Samenwerkingsovereenkomst

Cyber Response Team voor de 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 **Cyber Response Team 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 moet tweemaal per jaar worden gerapporteerd aan een stuurgroep 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 1.000.000 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 23/12/2022 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.

[handtekening]

Agentschap Digitaal Vlaanderen

Jan Smedts

Administrateur-Generaal

[handtekening]

Eigen Vermogen Digitaal Vlaanderen

Jan Smedts

Voorzitter beheerscommissie

[handtekening]

Agentschap Binnenlands Bestuur

Jeroen Windey

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

Digitale instrumenten zullen nu en in de toekomst meer dan ooit het verschil maken in de lokale besturen. Dat vereist een sterke cyber- en informatieveiligheid.

Naar aanleiding van de informatieveiligheidsincidenten bij de lokale besturen Zwijndrecht, Antwerpen en Diest is gebleken dat lokale besturen kwetsbaar zijn voor hacking. Bij deze verschillende incidenten is de dienstverlening aan de burger door het betrokken lokaal bestuur gedurende enkele dagen tot enkele weken in belangrijke mate onderbroken en/of verstoord. Wanneer een lokaal bestuur geconfronteerd wordt met een cyberaanval of ander IT-gerelateerd incident, dienen op korte termijn diverse maatregelen genomen te worden om de situatie onder controle te krijgen en terug te keren naar de gewone werking. Proactief nadenken over de te nemen stappen faciliteert het crisisbeheer bij grootschalige incidenten.

Het bestrijden van cyberveiligheidsincidenten is jammer genoeg geen rechtlijnig proces, maar een complexe oefening waarbij diverse acties door elkaar lopen, gaande van het detecteren van een incident, tot het inperken van schade, het herstellen van de dienstverlening, melden aan de bevoegde instanties, rapporteren aan regulatoren en slotbeschouwing. Er is een belangrijke rol weggelegd voor ICT, maar al even belangrijk zijn de organisatorische inrichting en de uitvoering van het afsprakenkader die interne en externe communicatie en organisatiebeheersing faciliteren. Om lokale besturen hierin te ondersteunen, is in het kader van het actieplan cyberveilige steden en gemeenten een toolkit cyberveiligheid ontwikkeld door de VVSG met sjablonen, richtlijnen en checklists. Hiermee worden de nodige handvaten aangereikt aan lokale besturen om zich preventief voor te bereiden op eventuele cyberincidenten.

Gezien de complexiteit van deze materie is het voor vele lokale besturen niet haalbaar om zich hier tijdig op te organiseren en om alle nodige gespecialiseerde expertise aan boord te hebben. De kans is reeël dat een lokaal bestuur externe expertise zal moeten inroepen om het incident zo vlot en efficiënt als mogelijk aan te pakken. Bovendien gebeurt het niet elke dag dat cybercriminelen je dienstverlening en werking volledig dreigen plat te leggen. Daarnaast is een gecoördineerde kennisdeling tussen alle betrokken partijen een must.

De oprichting van een op Vlaams niveau aangestuurd Cyber Response Team (CRT) zorgt voor de nodige synergie en efficiënte inzet van middelen. Digitaal Vlaanderen en het agentschap Binnenlands Bestuur zullen de krachten bundelen en hun expertise inzetten om de lokale besturen optimaal te ondersteunen.

Via de Smart Region Board wordt het Agentschap Innoveren en Ondernemen en het Vlaams Departement Economie, Wetenschap en Innovatie op de hoogte gehouden van de werkzaamheden van het CRT.

2. Deliverables

Het Cyber Response team biedt een centrale ondersteuning vanuit de Vlaamse overheid ter ondersteuning van de lokale besturen. Deze ondersteuning is gefocust op de preventie van cyberincidenten als op remediëring en herstel. Het is van belang dat deze ondersteuning in het geval van een incident, kan leiden tot een concreet incidentresponseplan, dat rekening houdt met de context, aanwezige middelen, capaciteit en rollen binnen het lokaal bestuur.

Het CRT zet hiervoor de nodige beheerssystemen en rapportering op (gebaseerd op de bestaande tooling binnen Digitaal Vlaanderen) zodat we een vlotte, professionele dienstverlening kunnen garanderen en deze dienstverlening kunnen opvolgen en waar nodig bijsturen.

Deze aanpak voorziet een flexibele opschaling of afbouw van de activiteiten in functie van het dreigingsniveau, de actuele situatie van de incidenten. Dit voorstel vormt de basis voor een korte-termijn respons op de recente gebeurtenissen en vormen de basis van meer structurele maatregelen op langere termijn.

Het CRT-team bestaat uit volgende rollen en verantwoordelijkheden:

Coördinator (Expert / Part time)

- Verzekeren dat de juiste functies de nodige rollen vervullen.
- Verzekeren dat alle acties tijdig worden uitgevoerd door de verschillende rollen.

Mailbox Analyst (Junior / Part time)

- Monitoren van de centrale mailbox.
- Documenteren / centraliseren van de vragen van lokale besturen.
- Toewijzen van de vragen aan de relevante rollen.

IT / Cyber Expert (Expert, Junior / Part time**)**

- Behandelen van technische vragen (bv. best practices rond patch management, vulnerability tools, …).
- Verzamelen en verwerken van verslagen om geleerde lessen te trekken en te delen met lokale besturen, zoals o.a.:
  - Lessons learned rapporten van voorbije incidenten bij lokale besturen.
- Audit findings ihkv Cyber Veilige Gemeenten (Audit Vlaanderen).

Communicatie Expert (Expert, Junior / Part time**)**

- Behandelen van vragen rond communicatie.
- Voorbereiden van communicaties voor externe stakeholders (e.g., CCVO, lokale besturen, …)
- Opvolgen van (sociale) media rond lopende / nieuwe cyberincidenten bij lokale besturen.

Juridisch Expert (Expert / Part time)

- Behandelen van juridische vragen (bv. meldingsplicht, …).

Toolkit Analyst (Junior / Part time)

- Verzamelen en centraliseren van toolkits die lokale besturen toelaten om cyberincidenten te beheersen (bv. toolkit van CCVO, VVSG, CCB, …).

Liaison met overheden, overheidsdiensten en gerechtelijke instanties (Expert / part time)

- Monitoren en uitvoeren van acties waarbij interactie met overheden, overheidsdiensten en/of gerechtelijke instanties vereist is.

Dit team zal worden besteld op het raamcontract van Audit Vlaanderen m.b.t. ICT-audits. Volgende prijszetting wordt gehanteerd.

Profiel	**Senioriteit**	**Profiel raamcontract**	**Dagprijs (ex BTW)**
Coordinator & Comms	Senior Manager	Profiel D	€ 2.621,94
IT Cyber Expert (analyse)	Exp. SR Consultant	Profiel C	€ 1.038,29
Juridisch expert	Senior Consultant	Profiel B	€ 812,80
Toolkit Analyst	Junior	Profiel A	€ 686,95
Mailbox analyst	Junior	Profiel A	€ 686,95
Communicatie	Junior	Profiel A	€ 686,95

De capaciteit is flexibel en zal variabel zijn i.f.v. de werklast. We herevalueren even de samenstelling van het team i.f.v. de doelstelling.

Ondersteuning Cyber Response Team van de Vlaamse overheid

Het Cyber Response Team biedt een centrale ondersteuning vanuit de Vlaamse overheid ter ondersteuning van de lokale besturen. Deze ondersteuning is zowel gefocust op de preventie van cyberincidenten als op remediëring en herstel. Het is van belang dat deze ondersteuning in het geval van een incident, kan leiden tot een concreet incidentresponseplan, dat rekening houdt met de context, aanwezige middelen, capaciteit en rollen binnen het lokaal bestuur.

Het CRT zet hiervoor de nodige beheerssystemen en rapportering op (gebaseerd op de bestaande tooling binnen Digitaal Vlaanderen) zodat we een vlotte, professionele dienstverlening kunnen garanderen en deze dienstverlening kunnen opvolgen en waar nodig bijsturen.

Deze aanpak voorziet een flexibele opschaling of afbouw van de activiteiten in functie van het dreigingsniveau en de actuele situatie van de incidenten. Dit voorstel vormt de basis voor een kortetermijnrespons op de recente gebeurtenissen en vormen de basis van meer structurele maatregelen op langere termijn.

Remediëring en herstel

Het CRT biedt ondersteuning bij de opstart van een cyber responseplan. Dit cyber responseplan bestaat uit een stappenplan en een kader dat de geïmpacteerde partij onmiddellijk kan toepassen zodat de business continuïteit zo snel mogelijk hersteld kan worden. Dit plan is gebaseerd op beste praktijken in dit domein en in overeenstemming met de procedures en richtlijnen van toepassing binnen de Vlaamse overheid.

Het team bundelt alle beschikbare informatie vanuit de verschillende partners binnen zowel de federale (CCB) als Vlaamse Overheid (Digitaal Vlaanderen en het Agentschap Binnenlands Bestuur). Daarnaast worden ook verschillende externe partijen betrokken (VVSG, V-ICT-OR, ICT-dienstenleveranciers en andere ledenorganisaties), de vragen ontvangen van de lokale besturen, de bevindingen van Audit Vlaanderen en de input vanuit threat intelligence (specifieke case info en advies van het Centrum voor Cybersecurity België (CCB), de geheime diensten en Cyber Threat Intelligence van commerciële partijen).

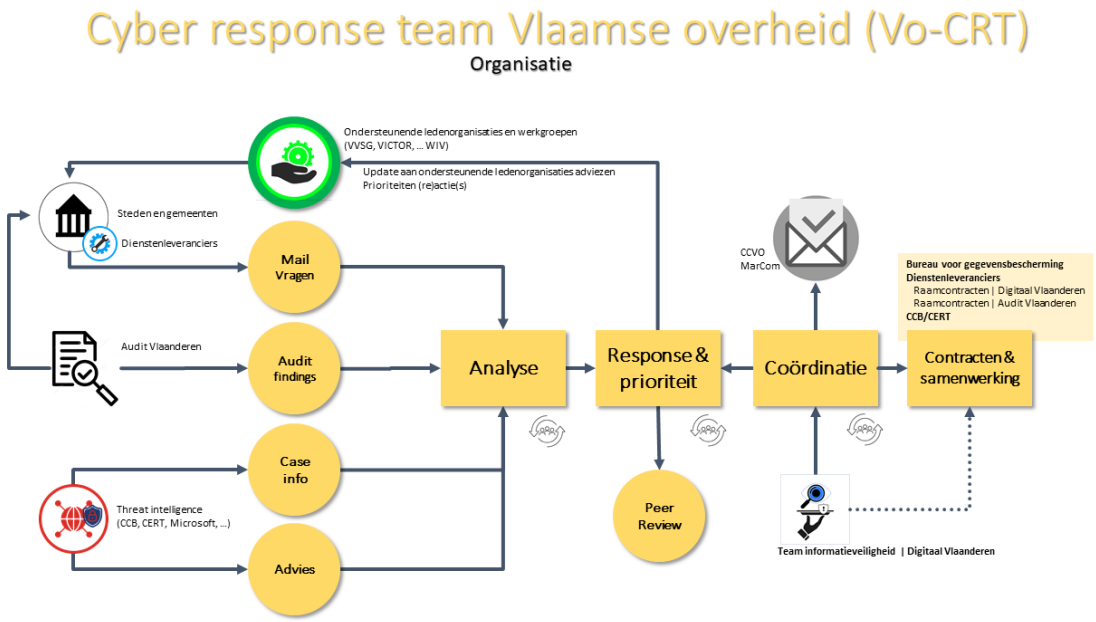
Het team analyseert de verzamelde informatie en bepaalt op basis daarvan de correcte response en prioriteit na afstemming met het VVSG en V-ICT-OR.

Verder coördineert het team de interne en externe communicatie naar alle belanghebbenden: waaronder geïmpacteerde partijen en de leidend ambtenaren van de Vlaamse Overheid.

Het team voert ook een analyse uit van de impact op de juridische en organisatorische relatie tussen de lokale besturen en de Vlaamse overheid (b.v. noodzaak van nooddecreten m.b.t. Omgevingsvergunningen). De bestaande draaiboeken (waaronder die van VVSG) worden hiermee verder uitgebreid. Nadien coördineert het team ook de nodige acties i.k.v de impact op de Vlaamse overheid.

Tenslotte zorgt het team voor de juridische begeleiding bij de te ondernemen stappen waaronder: informeren van de Gegevensbeschermingsautoriteit, het Bureau voor Gegevensbescherming van Digitaal Vlaanderen en de federale diensten.

Onderstaande figuur vat de taken en interacties van het CRT samen:



Preventief

Om nieuwe informatieveiligheidsincidenten te voorkomen, verzamelt het CRT de beschikbare informatie (actuele cases, informatie van het CCB, de geheime diensten en Cyber Threat Intelligence van commerciële partijen) en verwerkt deze informatie in nieuwe adviezen, dit in nauwe samenwerking met de ondersteunende ledenorganisaties.

Het team verspreidt deze adviezen naar de Vlaamse administratie en via de VVSG en andere ledenorganisaties (V-ICT-OR, VERA, …) naar de lokale besturen.

Het team capteert ook de noden van lokale besturen om extra dienstverlening en tools te ontwikkelen om de adviezen ook daadwerkelijk te implementeren.

We bieden snelle communicatie, kant-en-klare overeenkomsten, processen en procesbegeleiding aan met zowel gespecialiseerde cyber defense-organisatie als de dienstverlening en expertise van Digitaal Vlaanderen: Bureau voor Gegevensbescherming en Team Informatieveiligheid.

Lokaal ondersteuningsteam

Het CRT voorziet in een 'vliegend team' dat naar een lokaal bestuur dat getroffen is door een cyberaanval ter plaatse kan worden gestuurd. Er wordt dan gezorgd voor eerste contactname, coördinatie en begeleiding. Op die manier zal het CRT het getroffen lokaal bestuur vlot laten kennisnemen van bestaande draaiboeken en van het aanbod van CRT.

Het CRT zal opereren in nauwe samenwerking met onder andere het CCB en de politiediensten. Hun diensten zullen complementair zijn aan de diensten die worden aangeboden door het CCB.

Op vraag van het lokaal bestuur kan de ondersteuning verder gaan dan voorzien. Het CRT zal in dat geval een statement of work voorstellen en in functie van de opdracht contact opnemen met een beschikbare partner en een offerte aanbieden. Op vraag van het lokaal bestuur zal het CRT dan contact opnemen en de opdracht uitzetten bij de externe dienstverlener. De uitvoering gebeurt in nauwe afstemming met het CRT, zodat maximaal hergebruik en standaardisatie wordt bereikt.

Onderstaande figuur vat dit samen:

3. Timing

Volgende activiteiten zullen worden uitgevoerd voor een periode van 13 maanden t.e.m. 31/12/2023.

Bijlage 2. Kostprijs en betalingsmodaliteiten

1. Kostprijs en detailberekening

Voor de opstart van het Cyber Response Team en de operationele werking 2022-2023 is een budget nodig van in totaal 1.000.000 EUR opgedeeld zoals hieronder aangegeven. Hiervoor zal de kost op onderbenutte middelen van begroting 2022 gecompenseerd worden.

Onderstaande tabel betreft de detail van de kosten door Digitaal Vlaanderen op basis van de vereisten die werden weergegeven in deze nota.

Activiteit	2022 (eenmalig)	2023 (eenmalig)
Opstart ondersteunende tooling: Service Management		80.000 €
Curatieve en preventieve ondersteuning (1 maand in 2022)	120.000 €	
Curatieve en preventieve ondersteuning		700.000 €
Coördinatie		100.000 €

Voor de werking zal vanaf 2024 een jaarlijks recurrent budget nodig zijn. De business case hiervoor moet door het Agentschap Binnenlands Bestuur en Digitaal Vlaanderen nog worden opgemaakt en dit in nauwe samenwerking met het Lokaal Digitaal-team van Digitaal Vlaanderen (cfr. VR 2022 1507 VV DOC.0086/1).

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. De bijhorende raamovereenkomsten staan wel voor hen ter beschikking om in te zetten in de cyber response van hun ICT-dienstverlening. 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 uitvoering van het programma wordt verzekerd door Digitaal Vlaanderen. De noden en behoeften van de verschillende belanghebbenden bij de respectieve deelprojecten worden bevraagd via bestaande fora van het agentschap Digitaal Vlaanderen.

De uitvoering van de opdracht zal plaatsvinden via het raamcontract van Audit Vlaanderen m.b.t. ICT-audit activiteiten.

2. Projectopvolging

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).

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.