Marktconsultatie Cloudplatform en Rekencentrumtransitie

Outline voor marktconsultatie | definitief 1.0 | 18 november 2026

Documentkenmerk [behoort bij kenmerk 20260452917]	**Omschrijving**
Onderwerp	Cloudplatform en rekencentrumtransitie voor gemeenten Haarlem en Zandvoort
Status	Concept voor marktconsultatie
Doelgroep	Cloud-, platform-, beheer-, integratie- en applicatieontsluitingspartijen
Reactiewijze	Via het afzonderlijke Excel-invuldocument
Karakter	Vrijblijvende marktconsultatie; geen aanbestedingsprocedure en geen aanbod

Doel: de voorgenomen opdracht aantoonbaar uitvoerbaar, marktconform, proportioneel, bewijsbaar en prijsbaar maken voordat de aanbestedingsstukken definitief worden vastgesteld.

1. Inleiding

1.1 Aanleiding

De aanbestedende dienst bereidt de transitie voor van het huidige eigen rekencentrum naar een beheersbaar cloud- en platformlandschap. De bestaande datacenterhuisvesting en hardwarecontracten lopen af op 31 december 2029. Het toekomstige landschap moet gemeentelijke workloads veilig en controleerbaar ondersteunen, de operationele beheerlast verminderen, leveranciersafhankelijkheid begrenzen en een aantoonbaar uitvoerbare exit bieden.

De voorgenomen opdracht omvat vier percelen: IaaS en connectiviteit, een managed container- en dataplatform, service-integratie en cloudregieondersteuning, en digitale applicatieontsluiting. Percelen 1, 2 en 3 worden gelijktijdig aanbesteed. Van perceel 4 is nog niet vastgesteld of dit ook gelijk wordt meegenomen.

Deze outline bevat zelfstandig de context en uitgangspunten die marktpartijen nodig hebben om de consultatievragen te beantwoorden; het onderliggende Programma van Eisen wordt niet met de marktconsultatie meegestuurd.

1.2 Waarom een marktconsultatie

De consultatie is bedoeld om vóór publicatie te toetsen welke onderdelen door de markt leverbaar zijn, welke combinaties tot een gezonde mededinging leiden, welke eisen disproportioneel of onvoldoende bewijsbaar zijn en welke keuzes de grootste invloed hebben op prijs, doorlooptijd en risico. De consultatie is nadrukkelijk geen verzoek om een volledige offerte of een bindende ontwerpuitwerking.

1.3 Doelstellingen

- Valideren of de voorgenomen perceel- en contractstructuur aansluit op het aanbod en de verantwoordelijkheidsmodellen in de markt.
- Toetsen of de eisen rond SEAL-niveau 3, EU/EER-beheer, control planes, subverwerking en derde-landjurisdictie haalbaar en aantoonbaar zijn.
- Toetsen of multi-stack, geo-redundantie, herstel buiten de primaire leveranciersomgeving en de onafhankelijke regiezone technisch en economisch uitvoerbaar zijn.
- Vaststellen welke eisen als knock-out, contracteis, wens of informatieverplichting passend en proportioneel zijn.
- Inzicht krijgen in kostendrijvers, prijsmodellen, minimumafname, schaalbaarheid, migratiepieken, krimp en exitkosten.
- Praktijkervaring ophalen over transitie, service-integratie, kennisoverdracht en de inrichting van een duurzaam gezamenlijk beheermodel tussen leverancier en gemeente.
- Valideren hoe marktpartijen security en privacy vanaf ontwerp, bouw en configuratie integreren in architectuur, automatisering, standaardconfiguraties, beheerprocessen en lifecyclemanagement.

1.4 Beoogde opbrengst

De reacties worden gebruikt om de scope, fasering, perceelindeling, eisenclassificatie, verificatiemethode, prijsstructuur, contractuele borging en planning aan te scherpen. Individuele bedrijfsinformatie wordt alleen gebruikt voor de voorbereiding van de opdracht. In de aanbesteding worden geen voordelen toegekend aan deelnemers aan deze consultatie.

1.5 Afbakening

- Geen selectie of voorselectie van leveranciers.
- Geen verzoek om een bindend aanbod of definitieve prijs.
- Geen toezegging dat de aanbesteding ongewijzigd of op het genoemde moment wordt gepubliceerd.
- De aanbestedende dienst kan reacties geanonimiseerd en geaggregeerd verwerken in een consultatieverslag.

2. Context en uitgangssituatie

2.1 Huidige situatie

De organisatie exploiteert een gestrekt rekencentrum op eigen hardware, verdeeld over commerciële rackspace en een intern datacenter. De huidige omgeving is gebaseerd op VMware Cloud Foundation met onder meer vSphere, vSAN, NSX en de Aria-suite. Voor applicatieontsluiting wordt daarnaast een Omnissa Horizon-omgeving gebruikt. De bestaande VMware-laag wordt buiten deze opdracht opgewaardeerd en blijft tijdelijk in beheer totdat de migraties zijn afgerond. De marktconsultatie begint voor perceel 1 daarom bij de inrichting van de aangeboden doel-IaaS: technologie, virtualisatielaag, opslag, netwerkvirtualisatie, beheer- en automatiseringslaag, beschikbaarheidsmodel, locaties, licenties en portabiliteit. Pas daarna wordt gevraagd hoe de migratie vanuit de huidige VMware-omgeving naar die doelomgeving wordt uitgevoerd.

De gemeente is eigenaar van een publiek IP-adresblok en een eigen BGP Autonomous System Number. De marktconsultatie moet duidelijk maken hoe deze adressen en het eigen AS in de doelomgeving kunnen worden gebruikt en geadverteerd, inclusief BGP, RPKI/ROA, IPv4/IPv6, DDoS-bescherming, route-portabiliteit, beheerrechten en exit.

2.2 Inkoopdoelen

- Een tijdig beschikbaar platform voor uitfasering van het huidige rekencentrum voor 31 december 2029.
- Aantoonbare cloudsoevereiniteit en periodieke herbeoordeling.
- Open en gedocumenteerde koppelvlakken, overdraagbare configuraties en dataportabiliteit.
- Meetbare beschikbaarheid, cyberweerbaarheid, herstelbaarheid, prestaties en kosten.
- Ondersteuning van het Common Ground-gedachtengoed en van open source, open standaarden en herbruikbare voorzieningen, voor zover dit bijdraagt aan interoperabiliteit, transparantie, digitale autonomie, samenwerking tussen gemeenten en beperking van leveranciersafhankelijkheid.
- Nog niet vastgesteld in welke vorm, uitbesteding van operationele beheerlast met behoud van gemeentelijke regie, mogelijkheid om naleving en werking onafhankelijk aan te tonen en exitvermogen.

2.3 Organisatorische context

De oplossing ondersteunt de werkzaamheden voor twee afzonderlijke gemeenten (Haarlem en Zandvoort). Binnen de technische omgeving worden drie tenants onderscheiden: één gezamenlijke ambtelijke tenant voor de organisatie die voor beide gemeenten werkt en per gemeente één afzonderlijke tenant voor raad en griffie. Hoewel een deel van de ambtelijke organisatie gezamenlijk werkt, blijven de gemeenten afzonderlijk verantwoordelijk voor hun eigen gegevens, bevoegdheden, kosten, archiefbescheiden en bestuurlijke verantwoording. Gegevens, toegang, logging, kosten, bewaartermijnen, export en vernietiging moeten daarom per gemeente en per tenant afzonderlijk kunnen worden ingericht, uitgevoerd en aangetoond.

De dienstverlening moet bij voorkeur zonder fundamenteel herontwerp uitbreidbaar zijn naar een regionale dienst of andere ondersteunde organisatie. De markt wordt gevraagd de gevolgen te beschrijven voor tenant- en

datascheiding, identity, autorisatie, netwerksegmentatie, logging, kostenverdeling, archief- en privacyverantwoordelijkheden, servicelevels, licenties, minimale afname, onboarding en governance.

2.4 Planning en randvoorwaarden

Mijlpaal	Indicatie	Betekenis voor de markt
Marktconsultatie	Najaar 2026	Toets op haalbaarheid, proportionaliteit, prijsdrijvers, bewijsbaarheid en marktconformiteit
Publicatie percelen 1, 2 en 3. Perceel 4 wordt overwogen.	Voorgenomen Q1 2027	Gezamenlijke aanbesteding van IaaS/connectiviteit, platform en service-integratie, afhankelijk van besluitvorming en verwerking consultatieresultaten
Inrichting fundament	Beschikbaar Q3 2027	Regiezone, IaaS, container- en dataplatform, service-integratie, acceptatie en eerste kennisoverdracht operationeel beschikbaar
Migratiegolven	Q3 2027 - Q3 2029	Gefaseerde onboarding met kleine, omkeerbare eerste golf
Einde huidig rekencentrum	31 december 2029	Bepalende einddatum; daarna geen terugval op huidige hardware

3. Voorgenomen scope en perceelstructuur

3.1 Percelen

Perceel	Kernprestatie	Marktvraag
1. IaaS en connectiviteit	Doel-IaaS, landingszone, compute, opslag, netwerk, interconnect, migratie van VMware-workloads en afbakening van het operationele beheer.	Welke IaaS-architectuur en migratieaanpak zijn nodig, en welke operationele beheeractiviteiten horen bij de perceel-1-leverancier, perceel 3 of de gemeente?
2. Managed container- en dataplatform	Levering en platformbasisdiensten door perceel 2; implementatie en eventueel beheer door platformleverancier, of implementatie en eventueel beheer van witte/P3-onderdelen door een onafhankelijke partij onder perceel 3 of beheer door de gemeente zelf.	Welk samenhangend model is marktconform: implementatie en eventueel beheer door de platformleverancier, of implementatie en eventueel beheer van witte/P3-onderdelen door een onafhankelijke partij onder perceel 3? Wanneer en hoe kan kennis en beheer aan de eigen gemeentelijke beheerafdeling worden overgedragen?
3. Service-integratie en cloudregieondersteuning	Procesintegratie, leverancierscoördinatie, FinOps, compliancebewijs, lifecycle, adoptie en exitgereedheid.	Bestaat hiervoor een zelfstandige markt en welk mandaat is minimaal nodig?
4. Digitale applicatieontsluiting	Functionele ontsluiting van grafisch-intensieve en tijdelijke lift-and-shift-applicaties.	Is een productneutrale, krimpbare dienst marktconform en afzonderlijk prijsbaar?

3.2 Gezamenlijke aanbesteding en samenhang

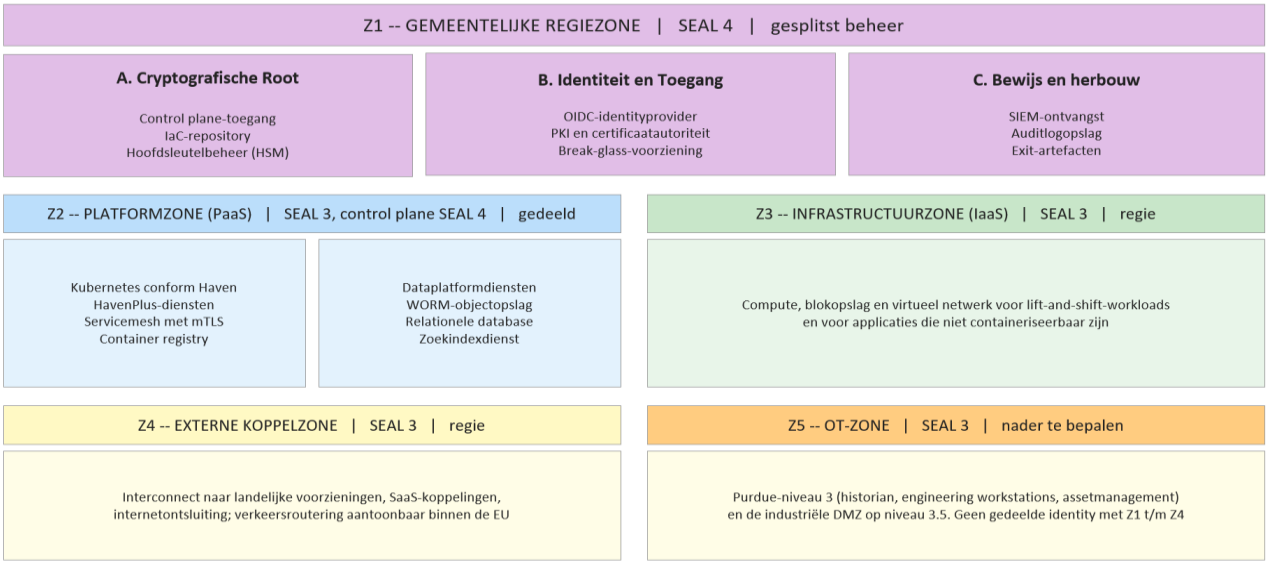
De huidige denkrichting is om percelen 1, 2 en 3 gelijktijdig in één aanbestedingsprocedure op de markt te brengen. Daarmee worden IaaS en connectiviteit, het managed container- en dataplatform en service-integratie/cloudregie vanaf de start in samenhang gecontracteerd. De aanbesteding moet duidelijke, leveranciersneutrale koppelvlakken, gezamenlijke transitieafspraken, end-to-end verantwoordelijkheden en werkbare samenwerking tussen de drie percelen borgen. Perceel 4 kan afzonderlijk en eventueel op een later moment worden aanbesteed, zonder dat dit het ontwerp of de ingebruikname van percelen 1, 2 en 3 blokkeert.

3.3 Buiten scope

- Functionele applicatiemigraties en applicatieaanpassingen, behoudens technische onboarding.
- Backup/restore-omgeving, behoudens technische aansluiting van de platformen.
- De bestaande virtualisatielaag en het beheer daarvan tot uitfasering.
- Microsoft 365 en een afzonderlijk AI-platform voor training en fine-tuning.
- Besturingslagen van OT op Purdue-niveau 0 tot en met 2.

4. Doelarchitectuur en verantwoordelijkheidsmodel

4.1 Zonemodel



Leeswijzer zonemodel. Het zonemodel toont de voorgenomen technische en organisatorische scheiding tussen gemeentelijke regie, onafhankelijke regievoorzieningen en de vier percelen. Z1A, Z1B en Z1C ondersteunen gemeentelijke zeggenschap en onafhankelijke controle. Z2 bevat het managed container- en dataplatform van perceel 2. Z3 bevat de IaaS-omgeving van perceel 1. Z4 verzorgt de externe koppelzone en interconnect. Z5 betreft uitsluitend infrastructuurdiensten voor OT, voor zover deze na afzonderlijke besluitvorming binnen de opdracht worden gebracht. Het model beschrijft een voorgenomen richting die met deze marktconsultatie wordt getoetst.

Zone	Functie	Voorgenomen positionering
Z1a	Cryptografische root: hoofdsleutels, HSM en escrow.	Eigen beheer, fysiek gescheiden van platformleveranciers.
Z1b en Z1c	Identity, control-plane-toegang, repositories, SIEM-ontvangst en bewijsopslag.	Bij onafhankelijke derde, buiten platformpercelen.
Z2	Managed container- en dataplatform.	Perceel 2.
Z3	IaaS voor niet-PaaS-geschikte workloads.	Perceel 1.
Z4	Externe koppelzone en interconnect.	Perceel 1 en waar relevant 2.
Z5	OT-infrastructuurdiensten en industriële DMZ.	Alleen na afzonderlijk scopebesluit.

4.2 Niet-uitbesteedbare verantwoordelijkheden

- Informatieclassificatie en risicoacceptatie.
- Toelatingsbeleid voor workloads en gegevens.
- Architectuurkaders en uitzonderingsbesluiten.
- Eigenaarschap van hoofdsleutels, repositories, beleidsdefinities en bewijs.
- Contract- en leveranciersregie en bestuurlijke verantwoording.
- Budgeteigenaarschap en besluitvorming over waarschuwingsdrempels.

4.3 Shared responsibility

De aanbestedende dienst zoekt per technische laag en ketendienst een expliciete verantwoordelijkheidsmatrix en RASCI, uitgebeeld in 4.4. Voor perceel 1 staat vast dat de leverancier de IaaS-dienst levert, maar nog niet wie het operationele beheer aan gemeentelijke zijde uitvoert: perceel 3 of de gemeente zelf. Voor perceel 2 wordt primair een keuze tussen twee samenhangende modellen onderzocht. Model A – uitvoering door de platformleverancier: de platformleverancier voert de technische implementatie uit van de basisinrichting binnen het platform en kan daarna ook het beheer uitvoeren; wanneer de gemeente het beheer zelf wil uitvoeren, draagt de platformleverancier kennis en beheer over aan de eigen beheerafdeling. Model B – uitvoering door een onafhankelijke beheerpartij onder perceel 3: deze partij voert op het door perceel 2 geleverde platform de technische implementatie uit van de basisinrichting binnen het platform, de onderdelen die in het grafische beheermodel wit zijn, of aan perceel 3 zijn toegewezen. Deze partij kan die onderdelen daarna beheren of kennis en beheer overdragen aan de eigen beheerafdeling van de gemeente. De platformleverancier blijft in Model B verantwoordelijk voor de levering, technische werking en lifecycle van de platformbasisdiensten en voor alle onderdelen die in het beheermodel aan perceel 2 zijn toegewezen. De marktconsultatie moet de uitvoerbaarheid, dienstgrenzen, verantwoordelijkheden, risico's, capaciteit, aansprakelijkheid, kosten en overdraagbaarheid van Model A en Model B inzichtelijk maken.

4.3.1 Security en privacy by design

Security en privacy worden vanaf het eerste ontwerp geïntegreerd in architectuur, landing zones, platformdiensten, connectiviteit, service-integratie, migratie en beheer. Beveiligingsmaatregelen worden waar mogelijk als code vastgelegd, geautomatiseerd getest en continu bewaakt. Uitgangspunten zijn least privilege, zero trust, functiescheiding, veilige standaardconfiguraties, versleuteling, onafhankelijke logging, aantoonbare hardening, beheersing van de softwareketen en herstelbaarheid na compromittering. Marktpartijen wordt gevraagd duidelijk te maken welke maatregelen standaard onderdeel zijn van de dienst, welke configureerbaar zijn en welke aanvullende gemeentelijke inrichting vereisen.

4.4 Conceptueel beheermodel per laag

Het onderstaande beheermodel is een te toetsen concept. De kolommen tonen mogelijke uitvoerders en geen blijvende rol voor de gehele looptijd. Voor perceel 3 moet onderscheid worden gemaakt tussen twee rollen. De eerste is service-integratie en cloudregieondersteuning gedurende de looptijd. De tweede is een eventuele tijdelijke technische rol bij implementatie en stabilisatie van uitsluitend de witte en aan perceel 3 toegewezen onderdelen. Indien de gemeente kiest voor overdracht van kennis en beheer aan de eigen beheerafdeling, eindigt na beheeracceptatie de technische uitvoeringsrol van de partij onder perceel 3. FinOps, SLA/OLA-bewaking, lifecyclecoördinatie, complianceondersteuning, CMDB-coördinatie en overige service-integratie worden dan door de gemeente uitgevoerd, tenzij afzonderlijk langdurige ondersteuning door perceel 3 wordt gecontracteerd. De definitieve verdeling wordt per fase vastgelegd in een RASCI.

Onderstaande modellen zijn geen besluit en vormen geen voorkeursrichting. De marktconsultatie heeft tot doel te toetsen welke verantwoordelijkheidsverdeling marktconform, uitvoerbaar en contractueel werkbaar is.

Beheermodel: wie voert welke laag uit

CONCEPT -- knip binnen perceel 2 tussen hostingpartij en beheerpartij

Blijft bij onze organisatie, over alle percelen heen				
Strategie	Governance	Architectuur	Informatiebeveiliging en privacy	Beheer Backup / DR
Functioneel beheer	Servicedesk	Applicatie- en informatie-eigenaarschap	Roadmap- en lifecyclebesluiten	Meldplicht en crisiscommunicatie

Laag		Perceel 1 IaaS en connectiviteit	Perceel 2 Container- en dataplatform (PaaS)	Perceel 3 Service-integratie en beheer	Perceel 4 Applicatieontsluiting	Onze organisatie zone Z1
Application	Applicatie	Onze organisatie	Onze organisatie	Geen eigen laag Beheert in perceel 2 de inrichting binnen de basisdiensten (paars in de kolom van perceel 2), niet de basisdiensten zelf. Daarnaast: service-integratie en coordinerende rol bij verstoringen, leveranciers- en financieel beheer, bewijsvoering, lifecyclecoordinatie, kennisborging en exitgereedheid.	Onze organisatie	Toelatingsbeleid en migratie-intake
	Toegang en applicatieontsluiting				Opdrachtnemer	Autorisatiebeheer
Data	Gegevensbeleid: schema, retentie, encryptie	Onze organisatie	Onze organisatie		Onze organisatie	Informatieclassificatie en bewaartermijnen
Runtime	Werklastbeleid en toelating (namespaces, quota, policies)		Onze organisatie		Volgt uit de inschrijving	Platformarchitectuur en toelatingsbeleid
	Databases, buckets en shares binnen de dataplatformdiensten		Beheerpartij perceel 3		Volgt uit de inschrijving	Encryptiebeleid; hoofdsleutels (Z1a)
	Componenten binnen Kubernetes (ingress, policy- en certmanagers)		Beheerpartij perceel 3		Volgt uit de inschrijving	PKI en certificaatautoriteit (Z1b)
Middleware	Databasesystemen en storage-infrastructuur		Opdrachtnemer		Volgt uit de inschrijving	Ontvangst onveranderlijke logexport (SIEM, Z1b)
	Kubernetes-basislaag (control plane, nodes, lifecycle)		Opdrachtnemer		Volgt uit de inschrijving	Control plane-toegang en identityprovider (Z1b)
Besturingssysteem		Volgt uit de inschrijving	Opdrachtnemer		Volgt uit de inschrijving	Risicoacceptatie bij end-of-support
Virtualisatie en hypervisor		Opdrachtnemer	Opdrachtnemer		Volgt uit de inschrijving	IaC-definities en configuratiebezit
Compute, opslag, netwerk en datacenter (van de dienstenleverancier of hostingpartij)		Opdrachtnemer	Opdrachtnemer		Volgt uit de inschrijving	Contract- en leveranciersregie; SLA-bewaking
Eigen infrastructuur		Kantoornetwerken, WAN-verbindingen en eigen glasvezel: bestaand bezit van onze organisatie, buiten de percelen; wel randvoorwaarde en te gebruiken als interconnect - of uitwijkroute.				
Zone Z1 -- buiten de percelen, in elk perceel eigen		Z1a: hoofdsleutels, HSM en sleutel-escrow in eigen beheer, op twee fysiek gescheiden locaties. Z1b: control plane - toegang, identityprovider met PKI, IaC-repository, SIEM-ontvangst en auditlogopslag, bij een onafhankelijke derde. Wat per laag eigen blijft, staat in de rechterkolom.				

Onze organisatie niet uitbesteedbaar	Opdrachtnemer Hostingpartij	Beheerpartij perceel 3 inrichting binnen de basisdiensten	Volgt uit de inschrijving het bestek wijst de laag niet toe	Niet in dit perceel valt buiten de opdracht

Betekenis van de open posities. De open of witte posities zijn beslispunten die met deze marktconsultatie worden gevalideerd. Marktpartijen wordt gevraagd per open positie een voorkeursverdeling te adviseren en de gevolgen daarvan te beschrijven voor beschikbaarheid, wijzigingsbevoegdheid, privileged access, incidentdiagnose, herstel, aansprakelijkheid, overdraagbaarheid en kosten. De aanbestedende dienst stelt de definitieve verantwoordelijkheidsverdeling en RASCI vóór publicatie van de aanbesteding vast.

Laag / verantwoordelijkheid	Voorgestelde uitvoerder	Blijft bij organisatie / randvoorwaarde	Status
Strategie, governance, architectuur, IB&P, eigenaarschap en risicoacceptatie	Organisatie	Niet uitbesteedbaar; uitvoering kan ondersteunend worden ingekocht	Vast uitgangspunt
Applicatie, functioneel beheer en dienstverlening aan gebruikers	Organisatie; perceel 4 voor applicatieontsluiting	Applicatie- en informatie-eigenaarschap, toelatingsbeleid en functionele acceptatie blijven intern	Perceel 4 markttoets
Gegevensbeleid, classificatie, retentie en encryptiebeleid	Organisatie	Beleid, bewaartermijnen en hoofdsleutels blijven intern of in Z1	Vast uitgangspunt
Workloadbeleid, namespaces, quota en policies	Organisatie als kadersteller; uitvoering tijdens implementatie door perceel 2 of tijdelijke beheerpartij onder perceel 3 volgens gekozen model	Na overdracht: uitvoering en wijzigingsbevoegdheid bij eigen beheerafdeling; architectuur- en toelatingsbesluit blijven intern	Fasegebonden open beslispunt
Inrichting binnen managed databases, buckets en shares	Implementatie: perceel 2 of tijdelijke beheerpartij onder perceel 3 voor witte/P3-onderdelen; beheer daarna bij dezelfde partij of na overdracht bij gemeente	Na overdracht van kennis en beheer: uitvoering, wijzigingen en herstel bij eigen beheerafdeling; gemeente bezit definities, IaC en gegevensbeleid	Fasegebonden volgens Model A of B
Kubernetes-componenten, ingress, policy- en certificaatmanagers	Implementatie en eventueel beheer: perceel 2 of tijdelijke beheerpartij onder perceel 3, uitsluitend voor witte/P3-onderdelen	Na overdracht: uitvoering en herstel bij eigen beheerafdeling; Z1 levert identity/PKI-kaders en gemeente behoudt configuratiebezit	Fasegebonden volgens Model A of B
Databasesystemen, storage-infrastructuur en platformdiensten	Platformleverancier perceel 2 gedurende de looptijd	Blijft platformbasisdienst; geen overdracht naar perceel 3. Gemeente behoudt beleids-, toegangs- en exitkaders	Vast bij perceel 2
Kubernetes-basislaag: control plane, nodes en lifecycle	Platformleverancier perceel 2 gedurende de looptijd	Blijft platformbasisdienst; partij onder perceel 3 krijgt alleen overeengekomen toegang. Gemeente behoudt regie en identity via Z1	Vast bij perceel 2
Besturingssysteem	Binnen managed dienst: perceel 1 of 2; overige uitvoering tijdelijk door perceel 3 of structureel	Na overdracht: gemeentelijke beheerafdeling voert niet-managed OS-beheer uit; risicoacceptatie en beleidskaders blijven intern	Fasegebonden open beslispunt

	door gemeente, nader te bepalen		
Virtualisatie, hypervisor, compute, opslag, netwerk en datacenter	Perceel 1 voor de IaaS-dienst; aanvullende beheerhandelingen tijdelijk door perceel 3 of structureel door gemeente, nader te bepalen	Na overdracht: gemeentelijke beheerafdeling voert de overeengekomen beheerhandelingen uit; IaC, exitvereisten en onafhankelijke aantoonbaarheid blijven gemeentelijk geborgd	Marktconsultatie toetst dienstgrens en fase
Service-integratie, SLA/OLA-bewaking, FinOps, bewijs en exitcoördinatie	Tijdens implementatie/stabilisatie: perceel 3 of gemeente; na overdracht: gemeente, tenzij langdurige ondersteuning door perceel 3 afzonderlijk wordt gecontracteerd	Contract- en leveranciersregie blijft altijd bij organisatie; bij volledige overdracht voert gemeente FinOps, SLA/OLA-bewaking, lifecycle- en compliancecoördinatie uit	Looptijd en exitcriterium open beslispunt
Technische uitvoering en herstel	Perceel 1 en perceel 2 binnen hun managed dienstgrenzen; witte/P3-onderdelen tijdens implementatie en eventueel beheer door perceel 3, of na overdracht door gemeente	Na beheeracceptatie: eigen beheerafdeling verantwoordelijk voor overgedragen uitvoering en herstel; leveranciers blijven verantwoordelijk binnen hun managed dienstgrenzen	Fasegebonden volgens definitieve RASCI

Marktvraag (zie Excel invuldocument): beschrijf per fase wie verantwoordelijk is en wanneer die verantwoordelijkheid eindigt. Voor perceel 1 wordt getoetst welke operationele IaaS-beheeractiviteiten tijdelijk of structureel bij perceel 3 kunnen worden belegd en welke de gemeente zelf uitvoert. Voor perceel 2 wordt Model A vergeleken met Model B. Indien in Model B de partij onder perceel 3 alleen implementeert en daarna kennis en beheer overdraagt, heeft die partij na beheeracceptatie uitsluitend nog nazorg- en garantieverplichtingen. FinOps, SLA/OLA-bewaking, lifecyclecoördinatie, complianceondersteuning, CMDB-coördinatie en overige service-integratie worden dan door de gemeente uitgevoerd, tenzij langdurige ondersteuning door perceel 3 afzonderlijk wordt gecontracteerd. Benoem per fase de RASCI, toegangsrechten, exitcriteria, benodigde gemeentelijke capaciteit, kosten en terugvalmogelijkheid.

4.5 Perceel 1: IaaS en migratie vanuit VMware

Perceel 1 omvat de levering van de doel-IaaS en de technische migratie vanuit de huidige VMware Cloud Foundation-omgeving. De marktconsultatie behandelt daarbij drie samenhangende maar afzonderlijke vragen. Ten eerste wordt gevraagd hoe de aangeboden IaaS technisch is ingericht, waaronder virtualisatietechnologie, compute, opslag, netwerk, beheer- en automatiseringslaag, control plane, beschikbaarheidsmodel, locaties, licenties en portabiliteit. Ten tweede wordt gevraagd hoe de migratie vanuit VMware naar deze doelomgeving wordt uitgevoerd. Ten derde wordt de grens van het operationele beheer getoetst: welk beheer is onlosmakelijk onderdeel van de IaaS-dienst van perceel 1 en welke beheeractiviteiten aan gemeentelijke zijde kunnen door perceel 3 of door de gemeente zelf worden uitgevoerd. De onderstaande onderwerpen geven aan waarop de markt haar aanpak, aannames, verantwoordelijkheidsverdeling, planning en prijsdrijvers moet toelichten:

- Afbakening van het operationele IaaS-beheer tussen de perceel-1-leverancier, perceel 3 en de gemeente, inclusief VM-provisioning, OS-beheer, configuratie, monitoring, back-upaansturing, changes, incidentdiagnose, privileged access, capaciteitsbeheer en CMDB.
- Inventarisatie en discovery van virtuele machines, afhankelijkheden, netwerkstromen, opslag, back-up, licenties en technische schuld.
- Classificatie per workload in rehost, replatform, refactor, retire, retain of replace, met expliciete besliscriteria en uitzonderingsproces.
- Keuze en onderbouwing van de doel-IaaS, inclusief hypervisor- of cloudafhankelijkheden, operating systems, databases, appliances en licentieportabiliteit.
- Ontwerp van landing zones, netwerksegmentatie, IP- en DNS-migratie, identity, certificaten, secrets, logging, monitoring, back-up en security controls.
- Migratiegolven met pilot/canary, technische acceptatie, prestatie- en hersteltests, cutover, rollback, hypercare en decommissioning.
- Migratietooling en overdraagbare artefacten, waaronder discoverydata, wave plans, mappings, runbooks, scripts, IaC, testbewijs en CMDB-updates.
- Behandeling van workloads die niet direct migreerbaar zijn, waaronder legacy operating systems, hardwaregebonden licenties, appliances, latencygevoelige koppelingen en afhankelijkheden met het resterende rekencentrum.
- Prijsmodel en capaciteit voor reguliere IaaS, tijdelijke dubbele infrastructuur, datatransport, migratietooling, specialistische uren en terugvalvoorzieningen.

4.5.1 Connectiviteit, internet en interconnect

Connectiviteit vormt een ketendienst tussen de IaaS-omgeving, het managed container- en dataplatform, Z1, kantooromgevingen, internet, SaaS-diensten, ketenpartners en het resterende rekencentrum. De gemeente wil de markt laten adviseren over het doelmodel en vergelijkt daarbij ten minste twee opties voor internet-egress: een private verbinding naar een door de gemeente bepaalde centrale egressvoorziening en internet-egress als beheerde dienst van de leverancier. Ook hybride of decentrale varianten mogen worden voorgesteld wanneer deze aantoonbaar doelmatiger of veiliger zijn.

De markt wordt gevraagd in te gaan op gemeentelijke publieke IP-adressen en het eigen BGP-AS, BGP en RPKI/ROA, IPv4/IPv6, private interconnects, verbindingen naar kantooromgevingen, route- en carrierdiversiteit, netwerksegmentatie, DDoS-bescherming, DNS/DNSSEC, firewalls en egressbeperking, monitoring, onafhankelijke SIEM-export, beschikbaarheid, RASCI, portabiliteit, kosten en exit. Uitgangspunt is dat schijnredundantie wordt voorkomen en dat fysieke en logische afhankelijkheden aantoonbaar zijn.

Connectiviteitsarchitectuur voor internet, gemeentelijke kantooromgevingen, het resterende rekencentrum, Z1, SaaS-diensten, ketenpartners en private interconnects tussen platformen, inclusief routing, BGP, segmentatie, redundantie, beveiliging, monitoring, servicelevels, verantwoordelijkheden en prijsmodel.

4.6 Perceel 2: managed container- en dataplatform

Perceel 2 omvat de levering en technische werking van het managed container- en dataplatform en van de platformbasisdiensten die in het grafische beheermodel aan perceel 2 zijn toegewezen. De marktconsultatie toetst niet alle denkbare combinaties van implementatie en beheer, maar twee samenhangende modellen. In beide modellen blijft de platformleverancier verantwoordelijk voor de platformbasisdiensten en de onderdelen die in het beheermodel aan perceel 2 zijn toegewezen.

Model A – implementatie door de platformleverancier. De platformleverancier voert ontwerp, bouw, implementatie en stabilisatie uit. Daarna blijft het beheer bij dezelfde platformleverancier, tenzij de gemeente kiest voor overdracht van kennis en beheer aan de eigen beheerafdeling. Een overgang van implementatie door de platformleverancier naar beheer door een onafhankelijke derde partij onder perceel 3 is niet voorzien.

Model B – implementatie door een onafhankelijke beheerpartij onder perceel 3. Deze partij voert ontwerp, bouw, implementatie en stabilisatie uit, maar uitsluitend voor de witte onderdelen en de onderdelen die in het grafische beheermodel aan perceel 3 zijn toegewezen. De partij kan deze onderdelen daarna beheren of kennis en beheer overdragen aan de eigen beheerafdeling van de gemeente. De platformleverancier blijft verantwoordelijk voor de platformbasisdiensten en de aan perceel 2 toegewezen onderdelen.

De markt wordt gevraagd beide modellen te beoordelen op marktconformiteit, eenduidige verantwoordelijkheid, dienstgrenzen, benodigde toegangs- en wijzigingsrechten, continuïteit, gemeentelijke capaciteit, kennisborging, aansprakelijkheid, kosten, beheeracceptatie en overdraagbaarheid. De onderstaande onderwerpen geven aan waarop de markt haar antwoord moet toelichten:

- Technische architectuur van Kubernetes en managed data- en platformdiensten.
- Dienstgrens met perceel 1 voor compute, opslag, netwerk, operating systems, back-up, monitoring en herstel.
- Verantwoordelijkheid voor lifecycle, patching, hardening, beschikbaarheid, incidentdiagnose en herstel tijdens implementatie en stabilisatie, en de mogelijke overdracht van kennis en beheer voor de beheerfase.
- Verdeling van configuratie- en wijzigingsrechten.
- Levering van verbruiksgegevens, logs, configuratiestatus en lifecycle-informatie.
- Overdraagbaarheid van IaC, repositories, configuraties, runbooks, documentatie, tooling, licenties, supportcontracten, privileged access en leveranciersrelaties, inclusief beheeracceptatie en nazorg.
- Prijsmodel voor basisplatform, managed diensten, beheer, groei, krimp, redundantie en exit.

4.7 Perceel 3: service-integratie en cloudregieondersteuning

Perceel 3 kan twee verschillende soorten dienstverlening omvatten. Ten eerste kan een onafhankelijke beheerpartij onder perceel 3 tijdelijk de technische implementatie en stabilisatie uitvoeren van de witte en aan perceel 3 toegewezen onderdelen van perceel 2. Ten tweede kan perceel 3 service-integratie en ondersteuning van de gemeentelijke cloudregie leveren, waaronder ketenmonitoring, incidentcoördinatie, SLA/OLA-bewaking, FinOps, lifecycle- en CMDB-coördinatie, complianceondersteuning en exitgereedheid. Deze rollen hoeven niet dezelfde looptijd te hebben. Wanneer na implementatie kennis en beheer naar de eigen beheerafdeling worden overgedragen en de gemeente ook de regieactiviteiten zelf uitvoert, eindigen de uitvoerende en ondersteunende verantwoordelijkheden van perceel 3 na beheeracceptatie en nazorg. Alleen wanneer dit afzonderlijk wordt besloten en gecontracteerd, blijft perceel 3 daarna langdurige service-integratie of cloudregieondersteuning leveren. De marktconsultatie moet duidelijk maken welke diensten tijdelijk en welke eventueel structureel worden aangeboden, met welk mandaat, welke toegang en welk prijsmodel.

SIAM en servicemanagement als te toetsen inrichtingsmodel. De aanbestedende dienst onderzoekt welk servicemanagement- en service-integratiemodel passend is en in hoeverre SIAM daarbij bruikbaar is. De markt wordt gevraagd of zij 24/7 als hoofdaannemer of lead-provider kan optreden, andere leveranciers via OLA's operationeel kan aansturen en welke contractuele positie, aansprakelijkheid, escalatie en technische arbitrage daarvoor nodig zijn. Tevens wordt gevraagd welke standaard Producten- en Dienstencatalogus, SLA/OLA-structuur, processen, tooling en rapportages beschikbaar zijn en waar maatwerk mogelijk of noodzakelijk is. De gemeente blijft eigenaar van strategie, architectuur, beleid, contractregie, risicoacceptatie en bestuurlijke verantwoording.

- Ketenmonitoring, incidentcoördinatie, problem management, change-afstemming en escalatie.
- SLA- en OLA-bewaking, technische arbitrage en voorkoming van ticket-bouncing.
- FinOps, kostentoerekening, forecasting en ondersteuning van budgetsturing.
- Coördinatie en controle van informatie voor onafhankelijke aantoonbaarheid.
- Lifecyclecoördinatie, CMDB-samenhang en onderhoudskalenders.
- Kennisoverdracht en ondersteuning voor zelfstandige gemeentelijke regie.
- Benodigde read-only toegang, eventuele uitvoeringsrechten en functiescheiding.
- Prijsmodel voor service-integratie, rapportage, FinOps, transitie en exitcoördinatie.

4.8 Perceel 4: digitale applicatieontsluiting

Perceel 4 staat los van de gezamenlijke aanbesteding van percelen 1, 2 en 3, maar wordt in deze marktconsultatie wel inhoudelijk verkend. De huidige Omnissa Horizon-omgeving verdwijnt mee met het eigen rekencentrum. Het langetermijndoel is dat processen en applicaties vanuit een browser toegankelijk zijn. Voor een tijdelijke of blijvende restgroep blijft echter gerichte applicatieontsluiting nodig, met name voor grafisch-intensieve applicaties en voor applicaties die tijdelijk via lift-and-shift op perceel 1 worden gehost. De uitvraag blijft productneutraal: de markt wordt gevraagd oplossingsrichtingen, leveringsmodellen en afhankelijkheden te beschrijven, zonder dat vooraf VDI, DaaS, RDS, applicatiestreaming of een specifiek product wordt voorgeschreven. De onderstaande opsomming benoemt de onderwerpen waarop de markt voor perceel 4 wordt gevraagd oplossingsrichtingen, afhankelijkheden, leveringsmodellen, migratieaanpak en prijsdrijvers toe te lichten:

- Geschikte oplossingspatronen voor grafisch-intensieve, latencygevoelige, legacy- en tijdelijk gehoste applicaties.
- Samenhang met de IaaS-omgeving van perceel 1, waaronder nabijheid van workloads, netwerkvertraging, identity, profiel- en bestandsdiensten, printing, randapparatuur en GPU-capaciteit.
- Veilig ontsluitingsmodel voor beheerde en onbeheerde endpoints, inclusief browsertoegang, clientsoftware, MFA, conditional access, sessie-isolatie, logging en gegevensuitwisseling.
- Productneutraliteit en scheiding tussen functionele dienst, broker/control plane, compute, images, applicatiepackaging en beheer.
- Migratiepad vanuit Omnissa Horizon, inclusief coexistence, image- en applicatiemigratie, profielen, gebruikersacceptatie, rollback en uitfasering.
- Krimpbaar prijsmodel dat past bij een tijdelijke restgroep, seizoenspieken, gelijktijdigheid, GPU-profielen en afnemende volumes.
- Exit en portabiliteit van images, packages, profielen, configuratie, logging en documentatie.

5. Inhoudelijke consultatiethema’s

Per thema is hieronder één hoofdvraag opgenomen. De hoofdvragen geven aan welke richting de aanbestedende dienst met de markt wil toetsen. De markt wordt gevraagd de antwoorden te onderbouwen met bestaande dienstverlening, relevante aannames, afhankelijkheden, risico’s, prijsdrijvers en waar nodig een alternatief. De concrete beantwoording vindt plaats in het Excel-invuldocument.

5.1 Marktconformiteit van percelen en fasering

Hoofdvraag: leidt de voorgenomen perceelindeling, met gelijktijdige aanbesteding van percelen 1, 2 en 3 en een afzonderlijke positionering van perceel 4, tot voldoende mededinging, eenduidige verantwoordelijkheid en uitvoerbare samenwerking tussen leveranciers? Benoem welke combinaties, onderaannemingsconstructies, koppelvlakken en contractuele afspraken vóór aanbesteding moeten worden vastgelegd.

5.2 Soevereiniteit en jurisdictie

Hoofdvraag: in hoeverre kan de markt voldoen aan de voorgenomen eisen voor SEAL-niveau 3, EU/EER-locaties en beheer, onafhankelijke regievoorzieningen, control planes, eigendom en zeggenschap, subverwerkers en bescherming tegen derde-landwetgeving? Geef aan welke onderdelen standaard beschikbaar zijn, welke maatregelen aanvullend nodig zijn en wat de gevolgen zijn voor mededinging en prijs.

5.3 Architectuur, standaarden en portabiliteit

Hoofdvraag: hoe ondersteunt de aangeboden oplossing open standaarden, portabiliteit, open source en het Common Ground-gedachtengoed? Beschrijf de ondersteuning voor Haven, Kubernetes, S3, OIDC, SCIM, OpenTelemetry, Infrastructure as Code en gemeentelijke repositories. Licht toe hoe scheiding van gegevens,

services en interactie, gegevensontsluiting bij de bron, federatieve identity, herbruikbare componenten en gemeentelijke regie op gegevens en autorisaties worden ondersteund. Benoem per hoofdcomponent of deze open source, open core of proprietary is, inclusief licentie, upstream community, supportmodel, noodzakelijke commerciële extensies, risico op een leveranciersspecifieke fork en het terugval- of migratiepad. Open source heeft de voorkeur waar dit aantoonbaar bijdraagt aan transparantie, controleerbaarheid, herbruikbaarheid, portabiliteit en beperking van leveranciersafhankelijkheid, zonder afbreuk te doen aan professioneel beheer, security, lifecycle en continuïteit.

5.4 Platform- en datadiensten

Hoofdvraag: welke container-, data- en platformdiensten kan de markt als bestaande managed dienst leveren, met welke verantwoordelijkheidsgrenzen, servicelevels, beperkingen en prijsmodellen? Betrek minimaal databases, objectopslag met retentie en legal hold, bestandssystemen, zoekindex, streaming, cache, secrets, certificaten en observability. Neem, indien geboden, ook ondersteunend platform voor AI-inference op in uw beschrijving.

5.5 Security, identity en softwareketen

Hoofdvraag: hoe integreert de markt security en privacy vanaf ontwerp, bouw en configuratie en hoe maakt de leverancier de werking gedurende de looptijd aantoonbaar? Beschrijf threat modelling, secure-by-default, least privilege, zero trust, functiescheiding, policy as code, hardening en softwareketenbeveiliging. Ga tevens in op securitylogging en near-real-time SIEM-ontsluiting, forensische ondersteuning, kwetsbaarhedenbeheer en patchtermijnen, configuratiebeheer en driftdetectie, 24/7-securitymonitoring en incidentrespons, ketenverantwoordelijkheden, auditbaarheid tegen AVG, BIO2, ISO/IEC 27001 en waar toepasselijk de Cyberbeveiligingswet, en cryptografie voor data-at-rest, data-in-transit en beheercommunicatie. Beschrijf crypto-agility en de roadmap naar post-quantum cryptografie. Geef aan wat standaard, configureerbaar of aanvullend is en welk bewijs bij inschrijving of pas bij acceptatie beschikbaar kan zijn.

5.6 Continuïteit en herstel

Hoofdvraag: welke continuïteits- en herstelpatronen zijn per workloadprofiel technisch haalbaar en proportioneel? Beschrijf de inzet van failure domains, geo-redundantie, multi-stack, directe omschakeling, RTO/RPO, herstel buiten de primaire leverancier, back-upkoppelvlakken en periodieke hersteltests, inclusief de gevolgen voor kosten en beheercomplexiteit.

5.7 Tenant-, privacy- en archiefscheiding

Hoofdvraag: hoe realiseert de markt aantoonbare scheiding tussen drie tenants en de afzonderlijke verantwoordelijkheden van twee gemeenten binnen de gezamenlijke ambtelijke tenant? Beschrijf scheiding op identity-, netwerk-, opslag-, logging-, beheer- en rapportageniveau en hoe zeggenschap, export, vernietiging, WORM/Object Lock, bewaartermijnen, kosten en verwerkersrelaties per gemeente en tenant afzonderlijk worden uitgevoerd. Licht tevens toe hoe zonder fundamenteel herontwerp een regionale dienst of andere ondersteunde organisatie kan worden toegevoegd, inclusief onboarding, tenant- en datascheiding, servicelevels, licenties, minimale afname, kostenverdeling en governance.

5.8 Beheer, service-integratie en kennis

Hoofdvraag: welk implementatie-, beheer- en service-integratiemodel is passend tijdens ontwerp, bouw, implementatie, stabilisatie, overdracht en reguliere exploitatie? Beoordeel voor perceel 1 of het operationele IaaS-beheer aan gemeentelijke zijde tijdelijk of structureel door perceel 3 kan worden uitgevoerd of bij de gemeente moet blijven. Vergelijk voor perceel 2 Model A en Model B en maak per model expliciet wanneer verantwoordelijkheden eindigen. Indien kennis en beheer aan de eigen beheerafdeling worden overgedragen en de gemeente de regie zelf voert, komen na beheeracceptatie ook FinOps, SLA/OLA-bewaking, lifecyclecoördinatie, complianceondersteuning en overige service-integratie bij de gemeente te liggen. Langdurige ondersteuning door perceel 3 is dan alleen aan de orde wanneer deze afzonderlijk wordt besloten en gecontracteerd. Beschrijf per fase

rollen, RASCI, einddata of exitcriteria, mandaat, toegang, 24/7-verantwoordelijkheid, gemeentelijke capaciteit, beheeracceptatie, tooling, kosten en nazorg.

5.9 FinOps en prijsmodel

Hoofdvraag: welk prijs- en verbruiksmodel maakt groei en krimp mogelijk, waarbij financiële consequenties vooraf voorspelbaar en achteraf controleerbaar zijn? Beschrijf kostentoerekening, minimumafname, commitments, egress, loggingkosten, migratiepieken, benchmarks, waarschuwingsdrempels en exitkosten.

5.10 Transitie, adoptie en planning

Hoofdvraag: welke aanpak, capaciteit en beslismomenten zijn nodig om het cloudfundament in Q3 2027 beschikbaar te hebben en het huidige rekencentrum uiterlijk 31 december 2029 uit te faseren? Beschrijf voor perceel 1 de VMware-discovery, 6R-classificatie, migratiefabriek, landing zones, migratiegolven, cutover, rollback, hypercare en decommissioning, en voor perceel 2 de golden paths, onboarding en adoptie.

5.11 Digitale applicatieontsluiting

Hoofdvraag: welke productneutrale en krimpbare oplossingen zijn beschikbaar voor digitale applicatieontsluiting, hoe hangen deze samen met perceel 1 en hoe kan gecontroleerd vanuit Omnissa Horizon worden gemigreerd?

5.12 OT

Hoofdvraag: Beschrijf onder welke technische, security- en beheervoorwaarden OT-infrastructuurdiensten verantwoord binnen het doelplatform kunnen landen.

5.13 Duurzaamheid

Hoofdvraag: welke betrouwbare en vergelijkbare gegevens kan de markt leveren over energiegebruik, emissies, watergebruik en circulariteit? Beschrijf hoe deze informatie aan capaciteit, beschikbaarheid, databehoud en kosten kan worden gekoppeld zonder een disproportionele rapportagelast te veroorzaken.

5.14 Connectiviteit, internet en netwerkbeveiliging

Hoofdvraag: welk connectiviteitsmodel adviseert de markt voor veilige, beschikbare en beheersbare communicatie tussen de cloudplatformen, gemeentelijke kantooromgevingen, internet, SaaS-diensten, ketenpartners, Z1 en het resterende rekencentrum? Vergelijk private verbinding naar een centrale gemeentelijke egressvoorziening met internet-egress als leveranciersdienst en beschrijf eventuele hybride varianten. Ga in op gebruik van het gemeentelijke publieke IP-blok en BGP-AS, BGP/RPKI/ROA, private interconnects, carrier- en route-diversiteit, netwerksegmentatie, DDoS, DNS/DNSSEC, monitoring, SIEM-export, beschikbaarheid, verantwoordelijkheden, portabiliteit, kosten en exit.

6. Specifieke hypothesen die de marktconsultatie moet toetsen

ID	Te toetsen hypothese
H1	Voor perceel 2 zijn Model A en Model B uitvoerbaar als verantwoordelijkheden per fase worden vastgelegd. In Model B kan de partij onder perceel 3 implementeren en eventueel beheren, of na implementatie kennis en beheer overdragen aan de eigen beheerafdeling van de gemeente. Bij volledige overdracht eindigen na beheeracceptatie ook FinOps, SLA/OLA-bewaking, lifecyclecoördinatie, complianceondersteuning en overige service-integratie door perceel 3, tenzij deze diensten afzonderlijk langdurig worden gecontracteerd.

ID	Te toetsen hypothese
H2	Voor perceel 3 bestaat een zelfstandige markt die service-integratie, FinOps, compliancebewijs, lifecyclecoördinatie en exitgereedheid kan verzorgen zonder technisch eigenaarschap over de platformlagen.
H3	De scheiding van Z1a, Z1b en Z1c buiten de platformleverancier is technisch uitvoerbaar zonder onaanvaardbare beschikbaarheids- of beheerrisico's.
H4	SEAL 3 als minimum voor alle percelen is aantoonbaar en laat voldoende mededinging over.
H5	Parallelle multi-stack inzet met directe omschakeling is voor alle relevante workloads haalbaar en proportioneel, of kan verantwoord per workloadprofiel worden gedifferentieerd.
H6	Herstel door een onafhankelijke derde buiten de primaire leveranciersomgeving is technisch en contractueel realiseerbaar.
H7	Een gelijktijdige aanbesteding van percelen 1, 2 en 3 is uitvoerbaar, mits koppelvlakken, gezamenlijke transitieafspraken, end-to-end verantwoordelijkheden en samenwerking tussen leveranciers vooraf zijn vastgelegd.
H8	De voorgestelde knock-outset kan worden beperkt tot voorwaarden die vóór gunning objectief aantoonbaar en niet redelijk herstelbaar zijn.
H9	Een verbruiksgebaseerd model met begrensde minimumafname, transparante krimp en afzonderlijke migratiepiek is marktconform. Het moet mogelijk zijn eenvoudig op- en af te schalen en de financiële consequenties moeten vooraf bekend zijn.
H10	De einddatum 31 december 2029 is haalbaar als besluitvorming, regiezone, acceptatie en eerste migratiegolf tijdig worden afgerond.
H11	Een industriële migratieaanpak vanuit de bestaande VMware-omgeving naar de doel-IaaS is binnen de planning uitvoerbaar, mits discovery, workloadclassificatie, landing zones, migratietooling, verantwoordelijkheden, tijdelijke dubbele capaciteit en rollback vooraf zijn ingericht.
H12	Voor perceel 4 bestaat een productneutrale, zelfstandig contracteerbare en krimpbare marktoplossing die grafisch-intensieve en tijdelijk op IaaS gehoste applicaties veilig ontsluit en gecontroleerd vanuit de huidige Omnissa Horizon-omgeving kan worden ingevoerd.

7. Reactie-instructie voor marktpartijen

Marktpartijen beantwoorden alleen de vragen die relevant zijn voor de percelen, rollen of specialistische diensten die zij kunnen leveren. Het invuldocument hoeft dus niet volledig te worden ingevuld door partijen die slechts één of enkele percelen leveren. Vermeld duidelijk welke onderdelen worden overgeslagen en benoem afhankelijkheden van andere percelen en leveranciers. Antwoorden mogen verwijzen naar bijlagen, mits per verwijzing duidelijk is welk vraagnummer wordt onderbouwd. Geef aan of een antwoord betrekking heeft op een standaarddienst, configureerbare dienst, maatwerk, partnerdienst of roadmap.

7.1 Gewenste antwoordkwaliteit

- Maak onderscheid tussen bewezen beschikbaar, configureerbaar, maatwerk en roadmap.
- Benoem aannames, afhankelijkheden, uitsluitingen en benodigde besluiten expliciet.
- Geef aan welk bewijs bij inschrijving en welk bewijs pas bij acceptatie kan worden geleverd.
- Maak prijsdrijvers en drempeleffecten inzichtelijk; een definitieve offerte is niet nodig.
- Benoem alternatieven als een uitgangspunt niet haalbaar of niet proportioneel is.
- Vermeld per antwoord op welke percelen en rollen het betrekking heeft.

7.2 Vertrouwelijkheid

Markeer bedrijfsvertrouwelijke informatie herkenbaar. De aanbestedende dienst kan een openbaar of met deelnemers gedeeld consultatieverslag opstellen waarin reacties geanonimiseerd en geaggregeerd worden weergegeven.

7.3 Indicatieve consultatieprocedure

Stap	Toelichting
1. Publicatie	Outline en invuldocument worden beschikbaar gesteld. Het onderliggende Programma van Eisen wordt niet meegestuurd.
2. Schriftelijke reactie	Marktpartijen leveren het ingevulde document en eventuele bijlagen aan.
3. Verdiepende gesprekken	De aanbestedende dienst kan partijen uitnodigen voor toelichting op specifieke thema's.
4. Analyse	Reacties worden thematisch en geaggregeerd beoordeeld.
5. Terugkoppeling	Waar passend wordt een geanonimiseerd consultatieverslag gepubliceerd of gedeeld.
6. Verwerking	PvE, percelen, eisen, verificatie, prijsblad en planning worden aangescherpt.

8. Relatie tussen outline en invuldocument

Deze outline beschrijft zelfstandig de context, uitgangspunten, scope en thema's van de marktconsultatie. Het Excel-invuldocument bevat de concrete vragen waarmee de markt wordt uitgenodigd de denkrichting te toetsen. Het onderliggende Programma van Eisen is vooralsnog uitsluitend een intern brondocument en wordt niet met de marktconsultatie meegestuurd. Bij verschillen geldt dat de vragen in het invuldocument leidend zijn voor de gevraagde reactie.

Bijlage A. Begrippenlijst

Deze begrippenlijst licht termen toe die in de outline en het invuldocument worden gebruikt. De omschrijvingen zijn bedoeld als leeswijzer voor de marktconsultatie en vervangen geen definitie die later in de aanbestedingsdocumenten of overeenkomst wordt vastgesteld.

Begrip	Betekenis in deze marktconsultatie
6R-classificatie	Indeling van workloads in rehost, replatform, refactor, retire, retain of replace om per workload een migratiestrategie te bepalen.
AI-inference	Het toepassen van een bestaand AI-model op nieuwe invoer. Training en fine-tuning vallen buiten de in deze marktconsultatie bedoelde platformfunctie.
Common Ground	Informatiekundige visie voor de gemeentelijke informatievoorziening, gericht op onder meer scheiding van gegevens, services en interactie, gestandaardiseerde gegevensuitwisseling, herbruikbare voorzieningen en gemeentelijke regie op gegevens.
Control plane	Besturingslaag waarmee infrastructuur- en platformdiensten worden geconfigureerd, georkestreerd en beheerd. Het datavlak verwerkt het feitelijke netwerk- of applicatieverkeer.
Cyber recovery	Voorbereide en beproefde herstelcapaciteit voor scenario's zoals ransomware, gecompromitteerde identity, corrupte configuratie, sleutelverlies of besmette replicatie.
Datavlak	Technische laag waar het feitelijke gegevens- en netwerkverkeer wordt verwerkt, onderscheiden van de control plane die de dienst bestuurt.
Egress	Gegevensverkeer dat een cloudomgeving, regio of leveranciersdomein verlaat. Hiervoor kunnen technische beperkingen of afzonderlijke kosten gelden.
Failure domain	Afgebakend onderdeel van een infrastructuur waarvan een storing niet automatisch andere onderdelen hoort te raken, bijvoorbeeld een rack, beschikbaarheidszone of regio.
FinOps	Werkwijze voor financieel beheer van cloudgebruik, waaronder kostentoerekening, forecasting, budgetbewaking, anomaliedetectie en optimalisatie.
Golden path	Door de platformorganisatie ondersteunde standaardroute met vooraf ingerichte templates, beveiligingsmaatregelen, pipelines en beheerafspraken voor het onboarden van workloads.
Haven	Nederlandse standaard en referatie voor overdraagbare cloud-native platformen op basis van onder meer Kubernetes, gericht op interoperabiliteit en voorkoming van leveranciersafhankelijkheid.

HSM	Hardware Security Module: beveiligd apparaat voor het genereren, bewaren en gebruiken van cryptografische sleutels.
IaC / Infrastructure as Code	Het reproduceerbaar vastleggen en beheren van infrastructuurconfiguratie in versiebeheerbare code, bijvoorbeeld met Terraform, OpenTofu, Ansible of leveranciersspecifieke templates.
JIT-toegang	Just-in-time toegang: verhoogde toegangsrechten worden alleen voor een beperkte tijd en na autorisatie verstrekt.
Legal hold	Blokkade op verwijdering of wijziging van gegevens vanwege juridische, onderzoeks- of archiefverplichtingen, ongeacht de normale bewaartermijn.
Managed dienst	Dienst waarbij de leverancier vooraf overeengekomen technische beheeractiviteiten uitvoert en verantwoordelijk is voor onder meer beschikbaarheid, lifecycle, patching en herstel binnen de vastgestelde dienstgrens.
mTLS	Mutual Transport Layer Security: wederzijdse authenticatie waarbij beide communicatiepartijen een certificaat gebruiken.
Multi-stack	Gelijktijdige of uitwijkbare inzet van meer dan één technologiestack om afhankelijkheid en herstelrisico te beperken. De precieze reikwijdte wordt per workloadprofiel bepaald.
Object Lock / WORM	Techniek waarmee objecten gedurende een bewaartermijn niet kunnen worden gewijzigd of verwijderd. WORM staat voor Write Once Read Many.
OLA	Operational Level Agreement: operationele afspraak tussen interne teams of leveranciers die nodig is om een bovenliggende SLA te kunnen behalen.
Open core	Leveringsmodel waarbij een basisproduct open source is, maar aanvullende beheer-, security- of enterprisefunctionaliteit alleen onder een commerciële licentie beschikbaar is.
OpenTelemetry	Open standaard voor het verzamelen en exporteren van traces, metrics en logs ten behoeve van observability.
Privileged access	Beheer- of systeemtoegang met verhoogde rechten waarmee configuraties, gegevens of beveiligingsinstellingen kunnen worden gewijzigd.
Provenance	Herleidbare informatie over de oorsprong, samenstelling en bouwstappen van softwareartefacten, bijvoorbeeld wie een image heeft gebouwd en uit welke broncode en dependencies.
RASCI	Verantwoordelijkheidsmodel met Responsible, Accountable, Supporting, Consulted en Informed. Het model maakt per activiteit duidelijk wie uitvoert,

	eindverantwoordelijk is, ondersteunt, wordt geraadpleegd of wordt geïnformeerd.
RPO	Recovery Point Objective: maximaal aanvaardbaar gegevensverlies, uitgedrukt als tijd tussen het laatste herstelbare gegevenspunt en een verstoring.
RTO	Recovery Time Objective: maximaal beoogde tijd waarbinnen een dienst na een verstoring moet zijn hersteld.
SBOM	Software Bill of Materials: machineleesbare inventaris van softwarecomponenten en dependencies in een applicatie, image of platformcomponent.
SEAL	Sovereignty Effectiveness Assurance Level uit het EU Cloud Sovereignty Framework. Het niveau geeft aan in welke mate soevereiniteitsmaatregelen aantoonbaar zijn geborgd.
Security by design	Werkwijze waarbij security en privacy vanaf het eerste ontwerp worden geïntegreerd in architectuur, configuratie, automatisering, processen, testen en lifecyclemanagement.
Service mesh	Infrastructuurlaag voor communicatie tussen services, met functies zoals encryptie, authenticatie, verkeerssturing en observability.
Service-integratie	Coördinatie en bewaking van dienstverlening over meerdere leveranciers, waaronder ketenincidenten, SLA/OLA-bewaking, rapportage, escalatie, lifecyclecoördinatie en exitgereedheid.
SIAM	Service Integration and Management: framework voor het organiseren, integreren en bewaken van dienstverlening in een ecosysteem met meerdere leveranciers, met expliciete rollen, verantwoordelijkheden en ketenprocessen.
SLA	Service Level Agreement: contractuele afspraak over meetbare dienstverleningsniveaus, zoals beschikbaarheid, hersteltermijnen en responstijden.
Switching costs	Eenmalige en structurele kosten en inspanningen die ontstaan bij het overstappen naar een andere leverancier of technologiestack, inclusief migratie, conversie, kennisopbouw en tijdelijke dubbele capaciteit.
Tenant	Logisch en organisatorisch afgescheiden gebruikscontext met eigen identities, autorisaties, gegevens, configuraties, logging en kostentoerekening.
Ticket-bouncing	Situatie waarin leveranciers incidenten of verzoeken herhaaldelijk naar elkaar doorzetten omdat eigenaarschap, diagnose of herstelverantwoordelijkheid onvoldoende duidelijk is.

Upstream	Het oorspronkelijke open-sourceproject of de community waar code, releases en beveiligingsupdates worden ontwikkeld, voordat een leverancier daarvan een distributie of beheerde dienst maakt.
WORM	Write Once Read Many: gegevens kunnen na vastlegging gedurende de ingestelde termijn niet worden gewijzigd of verwijderd.
Z1 / regiezone	Onafhankelijke zone voor gemeentelijke zeggenschap en controle, waaronder cryptografische roots, identity, repositories, SIEM-ontvangst en bewijsopslag, buiten de reguliere platformleveranciers.