Samenwerkingsovereenkomst

Aanvullende opdracht voor het Cyber Response Team ter ondersteuning van lokale besturen

Tussen de ondergetekenden

enerzijds

VLAAMSE GEMEENSCHAP, vertegenwoordigd door de Vlaamse Regering, bij delegatie, in de persoon van de leidend ambtenaar van agentschap zonder rechtspersoonlijkheid Agentschap Binnenlands Bestuur, Jeroen Windey.

hierna “de opdrachtgever”,

en anderzijds

A. Het Vlaamse Gewest, vertegenwoordigd door de Vlaamse Regering, bij delegatie, in de persoon van de leidend ambtenaar van het intern verzelfstandigd agentschap zonder rechtspersoonlijkheid agentschap Digitaal Vlaanderen, administrateur-generaal Jan Smedts, ingeschreven in het KBO met nummer 0316.380.841 en vestigingsnummer 2.256.180.804, waarvan de administratieve zetel zich bevindt te Havenlaan 88, 1000 Brussel, hierna afgekort “Digitaal Vlaanderen”,

B. Het Eigen Vermogen Digitaal Vlaanderen, vertegenwoordigd door de voorzitter van de beheerscommissie van het Eigen Vermogen Digitaal Vlaanderen, in de persoon van de heer Jan Smedts, ingeschreven in het KBO met nummer 0643.634.986 waarvan de administratieve zetel zich bevindt te Havenlaan 88, 1000 Brussel, hierna afgekort “EV DV”;

A en B zijn samen “de opdrachtnemer”, ieder wat zijn decretale of reglementaire bevoegdheden betreft,

Agentschap Binnenlands Bestuur, Digitaal Vlaanderen en EV DV worden hieronder ook wel afzonderlijk aangeduid als een “partij” of gezamenlijk als de “partijen”;

wordt overeengekomen wat volgt.

Artikel 1. Voorwerp van de overeenkomst

De opdrachtgever belast de opdrachtnemer met het uitvoeren van de opdracht **aanvullende opdracht voor het Cyber Response Team ter ondersteuning van lokale besturen**, zoals nader beschreven in bijlage 1.

Artikel 2. Verbintenissen

De opdrachtnemer verbindt zich ertoe de nodige mensen en middelen in te zetten voor de kwaliteitsvolle en efficiënte uitvoering van de in bijlage 1 omschreven opdracht.

De opdrachtgever verbindt zich ertoe de middelen en de nodige informatie ter beschikking te stellen voor het correct uitvoeren van de opdracht.

Partijen verbinden zich ertoe deze overeenkomst als een inspanningsverbintenis op te vatten.

Over de voortgang van deze opdracht wordt gerapporteerd aan de stuurgroep van het Cyber Response Team, waarin vertegenwoordigers zetelen van Vlaams minister-president Jan Jambon en Vlaams viceminister-president en minister van Binnenlands Bestuur Gwendolyn Rutten, en van Digitaal Vlaanderen, Audit Vlaanderen en het Agentschap Binnenlands Bestuur.

Artikel 3. Kostprijs en betalingsmodaliteiten

De totale kostprijs van de opdracht bedraagt 640.000 euro, waarvan de detailberekening zich in bijlage 2 bevindt, evenals de verdeling van de kosten, betalingsmodaliteiten en facturatiegegevens.

Artikel 4. Uitvoeringsmodaliteiten

De uitvoeringsmodaliteiten van deze overeenkomst staan in detail beschreven in bijlage 3.

Alle communicatie in het kader van onderhavige overeenkomst wordt gericht aan de contactpersonen van elke partij, vermeld in bijlage 3.

De taken die toevertrouwd zijn aan de opdrachtnemer kunnen tijdens de uitvoering van het project gewijzigd worden in functie van de bekomen resultaten of met het oog op een nieuwe oriëntering van de opdracht. Deze wijzigingen maken het voorwerp uit van een ondertekend addendum bij deze overeenkomst.

Artikel 5. Gegevensbescherming

Elke partij zal alle persoonsgegevens die zij in het kader van de uitvoering van deze overeenkomst ontvangt, verwerken in overeenstemming met de regelgeving over de bescherming van natuurlijke personen bij de verwerking van persoonsgegevens, en in het bijzonder de Algemene Verordening Gegevensbescherming.
Elke partij treedt op als verwerkingsverantwoordelijke met betrekking tot de gegevens die zij verwerkt in het kader van de opdracht en zal voldoende technische en organisatorische maatregelen ter beveiliging en bescherming van de vertrouwelijkheid en integriteit van deze gegevens.

Artikel 6. Vertrouwelijkheid

Vertrouwelijke informatie is technische, commerciële of organisatorische informatie over de ene partij die ter kennis werd gebracht aan de andere partij en in het algemeen, elke informatie van welke aard of vorm dan ook die werd verstrekt aan een partij met het oog op de uitvoering van deze overeenkomst.

De partijen verbinden er zich toe vertrouwelijke informatie niet te gebruiken, te reproduceren en te verspreiden, rechtstreeks of onrechtstreeks, mondeling of schriftelijk, buiten het kader van de overeenkomst, tenzij voorafgaande schriftelijke toelating van de andere partij. Indien een partij

wettelijk verplicht wordt om enige van de vertrouwelijke informatie openbaar te maken, zal de gedwongen partij redelijke inspanningen ondernemen om de andere partij hiervan zo snel mogelijk schriftelijk in kennis stellen zodat de andere partij conservatoire maatregelen kan nemen of andere remedies kan zoeken.

De partijen verbinden er zich toe alle nodige stappen te ondernemen om de naleving te verzekeren van deze verplichting tot vertrouwelijkheid door hun personeelsleden en medecontractanten die betrokken zijn bij of werden aangeworven voor de uitvoering van de opdracht en die directe kennis moeten hebben van deze inlichtingen. Beide partijen blijven echter aansprakelijk tegenover elkaar voor elke inbreuk op de verplichting tot vertrouwelijkheid die in dit artikel wordt omschreven.

De partijen verplichten er zich toe om, op eerste verzoek, alle exemplaren en alle kopieën van vertrouwelijke inlichtingen die hen werden verstrekt terug te bezorgen of te vernietigen.

Artikel 7. Aansprakelijkheid

De opdrachtnemer is enkel aansprakelijk voor schade die rechtstreeks voortvloeit uit de gebrekkige uitvoering van deze overeenkomst. De opdrachtnemer is evenwel nooit aansprakelijk in geval van overmacht, i.e. onvoorziene omstandigheden die onafhankelijk zijn van haar wil en de correcte uitvoering van de verbintenissen onmogelijk maakt.

Artikel 8. Geschillen

Deze overeenkomst wordt beheerst door en geïnterpreteerd volgens de Belgische wetgeving.

Elk geschil of elke eis, voortvloeiend uit of in verband met de geldigheid, interpretatie, uitvoering of ontbinding van de overeenkomst zullen worden voorgelegd aan de bevoegde rechter in het arrondissement waar de opdrachtgever gevestigd is.

Voor elk geschil zal eerst getracht worden van het in der minne te regelen door onderhandeling en zal er dus een verplichte verzoeningspoging vooraf gaan aan elke mogelijke gerechtelijke beslechting van het geschil.

Artikel 9. Duur en beëindiging van de overeenkomst

De overeenkomst treedt in werking op xx/12/2023 voor de duur 13 maanden.

Artikel 10. Deelbaarheid

De nietigheid of ongeldigheid van één of meerdere bepalingen van deze overeenkomst beïnvloedt de geldigheid van de andere bepalingen niet. Elke bepaling, die nietig of ongeldig verklaard is, zal worden beschouwd als weggelaten uit de overeenkomst, zonder echter de andere bepalingen te beïnvloeden, die, wat hen betreft, van toepassing blijven, tenzij dat de nietig of ongeldig verklaarde bepaling(en) van wezenlijk belang is voor het voorwerp van de overeenkomst.

Opgemaakt te Brussel en door elke partij digitaal te ondertekenen.

Agentschap Binnenlands Bestuur

Jeroen Windey

Administrateur-Generaal

Agentschap Digitaal Vlaanderen

Jan Smedts

Administrateur-Generaal

Eigen Vermogen Digitaal Vlaanderen

Jan Smedts

Voorzitter beheerscommissie

Bijlagen: Onderstaande bijlagen maken integraal deel uit van deze overeenkomst:

Bijlage 1: Concrete opdrachtomschrijving – verbintenissen van alle partijen

Bijlage 2: Kostprijs en betalingsmodaliteiten

Bijlage 3: Uitvoeringsmodaliteiten

Bijlage 1. opdrachtomschrijving – verbintenissen van alle partijen

1. Situering

Naar aanleiding van o.a. de cyberaanval op stad Antwerpen heeft de Vlaamse Regering beslist op 13/01/2023 om een Cyber Response Team (CRT) voor lokale besturen op te richten. Het CRT is een kennisorganisatie dat kennis en expertise bundelt en lokale besturen ondersteunt bij cyberincidenten. De ondersteuning van het CRT is tweeledig:

- **Preventieve ondersteuning**: Om nieuwe cyberincidenten te voorkomen, verzamelt het CRT alle beschikbare informatie en verwerkt de informatie in gerichte adviezen en kennisartikelen, die o.a. via ledenorganisaties worden verspreid. Verder capteert en beantwoordt het CRT vragen van lokale besturen.
- **Reactieve ondersteuning**: In het geval een cyberincident zich voordoet, ondersteunt het CRT lokale besturen bij het opstarten van een Cyber Response Plan, de coördinatie van activiteiten en communicatie. Verder ondersteunt het CRT bij het verzamelen van alle nodige informatie en informeren van Vlaamse en federale diensten zoals de Gegevensbeschermingsautoriteit (GBA).

Met de oprichting van het CRT hebben lokale besturen een centraal aanspreekpunt, waar ze terecht kunnen met al hun vragen. Ook wanneer lokale besturen getroffen zijn door een cyberaanval, staat het CRT klaar voor ondersteuning. Het CRT, dat op Vlaams niveau, wordt aangestuurd zorgt voor de nodige synergie en efficiënte inzet van middelen. Digitaal Vlaanderen en het Agentschap Binnenlands Bestuur bundelen de krachten en zetten hun expertise in om de lokale besturen optimaal te ondersteunen.

Echter, uit de resultaten van onder andere de ICT-veiligheidsaudits met cofinanciering en het traject ethisch hacken i.s.m. VVSG blijkt dat er steeds verschillende organisatorische en technische kwetsbaarheden zijn bij lokale besturen. Ondanks het huidige ondersteuningsaanbod blijken lokale besturen nog onvoldoende voorbereid op cyberincidenten. De huidige ondersteuning vanuit de Vlaamse overheid maken kwetsbaarheden bij lokale besturen inzichtelijk (bv. via ICT-veiligheidsaudits) en bieden de nodige houvast (bv. toolkit cyberveiligheid), maar toch is er een duidelijke nood aan meer **proactieve ondersteuning**.

Omwille van het aanhoudende belang van informatieveiligheid voor lokale besturen, willen het Agentschap Binnenlands Bestuur en Digitaal Vlaanderen daarom inzetten op een meer hands-on begeleiding van steden en gemeenten in samenwerking met het Cyber Response Team. Hiervoor worden bestaande instrumenten, o.a. toolkit cyberveiligheid, zo veel als mogelijk hergebruikt. Omwille van het huidige takenpakket van het CRT en haar positie in het landschap, is het CRT de aangewezen partij om de verdere ondersteuning en begeleiding van lokale besturen op zich te nemen. Het CRT zal op die manier meer inzetten op netwerkontwikkeling en -verruiming, in samenwerking met bestaande partnerorganisaties zoals VVSG of V-ICT-OR. Hiermee beoogt ABB de zichtbaarheid van het CRT te verhogen en haar rol en positie in het landschap te consolideren.

Hiervoor worden, bovenop de voorziene middelen voor de opstart en operationele werking van het CRT, bijkomende middelen voorzien.

2. *Opdrachtomschrijving* - Aanvullende opdracht voor het Cyber Response Team ter ondersteuning van lokale besturen

De aanvullende ondersteuning voor lokale besturen door het Cyber Response Team omvat twee sporen. Enerzijds worden lokale besturen begeleid om de nodige voorbereidingen te treffen om snel te kunnen reageren wanneer een cyberaanval zich voordoet, anderzijds wordt ingezet op de beveiliging van de digitale infrastructuur.

Hieronder worden beide sporen meer in detail toegelicht.

Spoor 1: Begeleiding van lokale besturen bij het opmaken van een Business Continuïteitsplan

Wanner een lokaal bestuur slachtoffer wordt van een cyberincident, heeft dit grote gevolgen voor de dienstverlening aan de burger. Naargelang de impact en reikwijdte van het incident, kan de dienstverlening van het lokaal bestuur gedurende enkele dagen tot weken in belangrijke mate worden onderbroken en/of verstoord. Een lokaal bestuur dat geconfronteerd wordt met een cyberincident moet daarom snel en gepast actie ondernemen om de situatie zo snel mogelijk onder controle te krijgen en terug te keren naar de reguliere werking. Het CRT ondersteunt hier reeds in, maar toch is het belangrijk dat al proactief is nagedacht over welke stappen genomen moeten worden bij het crisisbeheer bij grootschalige incidenten en dat lokale besturen beschikken over een kwalitatief business continuïteitsplan (BCP).

Uit de resultaten van de ICT-veiligheidsaudits en het traject ethisch hacken blijkt echter dat een bruikbaar BCP vaak nog ontbreekt bij lokale besturen. Een gedegen Business Continuity Management (BCM) wordt almaar belangrijker voor lokale besturen om de continuïteit van hun dienstverlening aan burgers te kunnen waarborgen. Deze nood wordt zichtbaar wanneer incidenten met betrekking tot informatieveiligheid de toegang tot of het vertrouwen in diensten onmogelijk maken. Daarom is het van cruciaal belang dat lokale besturen zich effectief voorbereiden, onder meer via het opstellen van een Business Continuïteitsplan (BCP).

Het doel van het eerste spoor is om via een reeks van workshops lokale besturen bij te staan in het opmaken van een BCP. Hiervoor wordt gebruik gemaakt van de reeds ontwikkelde instrumenten uit de toolkit cyberveiligheid.

De begeleiding bestaat uit twee trajecten met telkens vijf workshops en 25 deelnemende lokale besturen. De vijf workshops worden dus twee keer georganiseerd en in totaal worden 50 lokale besturen begeleidt bij de opmaak van een BCP. De workshops worden over een periode van 8 à 9 maanden gespreid, opdat deelnemende lokale besturen voldoende tijd hebben om de nodige informatie te verzamelen, contacten te leggen en de nodige voorbereidingen te treffen. Het CRT neemt hierbij zijn rol op door de lokale besturen actief te contacteren en informeren over dit aanbod.

De opdracht wordt als volgt opgezet:

Voorbereiding en plannen van de workshops:

In een eerste fase worden de reeds bestaande BCM-gerelateerde informatie van het VO-CRT en de VVSG geconsulteerd (zoals bijv. de richtlijnen van het VVSG voor het opstellen van BCP's en de aangeboden templates). Daarnaast worden de lokale besturen geïdentificeerd met de nodige ervaring die later in de workshops kunnen worden betrokken als goede praktijk om geleerde lessen te delen.

Tot slot wordt de aanpak zoals hieronder beschreven verfijnd en wordt de inhoud/voorbereiding van iedere workshop door ABB gevalideerd.

Workshop 1: Theoretisch kader BCM en zelfevaluatie

In de eerste workshop zal een antwoord worden geboden op volgende vragen:

- Wat is een BCP en waarom is het nodig? Waarom is het relevant en hoe wordt het beheerd (binnen een lokaal bestuur)?
- Waarom is een BCP relevant op vlak van informatieveiligheid?
- Welke referentiedocumenten bestaan er binnen de VO en in het algemeen?
- Waar staat mijn lokaal bestuur vandaag? Middels een zelfevaluatie aan de hand van '10 vragen'.

Daarnaast wordt de inleiding naar de volgende sessie gegeven, waar verder wordt toegelicht hoe een BCP tot stand komt.

Tussen workshop 1 en 2 wordt aan de deelnemers gevraagd om relevante informatie te verzamelen en door te nemen zowel met betrekking tot het algemeen kader als voor het eigen lokaal bestuur.

Workshop 2: Identificatie kritieke processen – Business Impact Analyse (BIA)

In de tweede workshop wordt dieper ingegaan op de impact van een incident op de continuïteit in dienstverlening en het identificeren van kritieke processen, als voorbereiding op het uitwerken van een BCP. Tijdens de workshops komen volgende vragen aan bod:

- Hoe bepaal je de kritieke processen? Wie betrek je in dergelijke oefening?
- Welke lessen kunnen we trekken uit eerdere trajecten bij lokale besturen?

Tijdens de workshop worden bruikbare sjablonen ter beschikking gesteld voor de effectieve uitwerking van een business impact analyse ter beschikking gesteld.

OPDRACHT: Na workshop 2 worden deelnemers gevraagd om hun eigen BIA te maken en door te sturen.

Workshop 3: Hoe maak ik mijn BCP?

In de derde workshop krijgen deelnemers algemene feedback die relevant is voor groep met betrekking tot de nazicht van de BIA's. Verder zal de workshop zich toespitsen op de opmaak van een BCP en komen volgende vragen aan bod:

- Welke 'strategische keuzes' moet ik maken?
- Welke bouwstenen heeft het BCP, gelinkt aan het instrumentarium van het VO-CRT?
- Wat moet zeker aan bod komen met informatieveiligheid in het achterhoofd?
- Hoe kan ik dienstverleners betrekken?

Tot slot worden tijdens deze workshop sjablonen ter beschikking gesteld voor de effectieve uitwerking van een BCP.

OPDRACHT: Na workshop 3 worden deelnemers gevraagd om hun eigen BCP op te maken en door te sturen naar het projectteam.

Workshop 4: Hoe ziet mijn BCP er uit en hoe veranker ik dit in de organisatie?

Tijdens de vierde workshop krijgen deelnemers algemene feedback die relevant is voor de groep met betrekking tot nazicht BCP's. Er wordt gefaciliteerde terugkoppeling geboden. De deelnemers krijgen de kans om over hun eigen ervaringen en uitdagingen/struikelblokken te spreken zodat ze instant feedback kunnen krijgen van de groep en van het CRT. De terugkoppeling wordt in specifieke thema's opgedeeld in functie van de resultaten van het nazicht van de BCP's.

Verder voorziet de workshop duidelijkheid rond de rollen en verantwoordelijkheden rond goedkeuring, onderhoud en verankering van BCP binnen het lokale bestuur. Tijdens deze workshop worden ook oefeningen gegeven rond de aanpak en periodiciteit van BCP's.

Als laatste voorziet de workshop experten die voor terugkoppeling zorgen bij vragen van de deelnemers met betrekking tot de BCP.

OPDRACHT: Na workshop 4 worden deelnemers gevraagd om een update van het eigen BCP door te sturen naar het projectteam.

Workshop 5: Geleerde lessen voor de toekomst en verdere verankering

Tijdens de laatste workshop krijgen deelnemers algemene feedback die relevant is voor de groep met betrekking tot de gecontroleerde BCP's. Experten worden ingezet om bij terugkoppeling vragen van deelnemers met betrekking tot BCP en mogelijke volgende stappen te beantwoorden.

De workshop biedt een samenvatting van de geleerde lessen doorheen het hele traject. Daarbij wordt ook de feedback van de deelnemers over het traject gecapteerd en worden geleerde lessen gevalideerd. Daarbij wordt ruimte voorzien om aanbevelingen te doen voor toekomstige workshops

Individuele feedback

Tussen verschillende workshops wordt feedback voorzien op de resultaten van tussentijdse opdrachten bij het opmaken van een BIA of BCP. Deelnemende lokale besturen kunnen hun resultaten bezorgen en krijgen feedback in de vorm van vragen of opmerkingen op de aangeleverde elementen. Waar nodig wordt mondeling verduidelijkt. Doorheen iedere golf worden drie individuele feedbackrondes voorzien.

Rapportering rond geleerde lessen

Het CRT rapporteert over de geleerde lessen doorheen het traject, met specifieke focus op het belang van informatieveiligheid en de verankering van BCM binnen de lokale besturen. De geleerde lessen worden vertaald in een tastbaar instrument voor lokale besturen om zelf, zonder begeleiding, mee aan de slag te gaan. Het instrument wordt ter beschikking gesteld via de kanalen van het Cyber Response Team.

Spoor 2: Piloot begeleidingstraject ter ondersteuning van de implementatie van Vlaamse bouwstenen m.b.t. toegangsbeheer (ACM/IDM)

Uit de resultaten van de ICT-veiligheidsaudits blijkt eveneens dat naast organisatorische maatregelen, ook verschillende technische beveiligingsmaatregelen nog onvoldoende worden voorzien, in het bijzonder met betrekking tot toegangsbeheer. Slechts een beperkt aantal lokale besturen beschikt op dit moment over multifactor authenticatie (MFA). Lokale besturen hebben onvoldoende expertise om technische beveiligingsmaatregelen te implementeren of de reeds bestaande Vlaamse bouwstenen met betrekking tot toegangsbeheer ACM/IDM te integreren. Alle Vlaamse lokale besturen hebben reeds gebruik gemaakt van het Toegangs- en Gebruiksbeheer om de toegang tot de toepassingen van de Vlaamse Overheid binnen het bestuur te beheren.

Daarom wordt binnen de opdracht een tweede (piloot) begeleidingstraject opgestart om een aantal lokale besturen te ondersteunen bij de volledige implementatie of aankoppeling van Vlaamse veiligheidsbouwstenen inzake ACM/IDM. Het doel van dit spoor is tweeledig: (1) de effectieve integratie van Vlaamse bouwstenen realiseren bij lokale besturen en (2) meer inzicht krijgen in de lokale uitdagingen en noden van lokale besturen met betrekking tot implementatie van Vlaamse bouwstenen. Die inzichten moeten Digitaal Vlaanderen in staat stellen om bestaande oplossingen beter af te stemmen op de noden van lokale besturen en opschaling en brede implementatie te faciliteren.

Het CRT zal daarom een team van analisten ter beschikking stellen om bij 30 lokale besturen de integratie van Vlaamse bouwstenen met betrekking tot toegangsbeheer van A tot Z te ondersteunen. De selectie van de lokale besturen zal gebeuren op basis van vooraf bepaalde criteria. Daarbij gaat bijzondere aandacht naar de verschillende grootte, maturiteit en geografische spreiding van lokale besturen en de deelname aan eerdere ondersteuningsinitiatieven, zoals de ICT-veiligheidsaudits met cofinanciering of het traject ethisch hacken in samenwerking met VVSG. Het CRT neemt hierbij zijn rol op en zal actief lokale besturen contacteren, informeren alsook selecteren met betrekking tot dit aanbod.

Middels een voldoende intensieve begeleiding voor en tijdens de integratie kan eventueel technisch bezwaar of een eventueel gebrek aan technische expertise op een correcte manier geadresseerd en

gemitigeerd worden. Het bestuur behoudt zelf het initiatief en beslist doorheen het traject vanzelfsprekend autonoom, maar kan in het kader van dit project rekenen op een 'hands on'-begeleiding door de analisten van Digitaal Vlaanderen.

Een standaard-integratie met het Toegangs- en Gebruikersbeheer neemt minimaal 8 à 10 weken in beslag, al duurt het aansluitingsproces door de band genomen langer. Het traject start met een introductiegesprek en intakefase. Vervolgens worden toepassingen in eerste instantie geïntegreerd met de test- en integratie-omgevingen van het Toegangs- en Gebruikersbeheer en, na grondige testing, vervolgens met de productie-omgevingen van de bouwstenen.

Na afloop van het piloot begeleidingstraject wordt een evaluatie voorzien. Daar worden de impact van de begeleiding en individuele inzichten gebundeld en vertaald naar beleidsaanbevelingen. In een latere fase kan worden bekeken of een soortgelijke dienstverlening zinvol kan zijn bij het integreren van andere bouwstenen of het aansluiten op Cloudops voor lokale besturen.

De verschillende fasen van de hands on-gebaseerde benadering wordt onderstaand vormgegeven, zoals overeengekomen met Digitaal Vlaanderen:

Introductie

Digitaal Vlaanderen engageert zich om middels een breed-gecommuniceerde infosessie het proefproject voor te stellen aan de Vlaamse Lokale Besturen. Deze sessie wordt opgenomen en nadien gedeeld met de besturen die door omstandigheden niet present konden tekenen. Deze infosessie wordt georganiseerd door Veiligheidsbouwstenen in samenwerking en nauwe afstemming met het Cyber Response Team van Digitaal Vlaanderen.

Gedurende een *grace period* van een aantal weken krijgen de lokale besturen de kans om in te tekenen op het proefproject. Agentschap Binnenlands Bestuur benoemt op basis van de input begrepen in deze nota, het aantal besturen dat deel kan nemen aan het project. Indien dit aantal overschreden wordt – i.e. indien meer dan het voorziene aantal lokale besturen wenst deel te nemen – zal in samenspraak met de stuurgroep van het CRT een selectie worden gemaakt. Indien dit aantal niet gehaald wordt, zal middels een tweede infosessie opnieuw uitgereikt worden naar de Vlaamse Lokale Besturen.

Intake

De 30 Lokale Besturen worden verdeeld in 5 groepen van telkens 6 besturen op basis van geografische nabijheid (gouwen / provincies). In onderling overleg wordt er een locatie bepaald waar de intake met de besturen die deel uitmaken van dezelfde groep, zal plaatsvinden.

Een vliegende ploeg van Digitaal Vlaanderen begeeft zich naar deze locatie. Aldaar geeft de ploeg een uitgebreide presentatie omtrent het Veiligheidsbouwstenen-aanbod van Digitaal Vlaanderen. De klemtoon kan daarbij op verzoek gelegd worden op het Toegangs- en Gebruikersbeheer.

Deze vliegende ploeg zal bestaan uit twee analisten die zich doorheen het traject beschikbaar maken voor advies en ondersteuning, en zich flexibel ter beschikking stellen voor vergaderingen – virtueel of op locatie.

Integratiedossier

Het integratiedossier vormt de ruggengraat van een integratietraject. Hierin worden alle noodzakelijke gegevens gecapteerd om een succesvolle integratie met het Toegangs- en Gebruiksbeheer op te zetten, zoals doelpubliek van de applicatie, detail omtrent het integratie-protocol, detail omtrent het rechtenmodel.

Het integratiedossier wordt op locatie aangevuld door de analisten, in samenspraak met de contacten van het lokaal bestuur.

Ondersteuning tijdens het integratietraject

De vliegende ploeg gaat actief ondersteunen bij het opzetten van de integratie. Indien er een gebrek aan protocol-specifieke kennis aanwezig is langs de kant van het bestuur, treedt de vliegende ploeg bij – alsook als er vragen zijn bij de bouwstenen zelf. Concreet zal de vliegende ploeg tijdens de testfase samen met het bestuur een geijkt testplan doorlopen, en handvaten aanreiken om onsuccesvolle testen en problemen het hoofd te bieden.

De 'hands on'-begeleiding wordt, binnen dit project, bovenop de standaarddienstverlening van Digitaal Vlaanderen aangeboden. Onder deze 'hands on'-begeleiding valt protocol-specifieke ondersteuning bij het opmaken van de SAML-metadata, het opmaken van OIDC of OAuth-requests en het opzetten van de federatie. Alsook de mapping naar rechten-en rollenmodellen op maat en troubleshooting-sessie(s). Tot slot behoren ook test-sessies tot de scope van de ondersteuning tijdens het integratieproces.

Ondersteuning na het integratietraject

De vliegende ploeg voorziet, na een succesvol integratietraject, desgewenst in de nodige monitoring- en rapporteringsfunctionaliteit in het Gebruikersbeheer- en/of het Beheersportaal van het Toegangsbeheer.

Indien er volgend op een succesvol integratietraject door het bestuur gesignaleerd wordt dat één of meerdere bulk-upload of default entitlement scanners dienen ingeregeld te worden in het Gebruiksbeheer, zal de vliegende ploeg daarvoor de administratie en planning voor haar rekening nemen.

De vliegende ploeg zal, eenmaal de integratie met succes in productie gesteld is, tezamen met het participerende bestuur een evaluatie maken van het verloop en de resultaten van het traject, alsook van de tevredenheid ten aanzien van de aangeboden ondersteuning en de gretigheid om in de toekomst in een gelijkaardige context andere toepassingen te integreren met de Veiligheidsbouwstenen.

Bovenop de gerichte ondersteuning tijdens en na de integratietrajecten, zal de vliegende ploeg ook op volgende niveaus ageren en ondersteunen.

Cursus Toegangs- en Gebruikersbeheer

De vliegende ploeg kan de besturen die deel uitmaken van eenzelfde groep (cf. supra) desgewenst een cursus Toegangs- en Gebruikersbeheer geven. Met de cursus moeten lokale besturen vertrouwd geraken met het eigenlijke gebruik van de veiligheidsbouwstenen. Een dergelijke begeleiding kan ook ingeregeld worden richting de gebruikers van de toepassingen van deze lokale besturen.

Actief opmeten van de vragen, obstakels en feature request er leven bij de lokale besturen

De vliegende ploeg verzameld actief op welke vragen, obstakels en feature request leven bij de lokale besturen die deelnemen aan het project. Deze vereisten kunnen zowel op operationeel als op technisch niveau situeren. De vliegende ploeg verzamelt deze vragen en vereisten voor elk lokaal bestuur in een gedetailleerd rapport. Dit rapport wordt voorgelegd aan de Toepassingseigenaar van het Toegangs- en Gebruikersbeheer.

Rapport en feedback

De Toepassingseigenaar bespreekt het rapport en de daaraan gekoppelde feedback en eventuele beleidsmaatregelen rechtsreeks met het lokaal bestuur.

Budgettaire invulling:

De vliegende ploeg van Digitaal Vlaanderen zal bestaan uit twee profielen:

- 1 medium-level business analist / project manager
    - Profielprijs (/dag, incl. BTW): € 958,32
    - Dit profiel is bezwaard met de ondersteuning, begeleiding en rapportering op het niveau van elke groep van Lokale Besturen.
    - 10 mandagen per groep van Lokale Besturen
        - De 30 deelnemende Lokale Besturen worden verdeeld in 5 groepen van telkens 6 besturen op basis van geografische nabijheid.
    - Totaal (incl. BTW): **€ 47.916**
- 1 medium-level functioneel analist
    - Profielprijs (/dag, incl. BTW): € 962,57
    - Dit profiel is bezwaard met de ondersteuning, begeleiding en rapportering op het niveau van elke individuele integratie.
    - 10 mandagen per Lokaal Bestuur
        - Agentschap Binnenlands Bestuur heeft bepaald dat 30 Lokale Besturen kunnen deelnemen aan het project.
    - Totaal (incl. BTW): **€ 288.771**
- Totaal voor spoor 2 over beide profielen: **€ 337.000**

Eventuele bijkomende support vanuit het management, ondersteuningsteam of ontwikkel-team, kan plaatsvinden op afroep, maar hiervoor wordt geen budgettaire doorslag voorzien.

Governance:

Digitaal Vlaanderen rapporteert aan de stuurgroep van het Cyber Response Team over de voortgang van het project “ACM-IDM bij de Lokale Besturen”. Deze rapportering vindt plaats op het niveau van elk individueel bestuur dat deelneemt aan het project.

De stuurgroep van het CRT bepaalt in het kader van dit project de rapporteringsmodaliteiten en key performance indicators. Voor de hand liggend zijn bijvoorbeeld:

- Het aantal succesvolle integraties met ACM T&I, ACM PRD, IDM T&I en IDM PRD over de deelnemende besturen heen.
- Het aantal individuele besturen die een succesvolle integratie hebben opgezet in kader van dit project met ACM T&I, ACM PRD, IDM T&I en IDM PRD.

Vanuit het oogpunt van de evaluatie van de huidige dienstverlening van Digitaal Vlaanderen en eventuele, toekomstige conceptuele shift richting een dienstverlening die meer gestoeld is op 'hands on'-ondersteuning, worden volgende key performance indicators als waardevol beschouwd:

- De tevredenheid ten aanzien van de aangeboden ondersteuning voor, tijdens en na de integratietrajecten.
- De eagerness of gretigheid om in de toekomst in een gelijkaardige context andere toepassingen te integreren met de Veiligheidsbouwstenen.

Dit betreft voor een goed begrip geen exhaustieve doorslag van de toekomstige key performance indicators, maar slechts een initieel voorstel dat verder kan uitgebreid dan wel gereduceerd worden door Agentschap Binnenlands Bestuur.

3. Timing

Volgende activiteiten zullen worden uitgevoerd voor een periode van 12 maanden t.e.m. 31/12/2024.

Bijlage 2. Kostprijs en betalingsmodaliteiten

1. Kostprijs en detailberekening

Voor de verdere ondersteuning van lokale besturen door het CRT voorziet het Agentschap Binnenlands Bestuur een budget van 640.000 euro.

Onderstaande tabel betreft de indicatieve verdeling van het budget en de kosten door Digitaal Vlaanderen op basis van de vereisten die werden weergegeven in deze nota. De verdeling kan tijdens de duur van de samenwerkingsovereenkomst worden bijgestuurd op aangeven van de stuurgroep van het Cyber Response Team.

Activiteit	2023
Spoor 1: Begeleiding van lokale besturen bij het opmaken van een Business Continuïteitsplan	300.000€
Spoor 2: (Piloot-)begeleiding van lokale besturen bij de implementatie van Vlaamse bouwstenen m.b.t. Toegangs- en Gebruikersbeheer	340.000€
Totaal	640.000€

De coördinatie van beide opdrachten wordt opgenomen binnen de reguliere werking van het CRT.

Voor het uitwerken van spoor 1: begeleiding van lokale besturen bij het opmaken van een Business Continuïteitsplan', kan externe ondersteuning worden besteld op het raamcontract met referentie 2019/HFB/52630. Volgende prijszetting wordt gehanteerd:

	Prijs/dag (excl. BTW)	Prijs/dag (incl. BTW)
Profiel A	€746,02	€902,68
Profiel B	€882,69	€1.068,05
Profiel C	€1.127,57	€1.364,36
Profiel D	€2.847,39	€3.445,34

Voor het uitwerken van spoor 2: (Piloot-)begeleiding van lokale besturen bij de implementatie van Vlaamse bouwstenen m.b.t. toegangsbeheer (ACM/IDM), kan externe ondersteuning worden besteld op het raamcontract met referentie 2020/HFB/MPMO/63249. Volgende prijszetting wordt gehanteerd:

	Prijs/dag (excl. BTW)	Prijs/dag (incl. BTW)
Medium-level Business analist project manager	€792,00	€958,32
Medium-level functioneel analist	€795,52	€962,57

Digitaal Vlaanderen en het EV DV worden aangemerkt als niet-belastingplichtige publiekrechtelijke lichamen in de zin van artikel 6, eerste lid, van het BTW-wetboek en zijn bijgevolg niet onderworpen aan de BTW.

2. Facturatie- en betalingsmodaliteiten

Er wordt voor de beide sporen telkens een co-financiering van 20 % van de deelnemende lokale besturen gevraagd. Na het uitvoeren van de prestaties door de opdrachtnemer, zal het Eigen Vermogen Digitaal Vlaanderen een factuur aan de opdrachtgever bezorgen.

Betalingen aan de opdrachtnemer worden uitgevoerd op rekeningnummer BE86 3751 1175 0850, geopend op naam van het Eigen Vermogen Digitaal Vlaanderen.

Een betalingstermijn van 30 dagen is van toepassing.

Bijlage 3. Uitvoeringsmodaliteiten

1. Projectorganisatie

De operationele werking van het Cyber Response Team wordt verzekerd door Digitaal Vlaanderen, in samenwerking met het Agentschap Binnenlands Bestuur. De noden en behoeften van de verschillende belanghebbenden en partners (bv. VVSG) bij de respectieve deelprojecten worden bevraagd via bestaande fora van het agentschap Digitaal Vlaanderen.

De stuurgroep van het Cyber Response Team kan doorheen de opdracht de organisatie en allocatie van voorziene middelen op een andere manier dan hierboven beschreven inzetten om de vooropgestelde doelen te behalen.

De uitvoering van de opdracht zal plaatsvinden via de raamcontracten met referenties 2019/HFB/52630 en 2020/HFB/MPMO/63249.

2. Projectopvolging

De opvolging van de opdracht gebeurt via de stuurgroep van het Cyber Response Team, waarin vertegenwoordigers zetelen van Vlaams minister-president Jan Jambon en Vlaams viceminister-president en minister van Binnenlands Bestuur Gwendolyn Rutten, en van Digitaal Vlaanderen, Audit Vlaanderen en het Agentschap Binnenlands Bestuur, alsook de Vereniging van Vlaamse Steden en Gemeenten (VVSG). Digitaal Vlaanderen rapporteert op iedere stuurgroep over de geplande en gerealiseerde activiteiten en resultaten, alsook de tijdsbesteding en facturatie van interne en externe profielen per activiteit.

Waar nodig worden aanvullend specifieke projectstuurgroepen, werkgroepen en eventuele klankbordgroepen opgericht om maximaal te garanderen dat de opgeleverde resultaten beantwoorden aan concrete noden en behoeften van de beoogde doelgroepen (i.c. lokale besturen). Het Cyber Response Team voorziet de nodige coördinatie, indien van toepassing in samenwerking met relevante belanghebbenden en partners.

3. Communicatie

Over elke opdracht dient (intern en extern) te worden gecommuniceerd conform de te maken afspraken in de stuurgroep. In principe stellen alle partijen hun communicatiemiddelen en –kanalen ter beschikking.

Bijlage 4. Het advies van de Inspectie van financiën van 1/12/2023

Advies
IF_aanvullende opdra

Bijlage 5. Het advies van de Minister van Begroting van 18/12/2023

2023005033_Informat
ieveiligheid_Cyber_Res