



Algemeen Verslag Marktconsultatie

GRC-Tool

gemeente Eindhoven

Uitgave

Gemeente Eindhoven

Datum

15-08-2023



Inhoud

1 Inleiding	3	
1.1 Algemeen		3
1.2 Openbaarheid van de marktconsultatie		3
1.2 Nota van inlichtingen		3
1.3 Inschrijvingen		3
2. Resultaten	4	
2.1 Beantwoording vragen		4
3. Ten slotte	13	



1 Inleiding

1.1 Algemeen

Voorafgaand aan een mogelijke aanbesteding voor een 'GRC Tool' heeft de gemeente Eindhoven op 7 December 2022 een marktconsultatiedocument gepubliceerd op het aanbestedingsplatform TenderNed, kenmerk: 390060.

Met als doel voorafgaand aan een eventueel formeel aanbestedingsproces, wederzijds vrijblijvend en openbaar informatie verkrijgen vanuit de markt. De verkregen informatie zal mogelijk gebruikt worden bij het verder specificeren van de mogelijke opdracht(en) en bij de keuze(s) van de aanbestedingsvorm(en) c.q. contractvormen. Op deze wijze kan/kunnen de aan te besteden opdracht(en) afgestemd worden op de mogelijkheden die er zijn in de huidige markt. De marktconsultatie was vrij toegankelijk voor geïnteresseerde marktpartijen.

1.2 Openbaarheid van de marktconsultatie

In dit document schetst de Aanbestedende dienst een overzicht van de uitgevoerde marktconsultatie. Hiermee geeft de Aanbestedende dienst invulling aan het zorg dragen voor een 'level playing field'. In overeenstemming met de bepalingen uit het Marktconsultatiedocument geeft de Aanbestedende dienst in dit verslag een overzicht van de belangrijkste bevindingen uit de marktconsultatie. De Aanbestedende dienst heeft bij het opstellen van dit verslag zorg gedragen voor:

- Het anonimiseren van de verstrekte informatie, zodat deze nooit te herleiden zal zijn naar de betreffende marktpartij;
- Het vermijden van het opnemen van bedrijfs- en/of commercieel gevoelige gegevens;
- Het dermate veralgemeniseren van de resultaten en conclusies dat nooit te herleiden is welke informatie expliciet door de deelnemende partijen verstrekt is.

1.2 Nota van inlichtingen

Naar aanleiding van het marktconsultatiedocument hebben leveranciers de mogelijkheid gehad vragen te stellen. Op 22 december 2022 heeft de gemeente Eindhoven de antwoorden op de gestelde vragen op TenderNed gepubliceerd door middel van een nota van inlichtingen.

1.3 Inschrijvingen

De marktconsultatie sloot voor de inschrijvers op 18 januari 2023. In totaal hebben elf marktpartijen deelgenomen aan de schriftelijke marktconsultatie.

De gemeente heeft op basis van de verkregen schriftelijke informatie vier partijen uitgenodigd om een presentatie te geven.



2.0 Resultaten

Hieronder zal de gemeente Eindhoven een samenvatting geven van de antwoorden van de inschrijvers op de gestelde vragen in het marktconsultatie document. Door de veelheid aan verkregen informatie kan het voorkomen dat antwoorden met eenzelfde strekking zijn samengevoegd.

2.1 Beantwoording vragen

BEDRIJF:

Algemeen

Vraag 1: Geef wat algemene (contact) informatie van uw organisatie (naam contactpersoon, functie, telefoonnummer, e-mail adres, website etc.).

Alle leveranciers hebben naar tevredenheid algemene informatie van de organisatie toegevoegd.

Bedrijfskenmerken

Vraag 2: Geef een korte beschrijving van uw organisatie (historie, aantal medewerkers, onderscheidend vermogen t.o.v. andere partijen in de markt.)

Alle leveranciers hebben naar tevredenheid een korte beschrijving van de organisatie toegevoegd. Doordat in de antwoorden bedrijfsgevoelige, onderscheidende kenmerken worden benoemd kiest aanbestedende dienst ervoor om niet op deze antwoorden in te gaan.

OPLOSSING:

Product

Vraag 1: Kunt u een korte beschrijving geven van het product/de oplossing die u kunt bieden?

Alle leveranciers hebben hier een duidelijke beschrijving van het product/de oplossing gegeven.

Onderstaande aspecten sprak de aanbestedende dienst aan:

- Begeleiding bij organisatorische verandering;
- Ter beschikking hebben van een plug-and-play applicatie;
- Geautomatiseerde data import;
- Applicatie die standaard voorziet in alle functionaliteiten voor het documenteren van regelgeving;
- Real-time inzicht;
- Aanbieden van meerdere/verschillende modules;
- Mogelijkheid tot uitbreiden van de dashboards.

Compliance

Vraag 2: Eindhoven beheerst haar compliance risico's via drie lijnen: (1) de lijn van de bedrijfsvoering (of Lijnmanagement), (2) de lijn van de Compliance Functie (en andere tweedelijnsfuncties) en (3) de lijn van interne audit. Het drielijnenmodel maakt onderscheid tussen:

- 1) **Funcities die risico's hebben en beheren,**
- 2) **Funcities die risico's overzien en**
- 3) **Funcities die onafhankelijke zekerheid bieden.**

Hoe ondersteunt uw oplossing de functiescheiding tussen deze lijnen?

Als belangrijkste oplossingen voor functiescheiding tussen de drie lijnen wordt onderstaand benoemd:

- Per lijn meerdere rollen en rechten beschikbaar;
- Lijnmanagers op een laagdrempelige manier betrokken bij het intern beheersingsproces;
- Risico- en auditmodules hanteren;
- Alle medewerkers een rol toekennen;



- Hanteren van geautomatiseerde workflows die medewerkers uit alle lijnen kunnen attenderen op openstaande taken;
- Per rol definiëren welke dashboards en functionaliteiten de gebruiker dient te hebben.

In Control Statement

Vraag 3: Eindhoven beschrijft in de gewenste situatie de kapstok om te komen tot een managementverklaring (In Control Statement) over de zeven managementaandachtsgebieden. Kunt u beschrijven in hoeverre deze gewenste situatie aansluit bij de functionaliteiten van uw oplossing? En kunt u een voorbeeld aanleveren van een managementverklaring (In Control Statement) die uit uw systeem komt en aansluit bij de beschreven behoefte van Eindhoven?

De antwoorden van de betrokken onderneming lagen ver uit elkaar. Het algemene beeld is dat de aanbieders/oplossingen vrij flexibel zijn in het naar wens van de gemeente inrichten van tool, dashboards en rapportagevormen. dat zal dan om maatwerk vragen, echter het is wel technisch mogelijk. Onder andere werd gezegd dat:

- Het is mogelijk ICS te downloaden in PDF-format;
- Mogelijkheid verklaring te genereren in de oplossing. Deze verklaring beschrijft voor welke onderdelen de organisatie aantoonbaar 'in control' is;
- ICS kan niet in de oplossing gegenereerd worden. Alle informatie kan uit de oplossing geëxporteerd worden en geanalyseerd met Excel;
- een GRC-tool is een hulpmiddel, uiteindelijk moet gemeente Eindhoven het als organisatie een ICS opstellen.
- Om aantoonbaar in control te zijn bieden we per module managementoverzichten, maar ook een totaaloverzicht van de gehele waardeketen.

Toekomst

Vraag 4: Wat zijn de plannen voor de ontwikkeling van uw oplossing? Geef hierbij aan hoe u omgaat met eventuele wettelijke wijzigingen. Welke functionele uitbreidingen zijn te verwachten?

In het kader van het vermijden van het opnemen van bedrijfs- en/of commercieel gevoelige gegevens van de betrokkenen zullen geplande ontwikkelingen, strategie van omgaan met wettelijke wijzigingen en de te verwachten functionele uitbreidingen niet worden gedeeld.

Kansen

Vraag 5: Welke kansen (minimaal 2) biedt uw oplossing die meerwaarde bieden voor opdrachtgever? Waarin onderscheid uw oplossing zich ten op zichte van de concurrentie?

In het kader van het vermijden van het opnemen van bedrijfs- en/of commercieel gevoelige gegevens worden de benoemde kansen door betrokkenen niet gedeeld.

Referenties

Vraag 6: Bij welke organisatie(s) wordt uw oplossing gebruikt? Benoem een aantal referenties (bij voorkeur gemeenten). En geef contactgegevens bij deze referentieopdrachten zodat contact opgenomen kan worden.

In het kader van de Anonimiteit van de inschrijvers zullen referentie projecten niet worden gedeeld.

IMPLEMENTATIE:

Implementatieduur en impact

Vraag 1: Voor de planning van het traject is inzicht in de benodigde duur voor de implementatie nodig. Wat is een realistische implementatie duur bij een gemeente gelijkwaardig qua grootte



als de gemeente Eindhoven? Houd hier rekening met benodigde koppelingen, systeem inrichting, conversie en migratie van data en training van medewerkers.

- Een leverancier geeft aan dat het inrichten, koppelingen opzetten en conversies maken ongeveer 3 tot 6 weken in beslag neemt;
- Een realistische, haalbare en tegelijkertijd ambitieuze implementatieduur is op basis van de huidige informatie nog lastig in te schatten. Uit ervaring merken we dat het gebruikelijk is dat een implementatie gefaseerd verloopt. In de regel in volgtijdelijke fases van 6 maanden. Naast de implementatie fase kent aanbieder ook nog de nazorg- en beheerfase gedurende het toekomstige gebruik van de software. De implementatie richt zich op het technisch en functioneel gereed maken van de oplossing en het komen tot de start van de planning & control cyclus om toe te werken naar een In Control Statement.
- Een leverancier geeft aan in deze fase nog geen inschatting te kunnen maken;
- Een leverancier schat een doorlooptijd van 4 tot 5 maanden in;
- Een leverancier geeft aan: "voor een dergelijk traject maken we gezamenlijk een gedetailleerd Plan van Aanpak. Onze aanpak kenmerkt zich door gezamenlijk alle stappen uit te voeren. Dit betekent dat we tijdens het project mensen meenemen en opleiden en daar ondersteuning bij bieden. De ervaring leert dat het project tussen 6 en 9 maanden tijd zal vragen. Wij gaan een resultaatverplichting aan die wordt beschreven bij het projectplan. De doorlooptijd is ook afhankelijk van de gewenste koppelingen, van migratie van data en de hoeveelheid betrokken professionals";
- Een leverancier geeft aan dat de ervaring leert dat een periode van 2-3 maanden reëel is om implementatie op een niveau te hebben dat de eigen organisatie daar met voldoende vertrouwen zelf mee aan de slag kan.

Fasering

Vraag 2: De gemeente wil de oplossing uiteindelijk gemeente breed implementeren. Dit zal impact hebben op de gehele organisatie. Enkele sectoren/afdelingen zullen nog na moeten denken over de invulling van hun managementaandachtsgebied alvorens aan de slag te gaan met de toekomstige applicatie. Terwijl andere sectoren/afdelingen hier al een duidelijk beeld bij hebben en direct aan de slag willen om dit te vertalen in een applicatie. Wat adviseert u als aanpak voor de implementatie van de oplossing en de organisatie hierin goed mee te nemen?

De leveranciers gaven het volgende aan:

- Wij adviseren ook niet om direct de hele gemeente te implementeren, maar hier onderscheid per afdeling/team in te maken. Begin bijvoorbeeld met de afdeling Automatisering en IT of P&O en implementeer dit eerst. Vanuit deze 'voorbeeld'-afdeling kan dan de ervaring mee worden genomen in de volgende afdelingen/teams. Zo leert de organisatie van zichzelf en collega's.
- Een goed fundament in de vorm van een implementatieconcept is hiervoor van belang, zodat de inrichtingsarchitectuur voldoende draagkracht heeft voor het uiteindelijke GRC gebouw. Randvoorwaarde is een goed implementatieconcept dat aan het begin van het project wordt vastgelegd en op details kan worden bijgesteld.
- Een leverancier adviseert een gefaseerde doch geïntegreerde aanpak over silo's heen. Uniformeren van werkwijzen, integreren van werkstromen, uitfasen van puntoplossingen. Daarmee wordt voorkomen dat degenen die vooruitlopen en snel hun richting bepalen onbedoeld belemmeringen opwerpen voor teams die trager of zorgvuldiger te werk gaan.
- Een leverancier adviseert om te starten met de afdelingen waar de verantwoordelijkheden het meest decentraal zijn belegd. Dit kan men gebruiken als een blauwprint voor de rest van de organisatie. Hierna kan ook de inrichting worden gerealiseerd voor de overige afdelingen. Indien nodig kunnen de verantwoordelijkheden en vragenlijsten hiervoor ook op een centraler niveau



worden belegd. Aan de hand van een groeimodel kan men de verantwoordelijkheden later steeds decentraler beleggen.

- De belangrijkste randvoorwaarden voor de succesvolle ingebruikname van de applicatie ziet een leverancier als volgt:
 - Vanuit de gemeente Eindhoven zijn er voldoende mensen beschikbaar tijdens het implementatieproces voor het valideren en testen van de omgeving;
 - Vanuit gemeente Eindhoven is er bereidheid tot verandering.
- Een leverancier biedt een full service en selfservice implementatievorm aan.

Verwachte capaciteit

Vraag 3: Kunt u een indicatie geven wat de verwachte inzet (in uren) is voor:

- inrichten van het systeem

- operationaliseren van het systeem

De meeste leveranciers gaven in geen goede indicatie te kunnen geven op basis van de informatie die gemeente Eindhoven gedeeld heeft. Enkele leveranciers gaven het volgende aan:

- De verwachting is dat voor inrichten en structureel beheer van de oplossing 2-4 uren per maand nodig is;
- Een leverancier geeft aan functioneel beheerders op te leiden met wie we samen het systeem configureren. De basis configuratie vraagt relatief weinig tijd (20 tot 40 uur); na de basis configuratie zullen de applicatiebeheerders op vraag stap voor stap het systeem naar eigen inzicht kunnen uitbreiden;
- Een leverancier geeft aan op basis van zijn ervaring in soortgelijke trajecten, vraagt een implementatieproject ca. 25-30 consulting dagen om het systeem gereed en de key-users en functioneel beheerders getraind te hebben voor verdere uitrol in de organisatie.
- Voor de inrichting en implementatie is een investering in uren van leverancier van gemiddeld 120 tot 140 uur nodig. De implementatie duur is afhankelijk van beschikbaarheid en tempo van de gemeentelijke organisatie.

KOSTEN:

Licentiemodel

Vraag 1: Welk licentiemodel wordt gehanteerd? Welke kosten behoren bij de verschillende onderdelen/modules in het licentiemodel?

In het kader van het vermijden van het opnemen van bedrijfs- en/of commercieel gevoelige gegevens worden de benoemde prijzen door betrokkenen niet gedeeld.

De leveranciers geven het volgende aan:

- Een leverancier geeft aan dat de aangeboden prijs altijd maatwerk is en wordt aangeboden op basis van de behoeften van gemeente Eindhoven;
- Een leverancier geeft aan met een basisplatform te werken. Het is mogelijk om per gewenst thema normenkaders te activeren, deze kaders nemen ook een jaarlijkse vergoeding met zich mee;
- De licentievormen zijn gebaseerd op een SaaS-oplossing;
- Enkele leveranciers geven aan met staffelprijzen te werken per user;
- Een leverancier geeft aan een degressief licentiemodel te hanteren.

Kosten

Vraag 2: Met in achtneming van het antwoord op de andere vragen, kunt u een inschatting geven van de totale kosten (TCO) van aanschaf, implementatie, beheer en onderhoud van de oplossing? Graag de benoemde onderdelen separaat benoemen



In het kader van het vermijden van het opnemen van bedrijfs- en/of commercieel gevoelige gegevens worden er geen kosten gedeeld van afzonderlijke inschrijvers.

Kostendragers

Vraag 3: Welke aspecten (technisch en/of qua dienstverlening) hebben een sterk kostenverhogend effect?

De volgende aspecten worden door de leveranciers benoemd:

- Aantal gebruikers;
- Opslag;
- Maatwerk/consultancy uren;
- Trainingen;
- Verandermanagement;
- Specifieke configuratie voor gemeente Eindhoven;

Functioneel beheer

Vraag 4: Onze voorkeur gaat uit naar een cloud/saas oplossing. Hoe wordt het functioneel beheer door u geleverd en als dat niet mogelijk is wat is uw inschatting van benodigde capaciteit voor functioneel beheer?

Hoe ziet een samenwerking op de beheeractiviteiten vanuit uw organisatie en beheer van de gemeente Eindhoven eruit?

Alle leveranciers gaven aan een SaaS-oplossing aan te beiden. Op het gebied van functioneel beheer en samenwerking gaven zij het volgende aan:

- Functioneel beheer kan voor een gedeelte uit handen genomen worden. Hiervoor zullen dan SLA-afspraken gemaakt dienen te worden o.b.v. het programma van eisen;
- Door het aanbieden van een SaaS-oplossing is er minimale inspanning vanuit gemeente Eindhoven nodig. De inschatting is tussen de 2-4 uur per maand;
- Mogelijkheid om functioneel beheer middels een FaaS model onder te brengen bij een businesspartner;
- Doordat leverancier verantwoordelijk is voor het actualiseren van de content, wordt ook het functioneel beheer voor een deel uit handen genomen;
- Gemiddeld genomen neemt het functioneel beheer 3 uur per week in beslag;
- Functionele applicatie beheer na implementatie ligt binnen uw organisatie en zal zich in de praktijk beperken tot enkele uren per maand.

FUNCTIONALITEIT

GRC-procesketen

Vraag 1: Kunt u aangeven in hoeverre de oplossing de geschetste GRC-procesketen en informatiestromen kan ondersteunen en invulling kan geven aan de architectuurcomponenten uit bijlage 2?

De meeste leveranciers gaven aan de architectuur uit bijlage 2 te kunnen ondersteunen. De leveranciers gaven o.a. het volgende aan:

- De geschetste GRC-procesketen wordt door de oplossing geheel ondersteund;
- De architectuur is vrij logisch en gebruikelijk;
- Het volledige proces wordt ondersteund met behulp van de aangeboden applicatie.



Normen en kaders

Vraag 2: Kunt u kort beschrijven of en hoe de oplossing in staat is om te ondersteunen bij het toetsen van de opzet, bestaan en werking van onderstaande kaders en frameworks:

- AVG en Archiefwet
- NEN-ISO 15489 en NEN-ISO 16175
- Baseline Informatiehuishouding Gemeenten (BIO)
- Kwaliteitssysteem Informatiebeheer Decentrale Overheden (KIDO)
- Referentiekader Opbouw Digitaal Informatiebeheer (RODIN)
- Intern beleid

Leveranciers gaven aan dat de tijdens de implementatiefase normenkaders vastgesteld/ingevoerd kunnen worden. Daarnaast gaven leveranciers o.a. het volgende aan:

- De volgende normenkaders zitten in de oplossing: AVG-VNG, DigiD, BGT, KIDO, WPG, RVIG reisdocumenten en BRP, BIO, BAG, AVG-NOREA, SUWI, ENSIA Reisdocumenten en BRP;
- Met behulp van koppelingen kan de vraagstelling AVG en ISO15489 geautomatiseerd worden ingevoerd;
- Overige kaders kunnen middels een Excel-format worden geïmporteerd.

Uniformiteit en flexibiliteit

Vraag 3: Kunt u uw visie beschrijven tussen enerzijds het creëren van een uniforme GRC-werkwijze tussen de benoemde managementaandachtsgebieden en anderzijds het bieden van flexibiliteit binnen de managementaandachtsgebieden om eigen inricht keuzes te maken? Kunt u ook aangeven in hoeverre het mogelijk is om de GRC-functionaliteiten flexibel in te richten binnen de verschillende managementaandachtsgebieden of sectoren?

De volgende aspecten worden door de leveranciers benoemd:

- Een leverancier geeft als visie het bereiken van een stabiele beheerorganisatie;
- Een leverancier geeft aan een flexibele technologie aan te bieden met behoud van de volledige audit trail;
- Een leverancier geeft aan geen specifieke uniforme werkwijze te hanteren;
- Een leverancier geeft aan dat keuzes m.b.t. inrichten tijdens de implementatie in samenwerking met de projectgroep worden gemaakt;
- Een leverancier geeft aan dat de oplossing de mogelijkheid biedt om generieke en specifieke invullingen te creëren;
- Uniformiteit in de werkwijze in de oplossing op alle managementgebieden is nodig om tot een In Control Statement te kunnen komen. Echter is het begrijpelijk dat elk managementonderdeel flexibiliteit wenst om eigen inrichtingskeuzes te kunnen maken.

Risico register

Vraag 4: De IV-organisatie is bezig om op strategisch, tactisch en operationeel niveau haar risico's in kaart te brengen. Een voorbeeld van het risico-register op operationeel/tactisch niveau is in bijlage 3 opgenomen. Ondersteunt uw oplossing het in kaart brengen van alle drie deze niveaus van risico's en zo ja, hoe?

Alle leveranciers geven aan dat hun oplossing het in kaart brengen van alle drie de niveaus ondersteunt. Daarnaast gaven leveranciers o.a. het volgende aan:

- Een leverancier geeft aan dat het door gemeente Eindhoven aangedragen voorbeeld in bijlage 3 volledig ondersteund wordt door aanbieder. Onderscheidend en uniek is dat de risico module gekoppeld kan worden aan informatie uit de normenkaders in de basismodule;
- De 3-lagen structuur die het meest wordt toegepast komt default terug in gestandaardiseerde oplossingen;



- De risico's kunnen worden geïnventariseerd en geclassificeerd op het niveau van strategisch, tactisch en operationeel. Hier kan vervolgens ook op gefilterd worden in het risicoregister.
- Risico's worden geselecteerd uit de oplossing-risicobibliotheek en worden toegepast op de verschillende op de organisatie (strategisch), assets of processen (operationeel en tactisch).

COMPABILITEIT

Architectuur

Vraag 1: In hoeverre is de architectuur gebaseerd op open en de facto standaarden?

Leveranciers geven het volgende aan in hoeverre de architectuur gebaseerd is op open de facto standaarden:

- De architectuur is gebaseerd op marktconforme best-practices voor webapplicaties;
- Een leverancier geeft aan dat hij het Manifest Common Ground heeft ondertekend;
- Een leverancier geeft aan de software ontwikkeld te hebben met standaard architectuur;
- Een leverancier geeft aan het platform onder meer gebaseerd te hebben op IT4IT;
- Een leverancier geeft zo veel mogelijk open en de facto standaarden te gebruiken en kijken continu of deze vernieuwd moeten worden;
- Een leverancier geeft aan gebruik te maken van markup standaarden;
- Een leverancier geeft aan te streven naar de open standaard.

Koppelbaarheid

Vraag 2: Welke standaarden voor gegevensuitwisseling met andere applicaties ondersteunt uw oplossing?

Ondersteunt de oplossing de volgende standaarden vanuit de GEMMA referentiearchitectuur? En zo ja welke.

Leveranciers geven o.a. onderstaande antwoorden op deze vraag:

- De oplossing ondersteunt het importeren van vragen vanuit ENSIA, dit kan via CSV of Excel. Wij hanteren GEMMA niet bij het ontwikkelen van onze oplossingen.
- Aanbieder is ondertekenaar van het Manifest Open Standaarden van het Forum Standaardisatie en van het Manifest Common Ground van VNG. Aanbieder staat ook vermeld in de GEMMA softwarecatalogus.
- De oplossing ondersteunt uitwisseling d.m.v. een (REST) API. De API ondersteunt de standaard HTTP(S) methodes (GET, POST, PUT en DELETE). De oplossing is niet ontwikkeld op basis van de GEMMA referentiearchitectuur;
- Momenteel zijn er nog geen geautomatiseerde gegevensuitwisselingen mogelijk met andere applicaties;
- De oplossing ondersteunt de GEMMA.

Data conversie

Vraag 3: In de huidige situatie worden verschillende soorten GRC-informatie vastgelegd in verschillende systemen alsmede ook in kantoorautomatisering. Het doel van de gemeente Eindhoven is om alle GRC informatie in één informatiesysteem onder te brengen. In hoeverre is het mogelijk de bestaande gegevens te converteren naar uw oplossing. Welke voorwaarden stelt u daarbij? Welke problemen/risico's ziet u?

- Meerdere leveranciers geven aan te beschikken over importmogelijkheden middels Excel;
- Een leverancier geeft aan eigen importbestanden te hanteren met duidelijke uitleg;
- Een leverancier geeft aan dat de meest voorkomende bestandstypen zoals MS Office, Visio, PDF, afbeeldingen kunnen (in bulk) geïmporteerd worden;



- Een leverancier geeft aan dat importeren van gegevens uit Word en Excel mogelijk is. Verder is het mogelijk via een eenvoudige tabelstructuur gelijksoortige gegevens in te voeren.

BEVEILIGBAARHEID

Authenticatie

Vraag 1: Welke authenticatiemethodes (standaarden) worden door uw oplossing ondersteunt voor respectievelijk medewerkers en partnerorganisaties?

De volgende authenticatiemethodes worden benoemd:

- Wachtwoord;
- MFA;
- SSO-functionaliteit beschikbaar op AzureAD;
- SSO-functionaliteit o.b.v. SAML2.0;
- Middels lokale gebruikersnaam met wachtwoord;
- Certificaat gebaseerd;
- LDAP;
- OAUTH;
- Digest Token.

Normen en standaarden

Vraag 2: Aan welke normen en standaarden op het gebied van informatiebeveiliging voldoet uw oplossing?

De volgende normen en standaard worden benoemd:

- ISO/IEC 27017:2015;
- ISO/IEC 27001:2013;
- ISO/IEC 27018:2019;
- ISO/IEC 27701:2019;
- SSAE 18 SOC 1 en SOC 2-rapporten;
- BSI Cloud Computing Compliance Controls Catalog (C5) Standard;
- APEC Privacy Recognition for Processors (PRP);
- SOC 3.

INKOOPSTRATEGIE

Procedure

Vraag 1: Welke aanbestedingsprocedure adviseert u en adviseert u gebruik te maken van percelen, zo ja welke dan en waarom?

Leveranciers geven aan (mits de raming van de opdracht dit toelaat) te kiezen voor een meervoudige onderhandse procedure, niet opgesplitst in percelen. Waarbij het van belang is dat partijen een Proof-of-Concept mogen aanbieden.

Selectiecriteria

Vraag 2: Kunt u een beschrijving geven over welke selectiecriteria belangrijk kunnen zijn voor een goede uitvoering van de opdracht?

Leveranciers geven de volgende selectiecriteria aan:

- Beroepsbekwaamheid;
- Flexibiliteit en mogelijkheden binnen de oplossing;
- ontwikkeling door NL bedrijven om ook de context en referentiekader van NL gemeenten te begrijpen;
- Hosting op Nederlands grondgebied in gecertificeerde datacenters;



- Beheer van data van de gemeente uitsluitend op Nederlands grondgebied dus ook de backup;
- Consultants, voorzien van aan te leveren cv's, waaruit blijkt de bewezen ervaring in de gemeentelijke overheid én kennis over interne beheersingsvraagstukken bij Nederlandse gemeenten;
- Softwareleverancier moet statutair in NL gevestigd zijn;
- Softwareleverancier moet bewezen implementaties hebben bij NL gemeenten in de afgelopen 3 jaar;
- Aantoonbare kunnen participeren in het ontwikkelproces door de gemeente;
- Softwareleverancier moet zowel ISO 9001 als 27001 gecertificeerd zijn omdat het niet alleen gaat om informatiebeveiliging maar ook om de kwaliteit van de eigen bedrijfsprocessen van de leverancier;
- ISO27001 (of vergelijkbaar);
- Financiële en organisatorische stabiliteit;
- Professionaliteit en betrouwbaarheid van de SaaS-oplossing;
- Referentieverklaring.

Gunningscriteria

Vraag 3: Kunt u een beschrijving geven over wat in uw ogen de beste gunningscriteria en gewichten zijn die leiden tot de beste inschrijving?

Leveranciers vermelden de volgende gunningscriteria in hun antwoorden:

- Gebruikerstest van de oplossing;
- Prijs;
- Kwaliteit;
- Kennis
- Voor-gedefinieerde inhoud;
- PowerBI rapportagemogelijkheden;
- TCO;
- Demonstratie / Proof of Concept;
- Adoptiegemak;
- Visie & Roadmap.

3. Ten slotte

Gemeente Eindhoven heeft nog geen mogelijke aanbestedingsstrategie bepaald. Op dit moment kan niet exact worden aangegeven, of en wanneer een mogelijke aanbesteding zal worden uitgezet. De vervolgstap is dat de tijdens de marktconsultatie aangesloten kerngroep hierover adviseert. Het besluit hierop vanuit de organisatie bepaalt het vervolg. De marktconsultatie heeft Eindhoven een goed beeld gegeven van de oplossingen op de markt, diens visies en ontwerpkeuzes. Mocht Eindhoven besluiten om aan te besteden dan zal het deze inzichten gebruiken om te komen tot een voor hen passende uitvraag. Indien er besloten wordt tot het publiceren van een aanbesteding zal dit waarschijnlijk ergens rond Q3 2023 zijn. Gemeente Eindhoven heeft een evaluatie gehouden bij de stakeholders. De meest opvallende analyse van deze evaluatie was dat alle stakeholders de toegevoegde waarde van een GRC-tool inzien.

Dit document is voor de aanbestedende dienst louter informatief en dient als input voor de aanbestedende dienst om te komen tot de juiste aanbestedingsstrategie en als input voor mogelijke aanbestedingsdocumenten. De gemeente bepaald aan de hand van gegeven antwoorden welke gegevens relevant worden geacht voor een mogelijke aanbesteding. Niet alle antwoorden zullen dan ook door de aanbestedende dienst als relevant worden beschouwd.