UPDATE

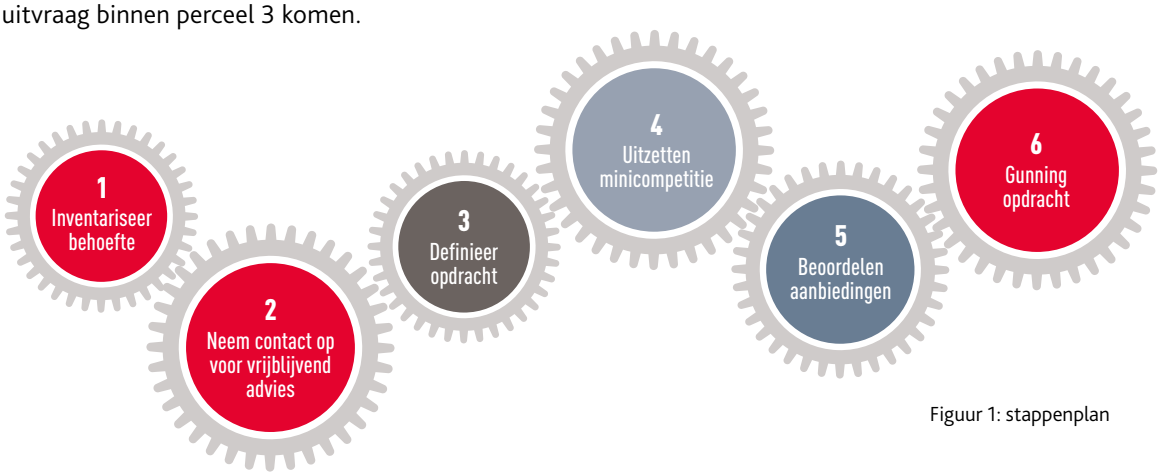
Stappenplan voor een succesvolle minicompetitie

GGI-Veilig perceel 3

De toenemende noodzaak voor gemeenten om informatiebeveiliging op orde te hebben, tezamen met de wens om slimmer en meer samen te werken, heeft ertoe geleid dat vanuit de Vereniging Nederlandse Gemeenten (VNG) een initiatief is gestart om een Gemeentelijke Gemeenschappelijke Infrastructuur (GGI) op te zetten. GGI-Veilig is daaruit voortgevloeid en faciliteert in het aanbestedingsproces waarmee gemeenten producten en diensten op het gebied van informatiebeveiliging af kunnen nemen.

In 6 stappen naar een succesvolle uitvraag

We merken dat het succesvol inkopen van cybersecuritydiensten en het selecteren van een passende leverancier niet eenvoudig is. Ook het aanbestedingsproces is niet altijd duidelijk. In dit stappenplan brengen we de te nemen stappen voor gemeenten in kaart, zodat zij effectief tot een succesvolle uitvraag binnen perceel 3 komen.



Figuur 1: stappenplan

Stap 1: inventariseer behoefte

Voordat u begint met een concrete uitvraag op het gebied van informatiebeveiliging of privacy, raden we u aan binnen uw eigen gemeente te inventariseren welke ondersteuningsbehoeften er in de toekomst zijn.

Door uw ondersteuningsbehoeften voor een langere periode in kaart te brengen en deze behoeften in één keer uit te vragen, brengt u de hoeveelheid benodigde aanvragen vermoedelijk terug. Dit scheelt tijd en verzekert u er bovendien van dat de benodigde ondersteuning tijdig geleverd kan worden. Een tijdige uitvraag resulteert immers in tijdige hulp. Dit laatste is met name relevant bij ondersteuning waarbij geen tijd verloren kan gaan, zoals hulp bij cyberincidenten.

Voor een dergelijke inventarisatie kunt u voor input bijvoorbeeld gebruik maken van de volgende bronnen:
- Uw jaarplan of meerjarenplan voor informatiebeveiliging (BIO) en/of privacy;
- De uitkomsten uit uw jaarlijkse ENSIA-evaluatie;
- Uw projectportfolio;
- Recent voorgevallen incidenten.

Naast een behoefte aan inventarisatie is het belangrijk te weten welke diensten exact binnen perceel 3 vallen. Naast de veelal technisch georiënteerde dienstverlening valt ook niet-technische ondersteuning voor informatiebeveiliging en privacy binnen perceel 3, zie figuur 2, tab Compliance. Denk hierbij aan de volgende ondersteuning:
- Uitvoeren van risicoanalyse(s) voor informatiebeveiliging;
- Opstellen meerjarenplan informatiebeveiliging;
- Implementatie van een Information Security Management System (ISMS);
- Vergroten awareness informatiebeveiliging;
- Uitvoeren van Data Protection Impact Assessments (DPIA's);
- Ondersteuning voor invulling van verschillende informatiebeveiligings- en privacyrollen.

Stap 2: neem contact op voor vrijblijvend advies

Nadat u voor uzelf inzichtelijk heeft welke behoeften uw gemeente op het gebied van informatiebeveiliging en privacy heeft, raden we u in stap 2 aan om nader kennis te maken met één of meerdere leveranciers binnen perceel 3. Dit stelt u in staat om:
- uw behoeften tezamen met de leveranciers verder aan te scherpen;
- meer inzicht te krijgen in de werkwijze van een leverancier;
- uiteindelijk uw wensen duidelijker te formuleren in de opdrachtbeschrijving, zoals:
  - benodigde senioriteit, bijvoorbeeld senior of een combinatie van junior/medior/senior;
  - doorlooptijd van de opdracht.

Daarnaast stelt dit de leverancier ook beter in staat om uw wensen te vertalen naar een passende aanbieding.

Stap 3: definieer opdracht

U vervolgt het proces door het definiëren van de opdracht in het aanvraagformulier. Hierin deelt u:
- De opdrachtomschrijving, inclusief duidelijke scope, en een contextomschrijving;
- Het op te lossen probleem;
- Uw eisen en wensen – gebruik de kennis opgedaan in stap 1 en 2;
- Het gewenste resultaat;
- De gewenste (start)data – definieer de eventuele maximale doorlooptijd en vraag in het geval van een spoedopdracht enkel relevante informatie, zodat leveranciers snel kunnen antwoorden.

Stap 4: uitzetten minicompetitie

Om één of meerdere producten en/of diensten uit perceel 3 af te kunnen nemen, dient u het proces van de minicompetitie te doorlopen met behulp van het 'aanvraagformulier minicompetitie', zoals behandeld in stap 3. In het proces zijn de volgende partijen betrokken:
- Gemeente als deelnemer;
- VNG Realisatie als opdrachtgever;
- Leveranciers GGI-Veilig perceel 3 als leveranciers.

Op de volgende pagina hebben wij de procedure schematisch voor u in kaart gebracht.

U kunt bij de administratieve afhandeling van de minicompetitie ondersteuning vragen bij het servicecentrum van VNG Realisatie via **scgemeenten.nl**.

Stap 5: beoordelen aanbiedingen

In deze stap beoordeelt u de ontvangen offertes. Op hoofdlijnen houdt u rekening met:
- Eisen – voldoet leverancier aan gestelde eisen?
- Kwaliteit – beoordeel de kwaliteit van het plan van aanpak. De beoordeling weegt voor 70% mee;
- Prijs – de prijs wordt beoordeeld door de VNG en weegt voor 30% mee.

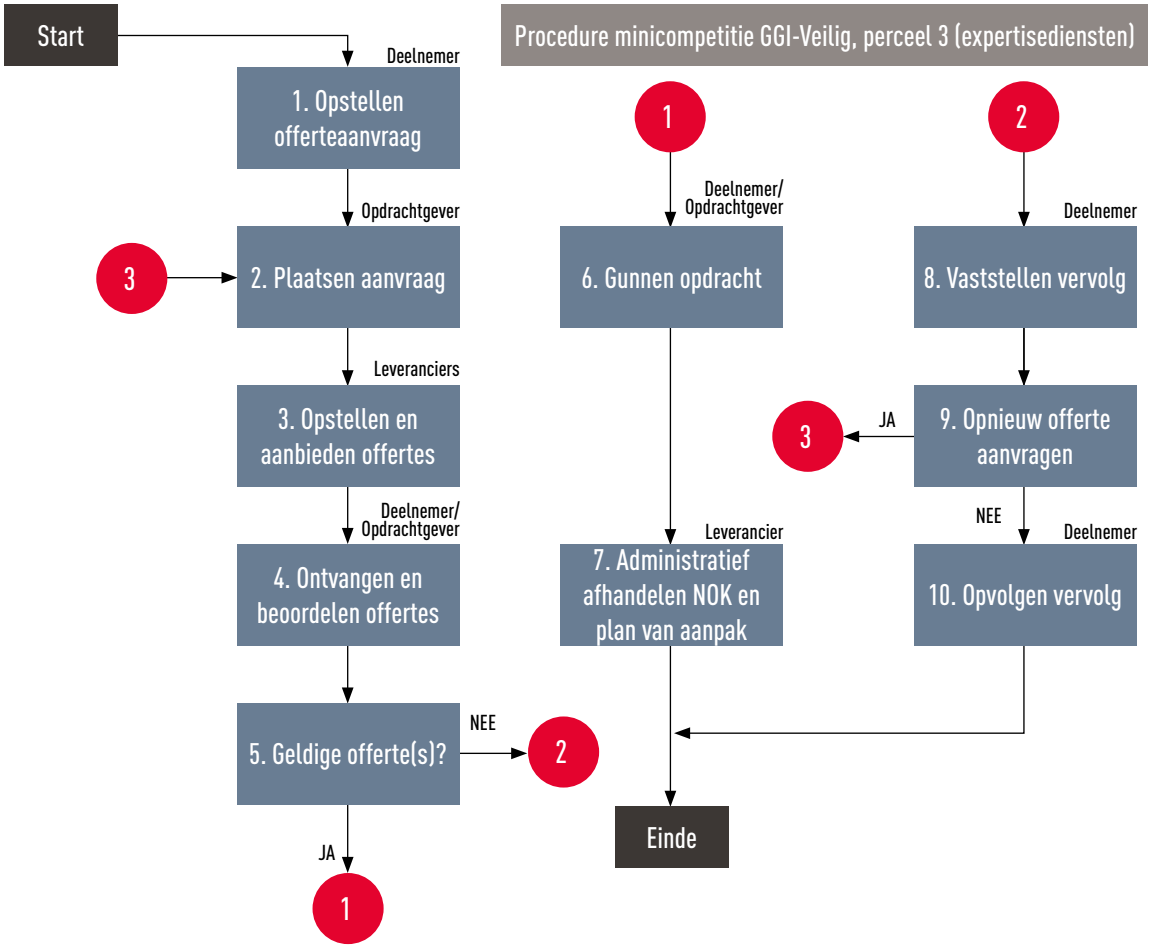
Dit leidt uiteindelijk tot een eindoordeel per ontvangen aanbieding.

Stap 6: gunning opdracht

U gunt de leverancier met de hoogste score uw opdracht. U hebt de aanbestedingsprocedure succesvol doorlopen en kunt gezamenlijk met de leverancier een officiële planning opstellen en starten met een kick-offmeeting.

Compliance Uitvoeren van compliancy scans/assessments/audits en aanbieden van ondersteuning op aandachtsgebieden BIO, BIG, AVG, ENSIA, ISO 900x en -270x.	**Pentesten** Uitvoeren van Ethical Hacking tests om mogelijke kwetsbaarheden in informatiesystemen inzichtelijk te maken.
Network hardening Onderzoeken van en adviseren over robuustheid van ICT-infrastructuren in gebruik bij gemeenten.	**Vulnerability** Uitvoeren van vulnerability scans/assessments op (het beheer van) de ICT-infrastructuur van gemeenten.
Forensics Levering van ondersteuning bij forensisch onderzoek n.a.v. securityincidenten.	**SIEM** Bieden van ondersteuning bij inrichting en uitvoering van SIEM-proces binnen gemeenten.

Figuur 2: leveranciers binnen perceel 3, waaronder BDO, leveren diensten op basis van zes gebieden



Figuur 3: proces minicompetitie

Meer informatie?

Neem contact op met een van onze adviseurs om tezamen met u het gesprek aan te gaan over uw behoeften op het gebied van informatiebeveiliging en privacyondersteuning.

Frank van der Lee
Partner BDO Advisory
T 06 – 11 00 31 17
E frank.van.der.lee@bdo.nl

Kees Plas
Partner BDO Advisory
T 06 – 53 59 85 13
E kees.plas@bdo.nl

Jeffrey de Bruijn
Senior Manager Cybersecurity
T 06 – 24 92 11 97
E jeffrey.de.bruijn@bdo.nl

07/2020 - PS2012

Vond u dit interessant? Ontvang - net als 17.000 andere organisaties - het laatste nieuws over bijvoorbeeld actuele publicaties en onderzoeken, fiscale regelgeving en wetswijzigingen tweewekelijks in uw mailbox! Meld u aan via **bdo.nl/nieuwsbrief**.