitslevering, gevolgenbeheer en rapportagevereisten. (criteria voor BCP plannen)
- **Monitoren, meten, analyseren en evalueren (9.1):** De organisatie bepaalt wat, hoe, wanneer en door wie er wordt gemonitord,

gemeten, geanalyseerd en geëvalueerd in het BCMS, en evalueert de prestaties en effectiviteit ervan.