**Samenwerkingsovereenkomst**

Cyberveilige Gemeenten – evaluatie en bijsturing project 'Cyberveilige Cloud infrastructuur voor 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 Audit Vlaanderen, Mark Vandersmissen.

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,

Audit Vlaanderen, 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 **Cyberveilige Gemeenten – evaluatie en bijsturing project 'Cyberveilige Cloud infrastructuur voor 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 op kwartaal gerapporteerd aan een de stuurgroep van het Vlaamse Cyber Response Team waarin vertegenwoordigers zetelen van Vlaams minister-president Jan Jambon en Vlaams viceminister-president en minister van Binnenlands Bestuur Bart Somers, en van Digitaal Vlaanderen, Audit Vlaanderen en het Agentschap Binnenlands Bestuur.

**Artikel 3. Kostprijs en betalingsmodaliteiten**

De totale kostprijs van de opdracht bedraagt 1.021.818 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/xx/xxxx en loopt tot 31/12/2025.

**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.

[handtekening]

Agentschap Digitaal Vlaanderen

Jan Smedts

Administrateur-Generaal

[handtekening]

Eigen Vermogen Digitaal Vlaanderen

Jan Smedts

Voorzitter beheerscommissie

[handtekening]

Audit Vlaanderen

Mark Vandersmissen

Administrateur-Generaal

**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. Concrete opdrachtomschrijving – verbintenissen van alle partijen***

## 1. Context

Evaluatie project Cloud Landingszone voor lokale besturen

De Vlaamse regering keurde eind 2022 het project 'Cyberveilige Cloudinfrastructuur voor lokale besturen' goed, met als doel het ontwikkelen van een proof of concept Cloudlandingszone voor lokale besturen. Dit project heeft anderhalf jaar gelopen en bleek niet evident, onder meer door het verschillend ICT-landschap bij de lokale besturen. De beveiliging van deze systemen is daarbij een belangrijk aandachtspunt. In sommige gevallen kunnen deze systemen niet aangepast worden om modernere beveiligingsmaatregelen toe te passen. Daarnaast stellen we vast dat de huidige raamcontracten op dit ogenblik voor deze hoogdringende problematiek geen oplossing bieden.

Uit workshops en gesprekken met de betrokken partijen werd echter duidelijk dat de dienstenleveranciers van onze lokale besturen het belang van moderne Cloudoplossingen erkennen en dat deze dienstenleveranciers inmiddels reeds initiatieven nemen om hun dienstverlening aan te passen aan meest moderne beveiligingsbehoeften.

De stuurgroep - met vertegenwoordiging van het kabinet van minister-president Jambon, het kabinet van minister van Binnenlands Bestuur Rutten, Digitaal Vlaanderen, Audit Vlaanderen en het Agentschap Binnenlands Bestuur - heeft de voortgang en realisaties van het project geëvalueerd en kwam tot de conclusie dat het verstandiger is om het voorbereidende studiewerk publiekelijk ter beschikking te stellen om zo in te zetten op verdere ontwikkelingen op de markt zonder daarbij de marktwerking te verstoren i.p.v. op termijn een afgescheiden testomgeving op te zetten waarin technologisch verouderde systemen een plaats zouden moeten krijgen.

De Vlaamse regering heeft daarom beslist het project af te ronden met een eindrapport met technische voorwaarden op basis van een gedetailleerde analyse. Het opzetten van een testconcept via een snel opzetbare Cloudlandingszone wordt niet verdergezet. Het eindproduct van het huidige traject wordt dus een rapport met de beschrijving van een Cloudnoodlandingszone met minimale beveiligingsmaatregelen als basisarchitectuur die door lokale besturen en hun dienstenleveranciers kunnen gebruikt worden ter evaluatie van hun eigen infrastructuur. Voor de effectieve realisatie kijken we naar de huidige dienstenleveranciers (en de daarbij afnemende lokale besturen).

Bijsturing project Cloud Landingszone voor lokale besturen

Het resterende budget van het project wordt aangewend om lokale besturen te begeleiden bij het verbeteren van het informatiebeveiligingsniveau. Dat doen we in de eerste plaats door een bruikbaar instrumentarium te ontwikkelen dat lokale besturen helpt bij het toepassen van het informatieclassificatieraamwerk (ICR). Verder ondersteunen en begeleiden we hen concreet in de eerste stappen van het toepassen van het ICR via een opleidingsprogramma. Tot slot verkennen we de mogelijkheden om toezicht/inzicht op de maturiteit wat betreft informatieveiligheid van deze doelgroep te monitoren via een haalbaarheidsstudie.

Dit laat de Vlaamse regering toe om kwetsbare lokale besturen te identificeren, na te gaan welke de meest gangbare en impactvolle beheersmaatregelen zijn binnen deze doelgroep en daar gepast op te ageren door middel van gerichte investeringen en ondersteuning.

Enerzijds willen we hiermee tegemoet komen aan de vaststellingen uit de ICT-veiligheidsaudits bij lokale besturen zoals beschreven in de initiële nota Vlaamse Regering van, namelijk dat:

- lokale besturen nog steeds moeite hebben met het identificeren en het beheersen van risico's op vlak van organisatiebeheersing en bedrijfscontinuïteit;
- lokale besturen in toenemende mate vragen om meer praktische ondersteuning met goede (technische) oplossingen.

Anderzijds geven we gevolg aan de vraag van o.a. VVSG en de besturen om het lokale niveau op een structurele en collectieve manier te coachen, begeleiden en ontzorgen door verschillende projecten beter op elkaar af te stemmen en geleerde lessen beter te delen.

## 2. Deliverables

<u>Ontwikkelen van een proceshandboek ICR voor lokale besturen</u>

Het toepassen van het informatieclassificatieraamwerk (ICR), impliceert dat het bestuur in de eerste plaats alle informatieverwerkingen inventariseert en de bijhorende '*informatieassets*' identificeert. Voor iedere informatieasset moet vervolgens een waardebepaling gebeuren conform de beschikbaarheids-, integriteits- en beschikbaarheidsvereisten.

In de voorbereiding van het beleidskader informatieveiligheid voor lokale besturen is reeds een beperkte pilootversie van een proceslijst opgemaakt om de haalbaarheid voor lokale besturen te onderzoeken. Hieruit blijkt dat voor lokale besturen organisatiebeheersing en de eerste stappen van het ICR geen evidente opgave zijn. Er blijken echter onvoldoende kennis- en ervaringsprofielen aanwezig te zijn binnen de lokale besturen om het inventariseren en prioriteren van processen en het definiëren van individuele informatieassets op een efficiënte manier aan te pakken. Dit heeft tot gevolg dat deze opdracht voor hen een zeer complexe en tijdsintensieve oefening. Aan de andere kant werken de lokale besturen volgens dezelfde basisverwerking en dienstverlening waardoor een groot deel van de processen van de lokale besturen gemeenschappelijk zijn. Het is dan ook niet wenselijk dat ieder lokaal bestuur voor zichzelf de mapping van identieke dienstverlening(en) individueel invult en bij wijze van spreken elk lokaal bestuur moet vertrekken van een wit blad.

Om lokale besturen zo veel mogelijk te ontzorgen bij het implementeren van het Vlaams ICR, wordt een generieke oplossing aangeboden om eigen kritieke processen te inventariseren, de informatieclassificatie (informatieassets) te definiëren en beoordelen volgens de informatieklassen van het ICR. Dit gebeurt in de vorm van een omvangrijk proceshandboek met reeds geïdentificeerde en beoordeelde processen en *informatieassets*. Dit is een concrete en cruciale eerste stap bij het toepassen van een overkoepelend veiligheidsbeleid en het verbeteren van de informatieveiligheid van lokale besturen.

De minimale maatregelen uit het Vlaamse ICR vormen de begeleidende documentatie. Ze bevatten de concrete kwaliteitscriteria waar de informatieverwerking van organisaties binnen de doelgroep aan moet voldoen. Bijvoorbeeld op vlak van gebruikers- en toegangsbeheer, fysieke beveiliging, netwerkinrichting en segmentatie, incident- en probleembeheer, toegangen voor beheerders, encryptie en encryptiesleutel beheer…

Deze maatregelen zijn tweeledig:

- Kwaliteitscriteria bij de inrichting van processen in relatie tot informatieveiligheidsbeheer. Dit aspect heeft een directe relatie met de reeds bestaande verwachtingen voor wat betreft organisatiebeheer.
- Kwaliteitscriteria bij gebruik van technische veiligheidsinrichting, volledigheid en effectiviteit.

Deze kwaliteitscriteria (gekend als minimale maatregelen in het veiligheidsbeleid) zijn onafhankelijk van organisatie of techniek opgesteld zodat er een maximale keuzevrijheid naar technologie en leverancier kan gegarandeerd worden bij de inrichting van de dienstverlening. Deze manier van werken is ook toegepast in het CyberFundamentals-veiligheidsraamwerk van het CCB. Het grootste verschil ligt in het feit dat het ICR ook de criteria uit andere wetgevingen (AVG, KSZ…) combineert tot een geheel in tegenstelling tot de CyberFundamentals die enkel focussen op de NIS2-regelgeving. Op die manier leggen we de complexe puzzel van criteria uit de verschillende wetgevingen als één geheel.

Om te garanderen dat de oplossing voldoende gedetailleerd is en voldoet aan de noden en verwachtingen van lokale besturen en ook effectief overeenkomt met de in het bestuur toegepaste realiteit, worden ook workshops met lokale besturen georganiseerd. Hiervoor wordt de methodiek van de pilootversie gevolgd om processen te inventariseren en noden te capteren. Aan de hand van de workshops wordt voor ieder proces een risicobeoordeling en overzicht van beheersmaatregelen voorgesteld. Dit kan enerzijds het overlopen van de reeds in de proceslijst gedefinieerde en gedocumenteerde processen zijn maar ook nieuwe processen die dan zullen worden toegevoegd aan de proceslijst. Geleerde lessen uit gelijklopende trajecten, zoals de aanvullende ondersteuning van het Vo-CRT voor het opmaken van een bedrijfscontinuïteitsplan, worden hergebruikt.

Daarnaast worden ook de vormvereisten van de oplossing- en koppelkansen met de lokale producten- en dienstencatalogus (LPDC) en het toekomstige open proceshuis onderzocht. Dit zijn reeds bestaande producten van ABB.

<u>Workshops voor lokale besturen ter ondersteuning bij de implementatie van het ICR</u>

Verder wordt eveneens een opleidingsprogramma ontwikkeld en aangeboden om het Vlaamse ICR en het ontwikkelde instrument kenbaar te maken bij lokale besturen. De inhoud van het opleidingsprogramma wordt verder afgestemd op maat van lokale besturen en moet ondersteunen bij de implementatie van het Vlaamse ICR, aan de hand van de ontwikkelde proceslijst. Dit houdt in dat het Cyber Reponse Team (Vo-CRT) interactieve sessies organiseert om lokale besturen concreet te helpen en begeleiden bij het doorlopen van zo'n oefening.

Haalbaarheidsstudie naar een Vlaamse GRC-tooling voor lokale besturen

Om de planlast voor lokale besturen m.b.t. documenteren en rapporteren van risicobeheersingsmaatregelen te beperkten, wordt eveneens de haalbaarheid van een Vlaamse Governance, Risk en Compliance (GRC)-tooling verkend. GRC-tools bieden organisaties de mogelijkheid om alle documentatie over controlemaatregelen overzichtelijk te centraliseren volgens een (gestandaardiseerde) template. Dit laat toe om gegevens over interne controle beter te beheren en analyseren maar ook om op een transparante, efficiënte en gestructureerde manier te rapporteren over de te nemen maatregelen en compliance. Hierbij gaat bijzondere aandacht naar compliance aan het Vlaamse ICR (incl. AVG, NIS2 en andere sectorale verplichtingen).

In dit traject wordt in eerste instantie de behoefte en haalbaarheid van een Vlaamse GRC-tooling onderzocht en worden vervolgstappen voor verdere ontwikkeling en operationalisering (bv. via raamcontracten) uitgewerkt.

## 3. Timing

Volgende activiteiten zullen worden uitgevoerd voor een periode van xx maanden t.e.m. 31/12/2025.

***Bijlage 2. Kostprijs en betalingsmodaliteiten***

**1. Kostprijs en detailberekening**

De investeringsmiddelen voorzien worden belast ten belope van € 1.021.818 VAK op het krediet dat bestemd was voor het project 'cyberveilige gemeenten' en in de begroting is ingeschreven op het artikel SB0-1SAC2ZZ-WT.

Onderstaande tabel betreft de indicatieve verdeling van de kostendoor Digitaal Vlaanderen op basis van de vereisten die zijn gesteld door de Vlaamse regering.

| **Activiteit** | **Budget (in euro)** |
|---|---|
| Ontwikkelen van een proceshandboek ICR voor lokale besturen | 500.000 |
| Organiseren van workshops voor lokale besturen ter ondersteuning bij de implementatie van het ICR | 321.818 |
| Haalbaarheidsstudie naar een Vlaamse GRC-tooling voor lokale besturen | 200.000 |
| **Totaal** | **1.021.818** |

Er zijn geen verdere recurrente kosten die voortvloeien uit dit project, aangezien het resterend budget van de initiële opdracht wordt ingezet om begeleiding en implementatie te voorzien van het Vlaamse ICR.

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**

Het voorstel van beslissing heeft geen directe weerslag op de werking of werkingsuitgaven van de lokale en provinciale besturen. 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. Projectcoördinatie

De operationele werking van het Cyber Response Team wordt verzekerd door Digitaal Vlaanderen, in samenwerking met het Agentschap Binnenlands Bestuur. Het Cyber Response Team (Vo-CRT) is de aangewezen partner omwille van de expertise over ICT-beveiliging en digitale oplossingen en de coördinatie van diverse initiatieven om de cyber- en informatiebeveiliging te verbeteren.

De noden en behoeften van de verschillende belanghebbenden en partners (bv. VVSG) bij de respectieve deelprojecten worden bevraagd via bestaande fora van Digitaal Vlaanderen.

De stuurgroep van het Cyber Response Team kan doorheen de opdracht bepalen 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 referentie 2023/HFB/OP/105639 of andere indien overeengekomen door beide partijen.

## 2. Projectopvolging

De opvolging van de opdracht gebeurt via de stuurgroep van het Vlaamse Cyber Response Team (Vo-CRT), waarin vertegenwoordigers zetelen van de Vlaams minister bevoegd voor digitalisering en de Vlaamse minister bevoegd voor Binnenlands Bestuur, alsook vertegenwoordigers van de agentschappen Digitaal Vlaanderen, Audit Vlaanderen en het Agentschap Binnenlands Bestuur en 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 aanvullende 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.