Bijlage 14. Marktconsultatieverslag vervanging IAM-systeem

Ten behoeve van

gemeente Zaanstad

Kenmerk: 2025-198

Publicatiedatum marktconsultatie: 12-1-2026

Datum verslag: 23-6-2026

Versie: Definitief

Inhoud

1. Inleiding

Gemeente Zaanstad is voornemens om een (Europees) aanbestedingstraject te starten voor de vervanging van de huidige IAM-tool/ -oplossing. Hoewel de huidige IAM-tool ons in het verleden goed heeft gediend, merken we dat deze niet langer volledig aansluit bij de groeiende eisen van een volwassen IAM-inrichting. We hebben enkele technische beperkingen en beheers uitdagingen geconstateerd die kunnen leiden tot risico's zoals verstoringen en een single-point-of-failure. We streven ernaar om een oplossing te vinden die beter aansluit bij onze toekomstige behoeften.

2. Doelstellingen marktconsultatie

Het doel van deze marktconsultatie is het verwerven van een modern, gebruiksvriendelijk en betaalbaar IAM-systeem, waarmee we de toegang tot systemen en middelen efficiënt kunnen beheren. Het systeem moet rolhouders binnen het autorisatieproces ondersteunen met gebruiksvriendelijke userinterfaces. Tegelijkertijd zorgt de goedkeuringsflow ervoor dat medewerkers snel beschikken over de toegangsrechten die zij nodig hebben om hun werkzaamheden uit te voeren, waarbij de autorisaties gecontroleerd en veilig worden toegekend of op tijd ingetrokken. Daarmee wordt de bedrijfscontinuïteit, informatieveiligheid en privacy binnen de organisatie gewaarborgd. Daarnaast wil de gemeente Zaanstad:

Met deze marktconsulatie willen wij een realistisch programma van eisen en wensen opstellen, dat aansluit bij de mogelijkheden van de markt. Zodat de kans op de best mogelijke keuze van een IAM-systeem, dat zowel functioneel onze ambities ondersteunt als voldoet aan de randvoorwaarden, zo groot mogelijk wordt.

3. Proces en respons

Datum	Omschrijving	Door
12-01-2026	Aankondiging marktconsultatie en beschikbaarstelling marktconsultatiedocument met bijlagen op TenderNed	Gemeente
26-01-2026 voor 10:00 uur	Indienen schriftelijke vragen over de marktconsultatie, via de berichtenmodule op TenderNed (bijlage 3)	Marktpartij
02-02-2026	Publiceren Nota van Inlichtingen	Gemeente
16-02-2026 voor 10:00 uur	Indienen schriftelijke reactie op de marktconsultatie	Marktpartij
16-03, 17-03, 23-03	Gesprekken mondelinge fase, indien van toepassing	Gemeente & marktpartijen
Bij aankondiging opdracht	Publicatie marktconsultatieverslag	Gemeente

Voor de schriftelijke marktconsultatie op TenderNed hebben vijf (5) leveranciers antwoorden ingestuurd. De vragen zijn door vier (4) leveranciers volledig beantwoord, één (1) leverancier heeft geen volledige beantwoording ingediend.

Vier (4) leveranciers hebben op verzoek van de gemeente Zaanstad via MS Teams een demonstratie van hun applicatie gegeven. De demonstraties gaven een dieper inzicht in het gebruik van de applicaties.

4. Bevindingen vragenlijst

4.1 Vragen algemeen

Vraag 01.
Indien u wordt gevraagd voor de mondelinge fase heeft u hierin dan interesse om aan deel te nemen? Indien ja, dan graag onderstaande gegevens invullen.

Alle vier (4) leveranciers die een volledige beantwoording hebben ingestuurd, hebben aangegeven interesse te hebben om deel te nemen aan de mondelinge fase.

Vraag 02.
De gemeente Zaanstad streeft ernaar om eind 2026 live te gaan met de Oplossing. Welke belangrijke fasen, randvoorwaarden en aandachtspunten ziet u bij het realiseren van deze planning? Welke risico's en afhankelijkheden zouden in kaart gebracht moeten worden?

De leveranciers achten een livegang van de IAM-oplossing eind 2026 haalbaar, mits de implementatie gefaseerd wordt uitgevoerd en de gemeente strak stuurt op scope, besluitvorming, datakwaliteit en beschikbaarheid van capaciteit. Zij benadrukken het belang van een duidelijke MVP-afbakening, tijdige integratie met HR- en doelsystemen en voldoende betrokkenheid van functioneel beheer, HR en proceseigenaren. Belangrijkste risico's zijn onvoldoende datakwaliteit, beperkte gemeentelijke capaciteit en scope-uitbreiding tijdens de implementatie. Deze risico's worden volgens leveranciers beheersbaar geacht door een gefaseerde aanpak, heldere governance en tijdige validatie en acceptatie.

Vraag 03.
De gemeente Zaanstad wil een toekomstvaste, goed beveiligde en beheersbare levering van de Oplossing realiseren. Welke levermodellen biedt u aan (zoals SaaS, hybride of On-Premise), welke keuze zou u adviseren voor de gemeente Zaanstad en welke overwegingen liggen hieraan ten grondslag? Graag toelichten met betrekking tot beveiliging, doorontwikkeling, beheerlast, schaalbaarheid, continuïteit en kosten.

De leveranciers bieden meerdere levermodellen aan, waaronder SaaS, hybride en on-premises. Het merendeel adviseert een (primair) SaaS-gebaseerd levermodel. Deze keuze wordt onderbouwd met voordelen op het gebied van met name een lagere beheerlast voor de gemeente. Datasoevereiniteit en Europese hosting (sovereign-cloud-varianten) wordt door meerdere leveranciers als een belangrijke ontwikkeling genoemd. In de nadere toelichting is bevestigd dat on-premise inzet in de meeste gevallen daadwerkelijk mogelijk is. Daarbij komt naar voren dat bepaalde AI-ondersteunende functionaliteiten primair beschikbaar zijn binnen SaaS-omgevingen en bij on-premise inzet niet beschikbaar zijn.

Vraag 04.
Indien u een SaaS-model aanbiedt, welke hostingopties zijn beschikbaar, inclusief geografische locatie van datacenters, gebruikte cloudplatformen en de borging van datasoevereiniteit, privacy en exitmogelijkheden?

De leveranciers geven aan dat SaaS-oplossingen worden gehost binnen Europese datacenters, onder meer op gangbare cloudplatformen zoals Microsoft Azure en AWS. Hostinglocaties worden veelal expliciet binnen de EU gepositioneerd, met aandacht voor redundantie en continuïteit. Datasoevereiniteit en privacy worden volgens leveranciers geborgd door opslag en verwerking van data binnen de EU, encryptie van data in rust en tijdens transport, tenant-isolatie en contractuele afspraken over eigenaarschap en datagebruik. Daarnaast benoemen leveranciers duidelijke exitmogelijkheden, waaronder het beschikbaar

stellen van data in open en overdraagbare formaten en ondersteuning bij gecontroleerde offboarding en migratie. Enkele leveranciers wijzen aanvullend op sovereign-cloud- of single-tenant-varianten om risico's rond buitenlandse wetgeving verder te beperken.

Vraag 05.
Indien uw SaaS-oplossing afhankelijk is van een grote internationale cloudleverancier (zoals AWS of Azure), welke maatregelen zijn voorzien om vendor-lock-in te beperken, en welke strategie hanteert u hiervoor op de lange termijn?

De leveranciers geven aan dat afhankelijkheid van internationale cloudplatformen zoals AWS of Azure niet automatisch leidt tot vendor lock-in. Zij benoemen als belangrijkste mitigerende maatregelen het gebruik van open standaarden en protocollen voor integratie en federatie, een duidelijke scheiding tussen IAM-governance, data en onderliggende infrastructuur, en contractuele afspraken over dataportabiliteit en exit. Daarnaast wordt genoemd dat data en configuraties overdraagbaar worden vastgelegd en dat ondersteuning bij migratie of exit beschikbaar is. Enkele leveranciers wijzen aanvullend op alternatieve hostingopties, zoals sovereign-cloud-varianten, single-tenant-oplossingen of hosting binnen de eigen cloudomgeving van de organisatie, als onderdeel van hun langetermijnstrategie.

Vraag 06.
Beschrijf welke relevante ervaring uw organisatie heeft met het leveren, integreren en beheren van een IAM-oplossing binnen een gemeentelijke IT-architectuur. Ga daarbij expliciet in op ervaring bij gemeenten van vergelijkbare omvang en organisatorische complexiteit.

Licht toe welke succesfactoren in deze trajecten bepalend zijn geweest voor een succesvolle implementatie en ingebruikname van het IAM-systeem, en welke lessen hieruit zijn geleerd die relevant zijn voor gemeenten met een vergelijkbare context en volwassenheidsniveau.

Benoem één of meer referentieprojecten bij gemeenten die inhoudelijk en qua werkwijze vergelijkbaar zijn met de door ons gevraagde IAM-oplossing. Beschrijf per referentie kort de betreffende gemeente en haar omvang, de scope van de IAM-oplossing, de gehanteerde aanpak en rol van uw organisatie, de belangrijkste succesfactoren en de meest relevante leerpunten. Indien beschikbaar en met toestemming, kan tevens de naam en contactgegevens van een verificatiecontact worden opgenomen.

De leveranciers geven aan ruime ervaring te hebben met het leveren, integreren en beheren van IAM-oplossingen binnen gemeentelijke en vergelijkbare publieke IT-architecturen, waaronder bij gemeenten van vergelijkbare omvang en complexiteit. Zij beschrijven rollen als architect, regisseur en implementatiepartner, met nadruk op het aansluiten van de IAM-oplossing op bestaande governance, processen en het applicatielandschap.

Als belangrijkste succesfactoren worden genoemd: nauwe samenwerking met functioneel beheer, HR, proceseigenaren en technisch beheer, een gefaseerde implementatie met focus op IDU-processen, duidelijke governance en tijdige besluitvorming. Leveranciers benoemen als belangrijkste leerpunten het belang van realistische planning, expliciete risicobeheersing en actieve betrokkenheid van beheerteams, met name rondom HR-bronsystemen en AD/Entra-integraties. Niet alle leveranciers delen concrete gemeentelijke referenties in deze fase, maar wijzen op inhoudelijk vergelijkbare trajecten bij publieke organisaties met een vergelijkbaar volwassenheidsniveau.

Vraag 07.
Op basis van het overzicht Functionaliteit en **3.000 identiteiten** (medewerkers gemeente Zaanstad, inhuur, uitbesteed werk en partnerorganisaties): wat zouden de kosten voor de gemeente Zaanstad worden, gesplitst naar incidentele kosten en structurele kosten per jaar?

Indien u zowel een SaaS-variant als een On-Premise-variant aanbiedt, gaan wij primair uit van SaaS en vragen wij u de SaaS-kosten te specificeren. Alleen wanneer u geen SaaS-variant kunt leveren, ontvangen wij graag de kosten voor een On-Premise-levering.

Eenmalige implementatiekosten 01-01-27 t/m 31-12-2027 [1)]	€
Gebruik oplossing tijdens implementatie	€
Gebruik oplossing structurele kosten per jaar	€

[1)] Voor de vergelijkbaarheid een inschatting gemaakt van de implementatieperiode

Hoe veranderen de structurele kosten per jaar bij een toenemend of afnemend aantal identiteiten? Het is aan u om de stappen (staffels) te wijzigen als anders van toepassing is, zolang maar duidelijk is welke aantallen corresponderen met welke kosten.

Een overzichtstabel kan bijvoorbeeld zo worden ingevuld:

Aantal identiteiten	**Structurele kosten per jaar (€)**
2.500 (minder)	
3.000 (initieel)	
3.500 (meer	

De gemeente Zaanstad heeft inzicht verkregen in de kostenstructuur en licentievoorwaarden, waaronder de criteria voor het meetellen van identiteiten voor licentiedoeleinden.

Vraag 08.
Welke maatregelen en technische keuzes zorgen ervoor dat het IAM-systeem technologisch actueel en toekomstbestendig blijft, zodat ingrijpende migraties of vervangingen in de toekomst zoveel mogelijk worden voorkomen?

Volgens de leveranciers wordt de toekomstbestendigheid van het IAM-systeem geborgd door een combinatie van een modulaire architectuur, het gebruik van open standaarden en een configuratie- in plaats van maatwerkgedreven inrichting. Hierdoor kunnen wijzigingen in organisatie, processen of applicatielandschap worden doorgevoerd zonder ingrijpende technische aanpassingen. Bij SaaS-oplossingen wordt het platform continu actueel gehouden door automatische updates en doorontwikkeling op het gebied van functionaliteit, security en compliance. Leveranciers benadrukken daarnaast het belang van API-first-architectuur en brede ondersteuning van standaarden zoals SCIM, SAML en REST, om flexibiliteit, uitwisselbaarheid en duurzame integratie te waarborgen en toekomstige migraties of vervanging zoveel mogelijk te voorkomen.

In de nadere toelichting komt naar voren dat afwijkingen in de meeste gevallen kunnen worden opgevangen met configuratie en standaardfunctionaliteit, zonder structureel maatwerk.

Vraag 09.
Welke aanpak hanteert uw organisatie voor doorontwikkeling, planning van releases en verwerking van gebruikersfeedback om het systeem up-to-date, veilig en gebruiksvriendelijk te houden?

De leveranciers geven aan een gestructureerde en voorspelbare aanpak te hanteren voor doorontwikkeling en releasemanagement, gericht op het actueel, veilig en gebruiksvriendelijk houden van het IAM-systeem. Veelal wordt gewerkt met vaste releasecycli, waarbij onderscheid wordt gemaakt tussen functionele uitbreidingen, bugfixes en security-updates, ondersteund door duidelijke release-informatie en impactanalyses. Doorontwikkeling vindt plaats op basis van een roadmap, aangevuld met agile werkwijzen. Gebruikersfeedback wordt structureel verzameld en verwerkt via onder meer gebruikersgroepen, feedbackkanalen, supporttickets en acceptatietests. Leveranciers benadrukken dat deze aanpak zorgt voor continue verbetering met minimale verstoring van de operationele IAM-processen.

Vraag 10.
Welke looptijd adviseert u voor deze dienstverlening en waarom?

De leveranciers adviseren overwegend een contractlooptijd van drie tot zes jaar, veelal met één of meerdere verlengingsmogelijkheden. Deze looptijd wordt passend geacht om de IAM-oplossing zorgvuldig te implementeren, te stabiliseren en door te ontwikkelen, en om investeringen in inrichting, conversie en adoptie terug te verdienen. Enkele leveranciers geven aan dat een langere samenwerkingsduur kan bijdragen aan lagere totale eigendomskosten en continuïteit, met name gezien het strategische en doorlopende karakter van IAM-dienstverlening. Tegelijkertijd wordt benadrukt dat flexibiliteit voor de gemeente geborgd moet blijven, onder andere door heldere verlengingsvoorwaarden, prijsafspraken en expliciete exit- en dataportabiliteitsafspraken.

Vraag 11.
Wat zijn naar uw idee goede kwalitatieve gunningscriteria, waarmee partijen zich van elkaar kunnen onderscheiden?

De leveranciers geven aan dat goede kwalitatieve gunningscriteria zich primair zouden moeten richten op de mate waarin een IAM-oplossing en leverancier bijdragen aan een beheersbare, veilige en toekomstvaste inrichting binnen een gemeentelijke context. Daarbij wordt benadrukt dat onderscheidend vermogen vooral ligt in de aansluiting op de gemeentelijke IAM-werkwijze en IDU-processen, met zo min mogelijk maatwerk, en in de mate van beheersbaarheid, auditability en transparantie van de oplossing. Daarnaast noemen leveranciers als belangrijke onderscheidende criteria de kwaliteit en realiteitszin van de implementatie- en migratieaanpak, de borging van risicobeheersing en continuïteit, en de wijze waarop vendor lock-in wordt beperkt door het gebruik van open standaarden en duidelijke exit-afspraken. Ook de kwaliteit van de implementatiepartner, waaronder expertise, ervaring met vergelijkbare organisaties, servicegerichtheid en certificeringen, wordt als relevant genoemd. Meerdere leveranciers benadrukken tot slot het belang van een evenwichtige prijs-kwaliteitverhouding, waarbij kwaliteit zwaarder weegt dan prijs.

Vraag 12.
Welke informatie is door de Gemeente Zaanstad niet gevraagd, maar volgens u wel van belang?

Leveranciers geven aan dat naast de uitgevraagde onderwerpen met name de borging van IAM-governance na implementatie van belang is. IAM wordt daarbij gezien als een structureel onderdeel van risicobeheersing en bedrijfsvoering, waarvoor duidelijke afspraken nodig zijn over eigenaarschap, mandatering, beheerrollen en besluitvorming. Daarnaast wordt het belang benadrukt van adoptie, kennisoverdracht en opleiding van beheerders en rolhouders om duurzame werking en draagvlak te borgen.

Verder wijzen leveranciers op het belang van realistische randvoorwaarden voor implementatie, zoals voldoende interne capaciteit en expertise aan gemeentelijke zijde, goed inzicht in het applicatielandschap en heldere regie bij samenwerking met meerdere partijen. Ook wordt genoemd dat aanbestedingen gebaat zijn bij het formuleren van doelen en gewenste uitkomsten, in plaats van het gedetailleerd voorschrijven van oplossingen, om maatwerk en onnodige risico's te voorkomen. Tot slot noemen enkele leveranciers aanvullende aandacht voor toekomstige identiteiten en governance-vraagstukken, zoals non-human identities, PAM en bredere identity-governance, als relevant voor een toekomstvaste inrichting.

4.2 Vragen functioneel

Instroom Doorstroom Uitstroom (IDU)-Proces

Vraag 13.
Welke mogelijkheden biedt uw oplossing voor handmatige registratie en beheer van identiteiten, ter voorkoming van dubbele invoer en voor het waarborgen dat de registratie correct en volledig blijft? Beschrijf daarnaast hoe de oplossing omgaat met invoer door verschillende organisatieonderdelen of entiteiten, zodat gegevens gescheiden en veilig blijven.

Leveranciers geven aan dat hun IAM-oplossingen zowel automatische als handmatige registratie van identiteiten ondersteunen. Handmatige invoer wordt met name toegepast voor doelgroepen die niet via een HR-bronsysteem worden ontsloten, zoals externen, partners of tijdelijke medewerkers. Om dubbele registraties te voorkomen ondersteunen leveranciers deduplicatie- en validatiemechanismen, waarbij registraties en wijzigingen auditbaar zijn. Daarnaast bieden leveranciers mogelijkheden voor logische scheiding van identiteiten, bijvoorbeeld via identiteitscontainers, business units of role-based toegangsrechten, zodat gegevens van verschillende entiteiten gescheiden kunnen worden beheerd terwijl governance en lifecycleprocessen uniform blijven.

In de nadere toelichting geven leveranciers expliciet aan dat handmatige registratie in de praktijk vooral bedoeld is voor niet-HR doelgroepen die wel toegang nodig hebben, en dat hiervoor vaak een aparte registratie- of externenmodule wordt gebruikt. Ook wordt toegelicht dat deduplicatie en identiteitsbeheer configureerbaar zijn, waarbij dubbele registraties worden beperkt en beheer binnen of tussen identiteitscontainers afhankelijk is van de inrichting van de organisatie.

Vraag 14.
Kan het IDU-proces voor handmatig ingevoerde identiteiten hetzelfde worden toegepast als voor automatisch gesynchroniseerde identiteiten vanuit YouForce? Welke verschillen zijn aanwezig, indien van toepassing?

De leveranciers geven aan dat het IDU-proces (instroom, doorstroom en uitstroom) voor handmatig ingevoerde identiteiten functioneel gelijk kan worden toegepast als voor automatisch gesynchroniseerde identiteiten vanuit YouForce. In beide gevallen doorlopen identiteiten dezelfde lifecycle-processen, controles, signaleringen, autorisaties en logging, wat volgens leveranciers leidt tot een uniforme werkwijze.

Het belangrijkste verschil zit in de herkomst van de gegevens en de manier waarop mutaties worden getriggerd: bij HR-identiteiten gebeurt dit via automatische synchronisatie vanuit het bronsysteem, terwijl bij handmatig ingevoerde identiteiten wijzigingen plaatsvinden via beheer- of registratieprocessen binnen het IAM-systeem. Functioneel en procesmatig leidt dit volgens leveranciers niet tot verschillen in behandeling, wat bijdraagt aan eenduidigheid, beheersbaarheid en auditability.

In de nadere toelichting komt naar voren dat met name de automatisering van instroom, doorstroom en uitstroom sterk afhankelijk is van de volledigheid, consistentie en tijdigheid van brondata uit het HR-systeem en, waar van toepassing, handmatige invoer voor partnerorganisaties. Kritieke onderdelen betreffen onder meer identiteitsmatching en deduplicatie, rol- en autorisatietoekenning op basis van HR-attributen, notificatie- en goedkeuringsworkflows en het tijdig intrekken van toegang bij uitdiensttreding. Leveranciers geven aan dat onvoldoende datakwaliteit kan leiden tot risico's zoals dubbele identiteiten, onjuiste of achterblijvende autorisaties, foutieve routing van goedkeuringen en verhoogde beveiligings- en auditrisico's. Tegelijkertijd beschrijven leveranciers dat moderne IAM-oplossingen beschikken over validatieregels, detectie- en uitzonderingsmechanismen, governance-processen en noodmaatregelen om deze risico's te signaleren en beheersbaar te houden.

Structureel blijft een goede inrichting van datagovernance en periodieke reconciliatie tussen bron- en doelsystemen volgens leveranciers een randvoorwaarde voor betrouwbare IDU-automatisering.

Vraag 15.
Welke signaleringsmogelijkheden zijn er om verantwoordelijken te informeren bij wijzigingen (zoals wanneer een medewerker doorstroomt of van functie verandert) zodat autorisaties (bij ons procesrollen) tijdig kunnen worden ingetrokken of toegekend?

De leveranciers geven aan dat hun IAM-oplossingen uitgebreide signaleringsmogelijkheden bieden om verantwoordelijken tijdig te informeren bij relevante wijzigingen in de lifecycle van identiteiten, zoals doorstroom, functiewijzigingen of afdelingswisselingen. Wijzigingen worden automatisch gedetecteerd op basis van mutaties in HR-bronsystemen of handmatige aanpassingen en leiden tot signaleringen richting betrokken rolhouders, zoals leidinggevenden, proceseigenaren of beheerders.

Signalen worden volgens leveranciers ondersteund via verschillende kanalen, zoals notificaties, taken, dashboards en workflows, waarbij opvolging en besluitvorming expliciet kunnen worden vastgelegd. Daarbij worden ook herhalingen of escalaties ingezet wanneer acties niet tijdig worden opgevolgd. Alle signaleringen, besluiten en wijzigingen worden gelogd en zijn auditbaar. Leveranciers geven aan dat deze aanpak het risico op achterblijvende of ongewenste autorisaties vermindert en bijdraagt aan tijdige en gecontroleerde toekenning of intrekking van procesrollen.

Vraag 16.
De inrichting van de IDU-keten betreft een eenmalige, kritische maatwerkconfiguratie van regels binnen het IAM-systeem. Deze inrichting moet langdurig stabiel functioneren, volledig in lijn zijn met wijzigingen vanuit het HR-systeem, en minimale structurele beheerinspanning vragen van de gemeente.

De maatwerkconfiguratie zorgt voor automatisering van instroom-, doorstroom- en uitstroomprocessen op basis van identiteiten en wijzigingen in identiteitskenmerken (zoals organisatorische eenheid, functie, roltoewijzing en contractgegevens), afkomstig uit het HR-systeem en/of handmatige invoer. Op basis van de uitkomst van een regel worden automatisch acties aangestuurd binnen het IAM-systeem en naar doelsystemen (AD, Topdesk of E-Mail)

Voor de eenmalige IDU-configuratie wordt gevraagd een toelichting te geven op:

1. **Configuratiemogelijkheden en scripting-opties:** Welke mogelijkheden biedt uw oplossing voor het definiëren en aanpassen van regels en workflows, en welke aanpassingen kan functioneel beheer zelfstandig uitvoeren?
2. **Logging en reproduceerbaarheid:** Welke mogelijkheden zijn er om acties en resultaten van workflows in het IAM-systeem en doelsystemen te loggen, zodat resultaten reproduceerbaar en traceerbaar zijn?
3. **Risicobeperking en continuïteit:** Welke maatregelen of mechanismen beperken risico's bij fouten of afwijkingen, zodat continuïteit, betrouwbaarheid en compliance worden gewaarborgd?

De leveranciers geven aan dat de inrichting van de IDU-keten wordt gerealiseerd via een configuratie- en regelgedreven aanpak binnen het IAM-systeem, waarbij instroom-, doorstroom- en uitstroomprocessen duurzaam en stabiel worden geautomatiseerd op basis van wijzigingen uit het HR-systeem en/of handmatige invoer. Daarbij wordt benadrukt dat functioneel beheer binnen afgesproken kaders zelfstandig regels en workflows kan aanpassen, zonder maatwerkprogrammering of complexe scripting.

Ten aanzien van logging en reproduceerbaarheid geven leveranciers aan dat alle lifecycle-events, workflow-acties en provisioning-handelingen volledig worden gelogd en herleidbaar zijn, zowel binnen het

IAM-systeem als richting doelsystemen. Dit maakt resultaten volgens leveranciers reproduceerbaar en ondersteunt audits en foutanalyse. Voor risicobeperking en continuïteit worden onder meer validatiemechanismen, monitoring, uitzonderingsafhandeling, retry- en rollback-mogelijkheden en scheiding tussen test- en productieomgevingen genoemd. Leveranciers geven aan dat deze combinatie bijdraagt aan een robuuste IDU-keten met minimale structurele beheerinspanning voor de gemeente.

Aanvragen en goedkeuren

Vraag 17.
Op basis van de beschreven eisen voor aanvraag- en goedkeurfunctionaliteit van procesrollen, middelen en autorisaties (inclusief regie en mandatering) vragen wij leveranciers het volgende:

- Welke aanvullende functionaliteiten of mogelijkheden biedt uw oplossing die mogelijk nog niet in onze eisen zijn opgenomen?
- Welke voordelen bieden deze mogelijkheden in het kader van aansluiting op onze werkwijze?

De leveranciers geven aan dat hun oplossingen, naast de gevraagde aanvraag- en goedkeurfunctionaliteit voor procesrollen, middelen en autorisaties, aanvullende mogelijkheden bieden die de regie, beheersbaarheid en gebruiksvriendelijkheid versterken. Genoemd worden onder meer inzicht voor rolhouders in de impact van aanvragen, flexibele inrichting van mandatering en vervanging, en context- of risicogestuurde goedkeuringsflows waarbij aanvragen worden gerouteerd naar de juiste verantwoordelijken. Daarnaast wordt genoemd verder vormen van automatisering, zoals event-gedreven workflows, lifecycle-gestuurde toekenning en intrekking van autorisaties, tijdelijke toekenningen met automatische expiratie en periodieke attestaties. Ook wordt AI-ondersteuning genoemd als aanvullend hulpmiddel, bijvoorbeeld voor aanbevelingen en analyses ter ondersteuning van besluitvorming en risicobeheersing. Deze AI-functionaliteit wordt expliciet gepositioneerd als adviserend en ondersteunend binnen de bestaande governance- en mandateringsstructuur en is afhankelijk van de kwaliteit van brondata. Volgens leveranciers dragen deze mogelijkheden bij aan lagere beheerlast, meer consistentie in besluiten en versterking van transparantie, auditability en compliance.

In de nadere toelichting geven leveranciers aan dat AI-ondersteuning nadrukkelijk een adviserend karakter heeft (zoals aanbevelingen en filters) en dat besluitvorming en autorisatieverlening altijd onderdeel blijven van het reguliere aanvraag- en goedkeurproces.

Autorisatiebeheer (IAM-beheer)

Vraag 18.
De gemeente Zaanstad streeft ernaar het autorisatiebeheer centraal, eenduidig en beheersbaar in te richten volgens de beschreven werkwijze, met continu inzicht in de impact en risico's van wijzigingen en met gecontroleerde toegang tot resources.

Welke out-of-the-box functionaliteiten of alternatieve oplossingsrichtingen biedt uw oplossing, naast of in plaats van de door ons beschreven functionaliteit, waarmee binnen deze werkwijze hetzelfde resultaat kan worden gerealiseerd?

De leveranciers geven aan dat hun oplossingen diverse out-of-the-box functionaliteiten bieden om autorisatiebeheer centraal, eenduidig en beheersbaar in te richten. Genoemd worden rol- en attribuutgebaseerde autorisatiemodellen, herbruikbare autorisatiebouwstenen en lifecycle-gestuurde toekenning en intrekking van rechten. Wijzigingen in autorisaties kunnen vooraf inzichtelijk worden gemaakt via impact- en risicoanalyses, zodat gevolgen gecontroleerd kunnen worden beoordeeld.

Daarnaast worden aanvullende mogelijkheden genoemd zoals workflow- en policy-gestuurde wijzigingen, continue monitoring en rapportages (zoals SOLL-IST-vergelijkingen, risico- en conflictanalyses en

functiescheidingscontroles) en, bij sommige oplossingen, AI-ondersteunde analyses en aanbevelingen. Deze functionaliteiten worden gepositioneerd als ondersteunend aan regie en besluitvorming. Volgens leveranciers maken deze standaardvoorzieningen het mogelijk om hetzelfde resultaat te bereiken als met de beschreven functionaliteit, met minder maatwerk, meer transparantie en blijvende grip op impact en risico's.

In de nadere toelichting geven leveranciers aan dat het automatisch genereren van bundeltickets afhankelijk is van de inrichting van koppelingen en workflowlogica tussen IAM- en ITSM-systemen en de bijbehorende integratieafspraken.

Vraag 19.
Welke mogelijkheden biedt uw oplossing voor het periodiek importeren van een bestand met update-informatie over welke autorisaties aan welke procesrollen moeten worden gekoppeld of ontkoppeld, waarbij de import via meerdere processtappen wordt verwerkt, waaronder: voorafgaande validatie, rapportage van afwijkingen in een verwerkingsverslag, verwerking in concept en definitieve verwerking uitsluitend na expliciete goedkeuring?

De leveranciers geven aan dat hun IAM-oplossingen het periodiek importeren van bestanden met autorisatie- en procesrolwijzigingen ondersteunen via een gecontroleerd, meerstaps verwerkingsproces. Dit omvat voorafgaande validatie van gegevens, rapportage van fouten en verwerking van wijzigingen in een concept- of stagingfase, waarin de impact zichtbaar wordt gemaakt zonder directe doorvoering. Definitieve verwerking vindt uitsluitend plaats na expliciete goedkeuring door bevoegde rolhouders, via single- of multi-step goedkeuringsflows. Alle stappen zijn auditbaar, inclusief validaties, goedkeuringen en doorgevoerde wijzigingen. Volgens leveranciers draagt dit bij aan gecontroleerd en beheersbaar onderhoud van het rollen- en autorisatiemodel met beperkte kans op fouten.

In de nadere toelichting geven leveranciers aan dat de mate waarin wijzigingen als 'delta' (inclusief verwijderingen) automatisch worden herkend en verwerkt kan verschillen per oplossing en inrichting, en dat hiervoor soms aanvullende configuratie of afspraken over het importformaat nodig zijn.

Integraties

Vraag 20.
Welke koppelvarianten met het HR-systeem YouForce biedt de Oplossing, en welke variant adviseert u voor onze organisatie? Licht de keuze toe.

De leveranciers geven aan dat hun oplossingen meerdere koppelvarianten met het HR-systeem YouForce ondersteunen, waaronder API-gebaseerde koppelingen, bestandsgebaseerde synchronisatie en in sommige gevallen een middleware- of ESB-oplossing. De meeste leveranciers adviseren primair een API-gebaseerde koppeling, omdat deze actuele of near-realtime verwerking van HR-mutaties mogelijk maakt en goed aansluit op geautomatiseerde instroom-, doorstroom- en uitstroomprocessen.

Bestandsgebaseerde koppelingen worden genoemd als alternatief of overgangsvariant wanneer technische of organisatorische randvoorwaarden API-integratie beperken. Enkele leveranciers adviseren een middleware-oplossing om aanvullende validatie, filtering of verrijking van HR-gegevens te realiseren. Leveranciers benadrukken dat ongeacht de gekozen koppelvariant robuuste validatie, foutafhandeling en monitoring noodzakelijk zijn om te voorkomen dat fouten in brondata ongecontroleerd doorwerken in de IAM-keten.

Vraag 21.
Welke optie voor e-mailverzending het meest geschikt is voor Zaanstad: via de eigen mailserver van de Oplossing of via de mailserver van de gemeente Zaanstad, inclusief motivatie van de keuze.

De leveranciers geven aan dat zowel e-mailverzending via de mailserver van de IAM-oplossing als via de mailserver van de gemeente technisch mogelijk is. Het merendeel adviseert echter om e-mailverzending te laten verlopen via de mailserver van de gemeente Zaanstad. Deze keuze wordt onderbouwd met argumenten op het gebied van beveiliging, compliance, logging en beheersbaarheid, doordat bestaande e-mailbeveiligingsmaatregelen, archivering en afzenderbeleid onder gemeentelijke regie blijven.

De IAM-oplossing blijft in dit scenario verantwoordelijk voor het genereren en structureren van notificaties en workflowberichten, terwijl de daadwerkelijke verzending via de gemeentelijke infrastructuur plaatsvindt. Verzendmogelijkheden via de eigen mailserver van de oplossing worden vooral genoemd als alternatief of fallback in specifieke situaties. Volgens leveranciers draagt de voorkeur voor verzending via de gemeentelijke mailserver bij aan consistente communicatie, eenvoudiger beheer en betere auditability.

Vraag 22.
Gezien onze situatie met een on-premises Active Directory, welke aanpak voor integratie met het IAM-systeem is het meest geschikt, inclusief de verwachte voordelen en eventuele risico's?

De leveranciers geven aan dat voor een on-premises Active Directory-omgeving meerdere integratie-aanpakken mogelijk zijn. Veelgenoemd is een hybride inrichting waarbij het IAM-systeem fungeert als centrale regielaag en autorisaties gecontroleerd worden doorgezet naar Active Directory via gestandaardiseerde koppelingen. Daarbij worden zowel directe koppelingen met on-premises Active Directory als integratiepatronen via Microsoft Entra ID genoemd.

Als voordelen van deze benaderingen wordt onder meer genoemd de aansluiting op de bestaande directory-structuur, behoud van controle en compliance, en flexibiliteit richting toekomstige ontwikkelingen in het directory-landschap. Enkele leveranciers adviseren expliciet een Entra-ID-first-benadering, waarbij provisioning eerst naar Entra ID plaatsvindt en vervolgens via synchronisatie wordt doorgezet naar on-premises Active Directory, om netwerk- en securitycomplexiteit te beperken.

Als aandachtspunten en risico's noemen leveranciers onder andere afhankelijkheid van synchronisatieprocessen, mogelijke vertraging in doorvoering van mutaties en de kwaliteit en structuur van bestaande AD-gegevens. Deze risico's kunnen volgens leveranciers worden beperkt door heldere architectuurkeuzes, goede monitoring en logging, eenduidige attributen- en naamgevingsregels en een gefaseerde aanpak met aandacht voor opschoning en beheer.

4.3 Vragen niet functioneel

Security & Compliancy

Vraag 23.
Welke maatregelen heeft Opdrachtnemer genomen om te gaan voldoen aan de NIS2 en CER, en hoe zorgt u dat u tijdig compliant bent?

De leveranciers geven aan dat zij zowel organisatorische als technische maatregelen hebben getroffen om te voldoen aan de vereisten uit NIS2 en CER en om tijdig compliant te blijven. Genoemd worden onder meer het toepassen van security-by-design-principes, formele informatiebeveiligingsprocessen, risicomanagement, incidentdetectie en -afhandeling, en structurele monitoring en logging van IAM-activiteiten. Daarnaast verwijzen leveranciers naar certificeringen en normenkaders zoals ISO-27001 en SOC-rapportages, periodieke audits en vulnerability management.

Daarbij wordt benadrukt dat hun IAM-oplossingen gemeenten ondersteunen bij onderdelen van NIS2 en CER, bijvoorbeeld door lifecycle-gestuurde toegangscontrole, audittrails, attestaties en functiescheidingscontroles. Tegelijkertijd wordt aangegeven dat IAM slechts een onderdeel is van bredere compliance en dat aanvullende organisatorische en technische maatregelen bij de gemeente zelf noodzakelijk blijven, zoals incidentrespons, ketenbeheer en netwerkbeveiliging. Door continue doorontwikkeling, security-updates en actieve opvolging van regelgeving geven leveranciers aan tijdig te kunnen blijven aansluiten op de geldende NIS2- en CER-vereisten.

In de nadere toelichting komt naar voren dat leveranciers verschillend invulling geven aan assurance-vereisten zoals ISAE3000, afhankelijk van hun rol in de keten en het gekozen levermodel. Sommige partijen beschikken reeds over een geldige ISAE3000-verklaring of hebben een aantoonbaar traject gestart om hier tijdig aan te voldoen. Andere partijen positioneren alternatieve assurance-vormen, zoals SOC- en ISO-certificeringen, als passend binnen hun dienstverlening, met name wanneer zij zelf geen hosting of operationeel beheer uitvoeren. Leveranciers benadrukken daarbij dat de verantwoordelijkheid voor ISAE3000-assurance samenhangt met waar hosting, dataverwerking en operationele beheersmaatregelen zijn belegd. De gemeente heeft hiermee inzicht gekregen in de verschillende assurance-modellen en de bijbehorende randvoorwaarden.

Vraag 24.
Welke technische voorzieningen zijn aanwezig voor logging en auditdata, en kunnen deze gegevens onafhankelijk en veilig worden geraadpleegd?

De leveranciers geven aan dat hun IAM-oplossingen uitgebreide technische voorzieningen bieden voor logging en auditdata, waarbij alle relevante acties en gebeurtenissen worden vastgelegd. Dit betreft onder meer wijzigingen in identiteiten, rollen en autorisaties, goedkeuringsbesluiten, workflow-acties en technische handelingen richting doelsystemen. Logging is fijnmazig ingericht en maakt herleidbaar wie welke actie heeft uitgevoerd, op welk moment en met welk resultaat.

Auditdata kan volgens leveranciers onafhankelijk en veilig worden geraadpleegd door bevoegde functionarissen, zoals auditors of security-rollen, zonder dat hiervoor operationele beheerrechten nodig zijn. De gegevens zijn beschermd tegen ongeautoriseerde wijziging en worden ontsloten via rapportages, zoekfunctionaliteit en – indien gewenst – integraties met externe audit- of SIEM-voorzieningen. Leveranciers geven aan dat deze voorzieningen interne controles, compliance-verantwoording en externe audits ondersteunen.

Vraag 25.

Welke mechanismen ondersteunt het systeem voor rolafbakening en toegangscontrole, zowel operationeel als voor audits?

De leveranciers geven aan dat hun IAM-oplossingen mechanismen ondersteunen voor duidelijke rolafbakening en toegangscontrole, toepasbaar voor zowel de dagelijkse operatie als auditdoeleinden. Genoemd worden onder meer rol- en attribuutgebaseerde autorisatiemodellen, lifecycle-gestuurde toekenning en intrekking van rechten en workflow-gestuurde goedkeuringsprocessen, waarmee verantwoordelijkheden en toegangsrechten eenduidig kunnen worden ingericht en beheerd.

Voor auditdoeleinden bieden leveranciers uitgebreide logging en rapportagemogelijkheden, waarmee inzicht ontstaat in wie welke rechten heeft, op basis van welke rol of besluitvorming, en welke wijzigingen zijn doorgevoerd. Mechanismen zoals functiescheidingscontroles, risicosignalering en traceerbare besluitvorming worden genoemd als ondersteuning om zowel operationele beheersing als auditbaarheid structureel te borgen.

Vraag 26.
Welke mogelijkheden biedt de Oplossing voor detectie en afhandeling van security-incidenten conform regelgeving?

De leveranciers geven aan dat hun IAM-oplossingen diverse mechanismen ondersteunen voor de detectie en gecontroleerde afhandeling van security-incidenten, in lijn met geldende wet- en regelgeving. Genoemd worden onder meer continue logging en monitoring van identiteits- en toegangsactiviteiten, signalering van afwijkende of risicovolle gebeurtenissen en het genereren van meldingen richting beheerders of security-functies.

Daarnaast benoemen leveranciers mogelijkheden voor integratie met bredere security- en incidentmanagementprocessen, zoals koppelingen met SIEM- of SOC-voorzieningen, zodat IAM-gebeurtenissen kunnen worden gecorreleerd met andere security-signalen. Voor de afhandeling van incidenten ondersteunen oplossingen gecontroleerde workflows en maatregelen zoals het tijdelijk blokkeren of intrekken van toegang. Alle stappen worden gelogd en zijn auditbaar, zodat incidenten reproduceerbaar kunnen worden geanalyseerd en aantoonbaar conform de geldende kaders worden afgehandeld.

Vraag 27.
Welke functionaliteit biedt de Oplossing voor tijdelijke of beperkte toegang tot gevoelige functies, inclusief:

- tijdgebonden rechten (bijv. einddatum instelbaar),
- afbakening van toegang tot zeer gevoelige functies, en
- audit/logging van deze activiteiten?

Welke randvoorwaarden, beperkingen of mogelijkheden voor integratie met een bestaand of toekomstig PAM-systeem gelden hierbij?

De leveranciers geven aan dat hun IAM-oplossingen functionaliteit ondersteunen voor het gecontroleerd toekennen van tijdelijke en beperkte toegang tot gevoelige functies. Dit omvat tijdgebonden autorisaties met automatische intrekking, aanvullende goedkeuringsvereisten voor hoogrisico- of privileged functies en volledige logging en audittrails. Voor zeer gevoelige toegang worden aanvullende mechanismen toegepast zoals risicoklassen, contextafhankelijke goedkeuringen en expliciete mandatering. Daarnaast geven leveranciers aan dat integratie met PAM-oplossingen mogelijk is, waarbij IAM de governance- en proceslaag verzorgt en PAM de technische uitvoering van privileged access afhandelt. Volgens

leveranciers wordt deze combinatie gezien als een toekomstvaste aanpak voor risicobeheersing en compliance.

In de nadere toelichting geven leveranciers aan dat volledige zero-knowledge encryptie niet gangbaar wordt geacht binnen IGA-oplossingen, omdat het platform identiteitsgegevens moet kunnen verwerken voor functies zoals analyse, policy-evaluatie en provisioning.

Implementatie & Beheer

Vraag 28.
Welke stappen en ondersteuning biedt u tijdens implementatie? Welke fasen en mijlpalen zijn voorzien, welke mogelijke problemen of risico's zijn er, en welke adviezen heeft u voor mitigatie?

De leveranciers beschrijven een gefaseerde en iteratieve implementatieaanpak met duidelijke mijlpalen en intensieve samenwerking met de gemeente. In hoofdlijnen worden fasen onderscheiden zoals mobilisatie, analyse & ontwerp, configuratie/basisimplementatie (vaak als MVP), testen en acceptatie, go-live/hypercare en overdracht naar beheer, gevolgd door doorontwikkeling. Per fase worden expliciete opleverpunten, documentatie en kennisoverdracht georganiseerd om de implementatie beheersbaar te houden.

Daarnaast wordt ondersteuning geboden in de vorm van templates en checklists, configuratie- en testondersteuning, evaluatiemomenten en een formele overdracht naar beheer, inclusief operationele controleroutines en (bij SaaS) monitoring.

Als belangrijkste risico's worden benoemd: datakwaliteit in bron- en doelsystemen, onvoldoende beschikbaarheid en mandaat aan gemeentelijke zijde, scope-uitbreiding en technische afhankelijkheden. Als mitigerende maatregelen noemen leveranciers onder meer dataprofiling en opschoning vooraf, inzet van testomgevingen, een gefaseerde uitrol en een duidelijke governance- en besluitstructuur.

In de nadere toelichting geven leveranciers aan dat de belangrijkste risico's vooral liggen in organisatorische en datagerelateerde randvoorwaarden, zoals de kwaliteit van HR-brondata, het combineren van meerdere identiteitsstromen en afhankelijkheden van externe systemen. Daarnaast wordt het belang benadrukt van duidelijke governance, belegd eigenaarschap en voldoende beschikbaarheid voor besluitvorming, validatie en testen. Deze risico's worden door leveranciers als beheersbaar beschouwd bij een gefaseerde aanpak en een duidelijke afbakening van de scope.

Vraag 29.
Wat is naar uw idee een realistische implementatietijd en welke inzet (uren en functionarissen) verwacht u hierbij van de gemeente?

De leveranciers geven uiteenlopende indicaties voor een realistische implementatietijd, variërend van circa 4 maanden voor een basisimplementatie tot 6–12 maanden voor een volledige, gefaseerde invoering, afhankelijk van scope, aantal koppelingen, complexiteit van het autorisatiemodel en de gekozen fasering. Meerdere leveranciers benadrukken dat met een gefaseerde aanpak al relatief snel een werkende basis kan worden gerealiseerd, waarna verdere uitbouw en optimalisatie volgt.

Ten aanzien van de inzet van de gemeente geven leveranciers aan dat actieve betrokkenheid cruciaal is voor een succesvolle implementatie. Genoemd worden rollen zoals opdrachtgever/product owner IAM, projectmanager, functioneel en technisch beheer, HR, security en applicatie-eigenaren. De benodigde inzet varieert per fase, met een hogere intensiteit tijdens analyse, ontwerp, testen en acceptatie.

Leveranciers geven aan dat duidelijke rolverdeling, tijdige besluitvorming en voldoende beschikbaarheid aan gemeentelijke zijde bepalend zijn voor het tempo en de beheersbaarheid van het traject.

Toekomstvastheid

Vraag 30.
Welke mogelijkheden en uitdagingen zien jullie voor het integreren van de Oplossing met alternatieve identiteits- en toegangsbeheersystemen, zoals Keycloak of andere oplossingen, in plaats van onze huidige Active Directory-omgeving? Zijn er recente ontwikkelingen of best practices die dit ondersteunen?

De leveranciers geven aan dat hun IAM-oplossingen kunnen integreren met alternatieve identiteits- en toegangsbeheersystemen, zoals Keycloak en andere non-Microsoft Identity Providers. Deze integraties zijn gebaseerd op open standaarden en protocollen zoals REST-API's, SCIM, SAML en OpenID Connect, waardoor de IAM-oplossing onafhankelijk kan functioneren van een specifieke directory-technologie. Leveranciers positioneren het IAM-systeem daarbij als centrale governance- en autorisatielaag, terwijl authenticatie kan plaatsvinden via een alternatieve Identity Provider.

Als aandachtspunten en uitdagingen benoemen leveranciers onder meer het consistent houden van identiteitsgegevens, het vaststellen van een duidelijke bron van waarheid, het scheiden van verantwoordelijkheden tussen authenticatie en autorisatie en het voorkomen van overlappende of conflicterende policies tijdens migratie- of co-existentiescenario's. Best practices die worden genoemd zijn een API-first benadering, gebruik van federatieve standaarden, centrale lifecycle-sturing en het toepassen van hybride of multicloud IAM-modellen. Volgens leveranciers maken deze ontwikkelingen het mogelijk om de huidige Active Directory-omgeving op termijn te combineren met of te vervangen door alternatieve oplossingen, zonder verlies van governance, auditability en beheersbaarheid.

5. Bevindingen functionele- en niet-functionele eisen

De ingevulde eisenmatrixen geven een goed beeld van hoe de markt aankijkt tegen de beoogde IAM-oplossing en de daarbij horende functionele en niet-functionele eisen.

Over de **functionele eisen** ontstaat een relatief eenduidig beeld. Alle geraadpleegde partijen herkennen het geschetste functionele kader en geven aan dit in hun oplossing te kunnen ondersteunen. De verschillen tussen leveranciers manifesteren zich hier vooral in de gekozen terminologie, de mate van detaillering in de toelichting en de wijze waarop functionaliteit is ingericht of gecombineerd, maar niet in de fundamentele aanwezigheid van de gevraagde functionaliteit.

De marktconsultatie bevestigt daarmee dat het functionele beeld aansluit bij wat de markt op dit moment als gangbaar en haalbaar beschouwt binnen het IAM-domein. Functioneel gezien lijkt het onderscheidend vermogen tussen leveranciers beperkt, en is er sprake van een zekere mate van convergentie in aangeboden mogelijkheden.

Bij de **niet-functionele eisen** ontstaat een meer divers beeld. Met name op het terrein van informatiebeveiliging, compliance en aantoonbaarheid van maatregelen laten de reacties verschillen zien. Leveranciers geven regelmatig aan dat aan eisen kan worden voldaan, maar koppelen hier voorwaarden aan, bijvoorbeeld in de vorm van aanvullende afspraken, specifieke inrichtingskeuzes, inzet van onderliggende platformvoorzieningen of aanvullende diensten. In een aantal gevallen is een eis niet standaard onderdeel van het product of de dienstverlening, maar afhankelijk van configuratie, contractuele borging of externe certificering.

Deze variatie maakt zichtbaar dat niet-functionele eisen in de praktijk minder uniform worden ingevuld dan functionele eisen. Tegelijkertijd onderstrepen de reacties het belang van duidelijke duiding: begrippen als ‘voldoen’, ‘ondersteunen’ en ‘aantoonbaar maken’ worden door leveranciers verschillend geïnterpreteerd. De marktconsultatie laat daarmee zien dat juist op dit vlak heldere afbakening en explicitering van verwachtingen essentieel is om interpretatieverschillen te voorkomen.

Als geheel laat de marktconsultatie zien dat het zwaartepunt van het onderscheid tussen oplossingen minder ligt bij de functionele mogelijkheden en sterker bij de niet-functionele randvoorwaarden, in het bijzonder waar het gaat om security, compliance, auditability en governance. Deze observatie vormt waardevolle input voor de verdere uitwerking van de aanbestedingsdocumenten, waarbij kan worden nagedacht over het juiste evenwicht tussen harde eisen, minimumniveaus en wensen, en over de manier waarop aantoonbaarheid en volwassenheid van oplossingen het beste kan worden beoordeeld.

6. Bevindingen mondelinge fase

Naast de schriftelijke beantwoording hebben de vier (4) leveranciers die een volledige beantwoording hebben ingestuurd, mondelinge toelichting plaatsgevonden. De demonstraties dienden ter verduidelijking van functionaliteit een beter begrip van de toepasbaarheid van de oplossingen binnen de beschreven werkwijze van Zaanstad. Daarbij is een kort gesprek geweest over de antwoorden van verificatievragen om deze indien nodig verder te verduidelijken.