

Verslag marktconsultatie

Netwerkdiensten openbare ruimte

Aanbestedingsnummer 2026SB1042

TenderNed-kenmerk: TN598613

5 oktober 2026

Versie 1.0

Definitief

1 Verslag

1.1 Aanleiding van deze marktconsultatie

De gemeente Utrecht¹ bereidt zich voor op een aanbesteding “Netwerkdiensten in de Openbare Ruimte”. In dit kader heeft de gemeente een marktconsultatie uitgevoerd.

1.2 Doel van de marktconsultatie

De gemeente heeft op 29 juni 2026 het marktconsultatiedocument op TenderNed gepubliceerd om zoveel mogelijk marktpartijen te bereiken en te interesseren om aan de aanbesteding deel te nemen. Het doel van de marktconsultatie is om informatie op te halen uit de markt om:

1. te onderzoeken of en in hoeverre het beheer en onderhoud van de heterogene datacommunicatienetwerken (inclusief OT-ondersteuning) realistisch kan worden uitbesteed aan één of meerdere dienstverleners;
2. te toetsen welke contract- en organisatie modellen (o.a. Single Service Integrator versus percelen) haalbaar, wenselijk en marktconform zijn;
3. inzicht te krijgen in de benodigde OT-specifieke kennis, risico's, pricingmodellen, transitieaanpak en compliance-eisen (waaronder de Cyberbeveiligingswet en BIO2/CSIR), zodat de gemeente een weloverwogen besluit kan nemen over een eventuele aanbesteding en de inkoopstrategie.

1.3 Aanpak van de marktconsultatie

Deze marktconsultatie bestond uit twee rondes, namelijk een schriftelijke vragenronde en een aantal verdiepingsgesprekken. In totaal hebben 9 leveranciers schriftelijk gereageerd op de vragenlijst en zijn er 3 verdiepingsgesprekken gevoerd met 9 uitgenodigde en 6 aanwezige partijen.

1.4 Leveranciers

De volgende leveranciers hebben de vragenlijst ingevuld en tijdig ingediend:

1. Axians Communication Solutions B.V.
2. BAM Telecom B.V.
3. Eurofiber Nederland B.V.
4. Hanab Telecom Network Solutions B.V.
5. Hoeflake Infratechniek B.V.
6. ICT Netherlands B.V.>
7. SPIE
8. Strukton Rail Nederland B.V.
9. VisieCon B.V.

Alle partijen zijn vervolgens uitgenodigd voor de mondelinge ronde. De gemeente heeft met de volgende leveranciers gesproken:

¹ Hierna: 'de gemeente'

1. Axians Communication Solutions B.V.
2. BAM Telecom B.V.
3. Eurofiber Nederland B.V.
4. ICT Netherlands B.V.
5. Proximus NXT Nederland B.V.
6. SPIE

1.5 Verslag en conclusies

Dit verslag bevat een geanonimiseerde samenvatting van de antwoorden per ronde per vraag, aangevuld met relevante inzichten uit de gespreksverslagen en is als volgt opgebouwd:

- Per vraag een samenvatting van de ontvangen antwoorden, inclusief nuances, afwijkende adviezen en inzichten uit de verdiepingsgesprekken.
- Overkoepelende bevindingen die als leidraad kunnen dienen voor de aanbestedingsstrategie.

Dankwoord

De gemeente wil allereerst alle deelnemende leveranciers hartelijk danken voor hun ingediende vragenlijsten, de constructieve gesprekken die eventueel hebben plaatsgevonden en de algehele inspanningen die zij in dit proces hebben geleverd.

2 Vragen schriftelijke ronde

2.1 Vraag 1: Hoe beoordeelt u de haalbaarheid van het onderbrengen van het beheer en onderhoud van de heterogene netwerken bij één dienstverlener, en welke alternatieve ordeningen acht u realistisch?

De markt acht het technisch en organisatorisch haalbaar om het beheer en onderhoud van de heterogene netwerken onder te brengen bij één regievoerende dienstverlener, bijvoorbeeld in een Single Service Integrator-model. Het merendeel van de respondenten ziet voordelen in één centraal aanspreekpunt, integrale incidentcoördinatie, uniforme beheerprocessen, gezamenlijke monitoring en eenduidige rapportage. Een dergelijk model kan de operationele regielast voor de gemeente verminderen en de samenhang binnen de keten verbeteren.

Daarbij wordt breed benadrukt dat het succes niet primair wordt bepaald door de keuze voor een SSI-model of een perceelmodel, maar door de wijze waarop governance, mandaat, verantwoordelijkheden, informatie-uitwisseling, escalatie en samenwerking worden ingericht. Een integrator moet voldoende bevoegdheden en toegang tot gegevens krijgen om onderliggende leveranciers daadwerkelijk te kunnen regisseren. Ook moet duidelijk zijn wat de integrator zelf levert, wat deze namens de gemeente regisseert en welke prestaties afhankelijk blijven van derden.

Een deel van de markt plaatst kanttekeningen bij een te brede integrale opdracht. Het samenvoegen van veel verschillende technische disciplines kan het aantal potentiële inschrijvers beperken, de afhankelijkheid van één leverancier vergroten en specialistische kennis onvoldoende tot haar recht laten komen. Als alternatief wordt een perceelmodel of hybride model genoemd, bijvoorbeeld met afzonderlijke onderdelen voor fysieke infrastructuur, telecom en mobiele verbindingen, actieve netwerkcomponenten, OT-componenten of cybersecurity. Voorwaarde is dat de ketenregie expliciet bij één partij of bij de gemeente wordt belegd.

Telecomverbindingen, mobiele diensten, glasvezeltracés, civiele werkzaamheden, fabrikantensupport, licentiegebonden dienstverlening en specialistische OT-componenten blijven in de praktijk vaak bij gespecialiseerde leveranciers. Een integrator kan hiervoor wel optreden als centraal aanspreekpunt en verantwoordelijk worden gemaakt voor coördinatie, monitoring, rapportage en escalatie.

De markt adviseert om de scope gedurende de looptijd modulair aanpasbaar te maken. Toevoeging of verwijdering van locaties, subnetwerken, verbindingen en assets kan worden ondersteund met een dienstencatalogus, een scopebaseline, vaste eenheidsprijzen, afgesproken volumebandbreedtes en een transparante wijzigingsprocedure. Grote wijzigingen vragen om een afzonderlijke impactanalyse; kleinere wijzigingen kunnen periodiek, bijvoorbeeld jaarlijks, worden verrekend.

2.2 Vraag 2: Welke beheer- en operationele diensten kan de gemeente uitbesteden voor een datanetwerk inclusief de genoemde centrale voorzieningen?

Volgens de markt kan een groot deel van de operationele dienstverlening worden uitbesteed. Als basisdienstverlening worden veelvuldig genoemd:

- technisch netwerkbeheer;
- monitoring en eventmanagement;
- incident- en problemmanagement;
- configuratie- en wijzigingsbeheer;
- patch- en kwetsbaarhedenbeheer;
- asset- en documentatiebeheer;
- lifecyclemanagement;
- leveranciers- en ketenregie;
- beveiligde beheer-toegang;
- rapportage en SLA-sturing.

Deze onderdelen vormen volgens de respondenten gezamenlijk de minimale basis voor een veilige, beschikbare en beheersbare OT-netwerkomgeving.

Als aanvullende of optionele dienstverlening worden onder meer genoemd: uitgebreide SOC-dienstverlening, geavanceerde dreigingsdetectie, DDoS-bescherming, architectuuradvies, security-assessments, penetratietesten, capaciteitsanalyses, voorspellend onderhoud, geavanceerde automatisering, complianceondersteuning en innovatieadvies. De precieze indeling tussen basis en optioneel hangt volgens de markt af van de kritikaliteit van de objecten, de risicobereidheid van de gemeente en het gewenste serviceniveau.

Er bestaat brede overeenstemming dat monitoring, incidentmanagement, wijzigingsbeheer, configuratiebeheer, patchmanagement en assetregistratie sterk samenhangen. Monitoring zonder adequate opvolging heeft weinig waarde en lifecyclemanagement kan niet goed functioneren zonder actuele assetgegevens. Ook cybersecurity kan niet los worden georganiseerd van netwerkbeheer, omdat wijzigingen in firewalls, toegangsrechten en segmentatie direct gevolgen kunnen hebben voor de beschikbaarheid van OT-installaties.

De gemeente blijft naar verwachting verantwoordelijk voor beleid, architectuurkaders, risicobereidheid, risicoacceptatie, budgetten, investeringsbesluiten en strategische regie. Functioneel beheer van de aangesloten OT-installaties kan eveneens bij de gemeente of bij gespecialiseerde OT-beheerders blijven. De netwerkbeheerder moet echter voldoende kennis hebben van de aangesloten installaties om de gevolgen van incidenten en wijzigingen voor de gehele keten te kunnen beoordelen.

2.3 Vraag 3: Welke prijsmodellen zijn gebruikelijk voor dit type dienstverlening, en wat zijn de voor- en nadelen?

De markt beschouwt een hybride prijsmodel als de meest passende oplossing. Dit bestaat doorgaans uit:

1. een eenmalige vergoeding voor transitie en inrichting;
2. een vaste periodieke vergoeding voor de basisdienstverlening;
3. variabele eenheidsprijzen voor groei en krimp;
4. afzonderlijke tarieven voor projecten, migraties en omvangrijke wijzigingen;
5. eventueel afzonderlijke lifecycle- of vervangingscomponenten.

Dit model combineert budgetvoorspelbaarheid met flexibiliteit voor veranderingen gedurende de contractperiode.

Mogelijke prijsparameters zijn het aantal locaties, verbindingen, assets, devices of subnetwerken, de kritikaliteit van objecten, het servicevenster, de beschikbaarheidseisen, de gewenste respons- en hersteltijden, de omvang van security operations en de complexiteit van governance en rapportage. De markt waarschuwt dat een prijs per asset alleen onvoldoende rekening kan houden met verschillen in complexiteit en beheerlast.

Als belangrijkste kostenbepalers worden genoemd:

- 24/7 dienstverlening en consignatie;
- hoge beschikbaarheids- en hersteltijdeisen;
- specialistische OT- en securitykennis;
- SOC- en securitydienstverlening;
- heterogeniteit van technologie en leveranciers;
- kwaliteit van bestaande documentatie en assetdata;
- lifecyclemanagement en vervanging;
- afhankelijkheden van telecom- en ketenpartners.

Standaardisatie van architectuur, componenten, configuraties en beheerprocessen wordt door verschillende partijen gezien als de belangrijkste structurele mogelijkheid om de beheerkosten en totale levensduurkosten te verlagen.

Regelmatig onderschatte kosten zijn transitie en kennisoverdracht, herstel en validatie van documentatie, opbouw en beheer van een CMDB, licenties, security en compliance, OTAP en testen, spare parts, lifecyclevervanging en de coördinatie van meerdere leveranciers. De markt wijst daarnaast op het risico dat een lage initiële beheerprijs leidt tot hogere kosten door achterstallig onderhoud, storingen of ongeplande vervangingen.

Een deel van de markt noemt ook Network as a Service of andere OPEX-modellen als alternatief. Daarbij worden hardware, software, support, beheer en lifecycle in een periodieke vergoeding opgenomen. Dit kan vervangingsinvesteringen beter voorspelbaar maken, maar vraagt om duidelijke afspraken over eigendom, restwaarde, overdraagbaarheid en exit om leveranciersafhankelijkheid te voorkomen.

Prestatie-indicatoren moeten vooral betrekking hebben op beïnvloedbare prestaties, zoals responstijden, incidentafhandeling, beschikbaarheid van beheerde componenten, patchcompliance, kwaliteit van wijzigingen, actualiteit van de CMDB en tijdigheid van rapportages. Ketenprestaties en afhankelijkheden van derden kunnen afzonderlijk worden gevolgd, waarbij de opdrachtnemer aanspreekbaar is op regie, escalatie en communicatie.

2.4 Vraag 4: Welke specifieke kennis, competenties en processen zijn noodzakelijk voor het beheer van een communicatienetwerk waarop OT-installaties zijn aangesloten?

De markt benadrukt unaniem dat het beheer van een OT-netwerk wezenlijk verschilt van regulier IT-netwerkbeheer. In een OT-omgeving staan beschikbaarheid, fysieke veiligheid, continuïteit en voorspelbaarheid centraal. OT-assets hebben vaak een lange levensduur, kennen beperkte onderhoudsvensters en maken gebruik van verouderde of leveranciersspecifieke protocollen en technologieën. Wijzigingen die vanuit IT-perspectief logisch zijn, kunnen daardoor de werking van operationele installaties verstoren.

Noodzakelijke kennis en competenties zijn onder meer:

- industriële netwerkarchitecturen en netwerksegmentatie;
- OT-protocollen en legacy-technologie;
- cybersecurity en OT-security;
- routing, switching, firewalls en remote access;
- incident-, wijzigings-, configuratie- en lifecyclemanagement;
- fysieke omstandigheden en veilig werken in de openbare ruimte;
- domeinkennis van VRI's, bruggen, openbare verlichting en andere aangesloten objecten;
- ketenregie en samenwerking in multi-vendor omgevingen.

Naast technische kennis worden risicobewustzijn, communicatieve vaardigheden, analytisch vermogen en het kunnen uitvoeren van operationele impactanalyses als essentieel beschouwd.

Het meest kritische risico is dat een netwerk-, security- of configuratiewijziging leidt tot uitval of onjuiste werking van een kritieke installatie. Dit kan gevolgen hebben voor verkeersveiligheid, bereikbaarheid en de continuïteit van gemeentelijke dienstverlening. Wijzigingen moeten daarom vooraf worden getoetst op operationele impact, worden uitgevoerd binnen geschikte onderhoudsvensters en beschikken over test-, acceptatie- en terugvalscenario's.

De samenwerking tussen OT-beheer, netwerkbeheer en cybersecurity kan het beste worden vastgelegd in één operating model, met een RACI- of RASCI-matrix, gezamenlijke wijzigingsprocedures en eenduidige escalatieafspraken. OT-beheer blijft daarbij verantwoordelijk voor het functionele proces, terwijl

netwerkbeheer de veilige en betrouwbare connectiviteit borgt. De ketenregisseur bewaakt de onderlinge samenhang.

2.5 Vraag 5: Welke contractmodellen zijn geschikt voor het uitbesteden van netwerkbeheer in een OT-context?

Een managed service- of prestatiegericht beheercontract met een combinatie van resultaat- en inspanningsverplichtingen wordt door de markt het meest passend gevonden. Resultaatverplichtingen zijn geschikt voor prestaties waarop de opdrachtnemer rechtstreeks invloed heeft, zoals monitoring, responstijden, incidentregistratie, configuratiebeheer, wijzigingsbeheer, rapportage en beschikbaarheid van de door hem beheerde componenten.

Inspannings- of regieverplichtingen zijn passender voor prestaties die mede afhankelijk zijn van telecomproviders, netbeheerders, OT-leveranciers, verouderde assets, stroomvoorzieningen, civiele werkzaamheden of besluitvorming door de gemeente. De opdrachtnemer kan hierbij verantwoordelijk zijn voor analyse, coördinatie, escalatie, communicatie en voortgangsbewaking, maar niet zonder meer voor de uiteindelijke hersteltijd van een derde.

Contractueel moet onderscheid worden gemaakt tussen component-SLA's, onderliggende operationele afspraken en end-to-end ketenprestaties. Daarbij zijn heldere demarcaties, keten-SLA's, operationele afspraken, escalatieprocedures, medewerkingsverplichtingen en rapportageverplichtingen nodig.

Combinatievorming en onderaanneming worden als mogelijk beschouwd wanneer de volledige scope niet binnen één organisatie kan worden afgedekt. De markt adviseert in dat geval één partij aanspreekbaar te maken op de regie en integrale coördinatie. Een aantal respondenten adviseert om bij combinaties aantoonbare ervaring met eerdere samenwerking te verlangen, zodat het risico van een uitsluitend voor de aanbesteding gevormde gelegenheidscombinatie wordt beperkt.

2.6 Vraag 6: Welke certificeringen en aantoonbare kwalificaties acht u passend voor: de organisatie van de opdrachtnemer en het door de opdrachtnemer in te zetten personeel?

ISO 9001 en ISO 27001 worden door vrijwel alle respondenten als passende basisvoorwaarden genoemd. Afhankelijk van de opdracht worden daarnaast ISO 20000, VCA, ISO 14001, de CO₂-Prestatieladder en de Safety Culture Ladder of Veiligheidsladder genoemd. ISAE 3402 Type II en vergelijkbare assuranceverklaringen worden door sommige partijen als onderscheidend gezien, omdat deze niet alleen de inrichting maar ook de werking van beheersmaatregelen aantonen.

Voor personeel worden kwalificaties genoemd op het gebied van ITIL, SIAM, netwerkbeheer, cybersecurity, projectmanagement en leveranciersspecifieke technologie. Voorbeelden zijn Cisco-, Fortinet-, Microsoft- en Juniper-certificeringen, aangevuld met OT-securitykennis zoals IEC 62443, GICSP, CISSP of CISM. Niet iedere medewerker hoeft over alle kwalificaties te beschikken, maar de benodigde competenties moeten aantoonbaar binnen het team aanwezig zijn.

De brede marktvisie is dat certificeringen noodzakelijk zijn, maar geen afdoende garantie vormen. Aantoonbare praktijkervaring met vergelijkbare OT-omgevingen, kritische infrastructuur, gemeentelijke objecten en multi-vendor ketens wordt minstens zo belangrijk gevonden. Kwaliteitsborging vraagt daarnaast om audits, SLA- en securityrapportages, evaluatie van incidenten en wijzigingen, periodieke toetsing, opleidingsplannen en structurele kennisborging.

2.7 Vraag 7: Hoe kan geborgd worden dat netwerkdocumentatie en assetregistratie gedurende de contractperiode actueel, volledig en overdraagbaar blijven?

Alle marktpartijen benadrukken het belang van één centrale, betrouwbare bron voor netwerkdocumentatie, configuraties, assets en onderlinge relaties. Hiervoor wordt meestal een CMDB of geïntegreerd assetmanagementsysteem genoemd, eventueel gekoppeld aan ITSM, monitoring, GIS, configuratiebeheer, netwerkdiscovery en documentmanagement.

De registratie moet volgens de respondenten verder gaan dan een lijst met netwerkcomponenten. Per asset zijn onder meer locatie, functie, technische configuratie, software- en firmwareversie, leverancier, lifecyclestatus, securitystatus en afhankelijkheden met andere netwerk- en OT-componenten relevant. Bij fysieke infrastructuur kan GIS of vergelijkbare tracé-informatie nodig zijn. Passieve discovery wordt genoemd als een bruikbare methode om OT-assets en afhankelijkheden te detecteren zonder de operationele processen te verstoren.

Iedere wijziging moet pas als afgerond worden beschouwd nadat de technische uitvoering én de administratieve verwerking in CMDB, configuratiedocumentatie en netwerkdiagrammen zijn voltooid. De opdrachtnemer kan verantwoordelijk worden gemaakt voor uitvoering en actualisatie; de gemeente blijft eigenaar van de data en stelt de kaders en goedkeuringscriteria vast.

Voor firewalls en andere securitycomponenten adviseert de markt aanvullend versiebeheer, configuratieback-ups, logging, rolgebaseerde autorisatie, het vierogenprincipe, impactanalyses,

periodieke audits en rollbackprocedures. Hierbij moet niet alleen naar cybersecurity worden gekeken, maar ook naar het risico dat een beveiligingswijziging de OT-dienstverlening verstoort.

Alle beheerinformatie moet in open, gangbare en herbruikbare formaten overdraagbaar zijn. Dit betreft niet alleen asset- en configuratiegegevens, maar ook incidenthistorie, wijzigingen, risicoregisters, rapportages en relevante procesinformatie. Periodieke exports en overdraagbaarheidstoetsen kunnen voorkomen dat dit onderwerp pas aan het einde van de contractperiode aan bod komt.

2.8 Vraag 8: Hoe kunnen adviesdiensten effectief worden geïntegreerd in een beheercontract?

De markt beschouwt advies over architectuur, lifecycle, cybersecurity, capaciteit en standaardisatie in belangrijke mate als een logisch onderdeel van professioneel beheer. Operationele beheerinformatie, incidenttrends, kwetsbaarheden en lifecycledata moeten volgens de respondenten worden vertaald naar concrete verbeteradviezen en meerjarige roadmaps.

De opdrachtnemer signaleert, analyseert, adviseert en onderbouwt. De gemeente blijft verantwoordelijk voor beleid, architectuurprincipes, prioriteiten, investeringsbesluiten en risicoacceptatie. Deze rolverdeling kan worden vastgelegd in een RACI- of RASCI-model.

Regulier gevraagd en ongevraagd advies op basis van de beheeractiviteiten kan in de basisvergoeding worden opgenomen. Uitgebreide architectuuronderzoeken, businesscases, migratiestrategieën en transformatieprojecten kunnen afzonderlijk worden bekostigd via een offerte, werkpakket, strippenkaart of vooraf overeengekomen adviesbudget.

De opvolging kan worden geborgd met operationele, tactische en strategische overleggen, een gezamenlijk verbeterregister, een lifecycle-roadmap, een risicodossier en expliciete vastlegging van eigenaar, prioriteit, besluit en planning. De markt adviseert niet alleen te rapporteren over afgegeven adviezen, maar ook over gerealiseerde verbeteringen en risicoreductie.

2.9 Vraag 9: Welke aanpak adviseert u voor de transitie van de huidige situatie naar de beoogde contractvorm?

De markt adviseert unaniem een gefaseerde en risicogestuurde transitie. Een big-bangoverdracht wordt voor deze OT-omgeving als onwenselijk beschouwd. De transitie begint met een nulmeting of due diligence naar assets, configuraties, documentatie, architectuur, contracten, toegangsrechten, beheerprocessen, leveranciersafhankelijkheden, openstaande wijzigingen en aanwezige kennis.

De belangrijkste transitierisico's zijn:

- onvolledige of verouderde documentatie;
- ontbrekende configuraties en toegangsgegevens;
- onbekende afhankelijkheden;

- verlies van impliciete praktijkkennis;
- onvoldoende medewerking van latende leveranciers;
- beperkte beschikbaarheid van sleutelpersonen;
- lopende projecten en gelijktijdige wijzigingen;
- onduidelijke verantwoordelijkheden;
- verschillen tussen ontwerpen en de feitelijke situatie.

Deze risico's zijn volgens de markt het grootst tijdens inventarisatie, kennisoverdracht en de feitelijke overdracht van verantwoordelijkheden.

Een werkbaar aanpak bestaat uit inventarisatie, validatie, kennisoverdracht, inrichting en beproeving van beheerprocessen, schaduwbeheer, gefaseerde overname per domein of objectgroep, formele acceptatie en een stabilisatie- of hypercareperiode. Go/no-go-momenten, acceptatiecriteria, rollbackscenario's en decharge van latende partijen moeten vooraf worden vastgelegd.

De genoemde indicatieve doorlooptijden lopen uiteen van circa drie maanden voor een relatief beperkte operationele overdracht tot ongeveer twaalf maanden bij een brede transitie met veel objecten, infrastructuurwijzigingen of ontbrekende informatie. De meest genoemde bandbreedte ligt grofweg tussen vier en negen maanden. De kwaliteit van de bestaande gegevens en de medewerking van betrokken partijen zijn bepalender dan uitsluitend het aantal assets.

De gemeente behoudt de regie op kaders, prioriteiten, risicoacceptatie, besluitvorming en formele acceptatie. De opdrachtnemer is verantwoordelijk voor het transitieplan, de uitvoering, validatie, kennisborging, procesinrichting, rapportage en coördinatie met leveranciers.

2.10 Vraag 10: Hoe kan in een contract geborgd worden dat wordt voldaan aan de cyberbeveiligingswet en BIO2?

Volgens de markt kan naleving niet worden geborgd met uitsluitend een algemene contractbepaling dat aan wet- en regelgeving moet worden voldaan. Nodig is een samenhangend stelsel van governance, risicomanagement, technische maatregelen, organisatorische processen, aantoonbaarheid en periodieke evaluatie. De gemeente blijft verantwoordelijk voor beleid, risicobereidheid, classificatie, bestuurlijke besluitvorming en risicoacceptatie. De opdrachtnemer voert de overeengekomen maatregelen uit en rapporteert daarover.

Veelgenoemde technische en organisatorische maatregelen zijn:

- netwerksegmentatie;
- identity- en accessmanagement;
- beveiligde beheer-toegang;
- monitoring en logging;
- patch- en kwetsbaarhedenbeheer;
- configuratie- en wijzigingsbeheer;

- back-up- en herstelvoorzieningen;
- incidentrespons en meldprocedures;
- businesscontinuity- en crisismanagement;
- leveranciers- en ketenrisicomanagement;
- lifecyclemanagement.

Voor de OT-specifieke invulling worden naast BIO2 ook IEC 62443, de Cyber Security Implementatie Richtlijn en risicogebaseerde raamwerken genoemd.

Aantoonbaarheid vraagt om structurele vastlegging van assets, configuraties, wijzigingen, kwetsbaarheden, incidenten, risicoafwegingen en uitgevoerde maatregelen. De markt noemt periodieke rapportages, auditrechten, interne en externe audits, securityreviews, compliancekalenders, risicoregisters en meetbare security-KPI's. Daarbij moet per maatregel zichtbaar zijn welke partij verantwoordelijk is en welke restrisico's resteren.

Een exitstrategie moet vanaf de start van de overeenkomst worden ingericht en periodiek worden bijgewerkt. Deze omvat overdracht van documentatie, configuraties, CMDB-gegevens, assetregistraties, accounts, autorisaties, certificaten, back-ups, risicodossiers, incidenthistorie, auditinformatie, leveranciersafspraken en relevante contracten. Ook ondersteuning en kennisoverdracht tijdens een retransitie moeten contractueel zijn vastgelegd.

2.11 Vraag 11: Indien u de dienstverlening zou moeten inrichten bij een beperkt budget: welke onderdelen zou u prioriteren en welke zou u versoberen; welke risico's accepteert de opdrachtgever daarmee; welke keuze zou u als eerste terugdraaien bij extra budget?

Bij een beperkt budget adviseert de markt om prioriteit te geven aan onderdelen die direct bijdragen aan veiligheid, beschikbaarheid en beheersbaarheid. Dit betreft in ieder geval monitoring, incidentmanagement, configuratie- en wijzigingsbeheer, cybersecurity, assetregistratie, actuele documentatie en beheer van de centrale netwerk- en securityvoorzieningen. Over het precieze niveau van 24/7 dienstverlening lopen de opvattingen uiteen, maar voor kritieke onderdelen wordt dit veelal als noodzakelijk gezien.

Versobering wordt vooral mogelijk geacht op:

- frequentie en diepgang van rapportages;
- niet-noodzakelijke governance-overleggen;
- uitgebreide dashboarding;
- innovatieprogramma's;
- omvangrijke adviestrajecten;
- niet-kritieke optimalisaties;
- frequentie van aanvullende health checks en analyses.

Daarmee accepteert de gemeente risico's zoals minder inzicht in trends, tragere doorontwikkeling, meer technische schuld, een grotere kans op onverwachte vervangingen en minder voorspelbaarheid van de toekomstige kosten.

Over lifecyclemanagement bestaat een nuanceverschil. Een deel van de markt ziet uitstel van niet-kritieke lifecyclemaatregelen als een mogelijke tijdelijke besparing. Andere respondenten vinden lifecyclemanagement onderdeel van de minimale basis, omdat versobering hiervan leidt tot technische schuld en hogere toekomstige kosten. Breed wordt wel onderschreven dat extra budget bij voorkeur wordt ingezet voor lifecyclemanagement, betere assetinformatie, standaardisatie, preventieve security, trendanalyse en datagedreven beheer.

Enkele partijen adviseren om niet uitsluitend in termen van versobering te denken, maar ook te onderzoeken of een andere financieringsvorm, standaardisatie, automatisering of een geïntegreerd OPEX-model de kosten beter voorspelbaar kan maken.

2.12 Vraag 12: Heeft u naar aanleiding van deze marktconsultatie aanvullende opmerkingen c.q. aandachtspunten?

De markt beschouwt de opgave nadrukkelijk niet alleen als een technisch netwerkbeheercontract. Het betreft vooral een keten-, governance- en veranderopgave waarin netwerkbeheer, OT-beheer, cybersecurity, leveranciersmanagement, assetinformatie en gemeentelijke besluitvorming samenkomen.

Veelgenoemde aandachtspunten zijn:

- duidelijke scope en demarcatie;
- expliciete ketenregie;
- actuele en betrouwbare assetdata;
- aantoonbare OT-praktijkervaring;
- standaardisatie en harmonisatie;
- cybersecurity en compliance;
- gefaseerde transitie;
- modulaire scope en prijsmechanismen;
- overdraagbaarheid en exit;
- ruimte voor innovatie en continue verbetering.

Ook wordt geadviseerd om kwaliteit, veiligheid, continuïteit en beheersbaarheid zwaarder te laten wegen dan de laagste initiële prijs.

Een aantal partijen adviseert om vóór of tijdens de aanbesteding ruimte te bieden voor nadere dialoog, validatie, een Proof of Concept of een gefaseerde uitwerking. Dit kan helpen om de gewenste eindsituatie, de technische afhankelijkheden en de samenwerkingsvorm voldoende concreet te maken en interpretatieverschillen of meerwerk tijdens de uitvoering te beperken.

3 Conclusie en rode draden analyse

3.1 Rode draden

Op basis van de schriftelijke vragenlijsten zijn de volgende rode draden zichtbaar:

- De opgave is vooral een ketenvraagstuk
- Breed draagvlak voor centrale ketenregie, maar geen volledige consensus over de contractstructuur
- De gemeente moet een sterke regieorganisatie behouden
- OT-ervaring is belangrijker dan netwerkkennis alleen
- Assetdata en documentatie zijn een kritieke randvoorwaarde
- Een gefaseerde transitie is noodzakelijk
- De contract- en prijsstructuur moet hybride en modulair zijn
- Cybersecurity en compliance zijn doorlopende beheerprocessen
- Lifecyclemanagement en standaardisatie bepalen de kosten op lange termijn
- Exit en overdraagbaarheid moeten vanaf de start worden ontworpen

3.2 Conclusie schriftelijke ronde

Uit de negen marktconsultatiereacties blijkt dat de voorgenomen uitbesteding haalbaar is, maar dat de gemeente de opdracht niet uitsluitend als een technisch netwerkbeheercontract moet benaderen. De kern van de opgave is het organiseren van een beheersbare OT-keten waarin netwerkbeheer, OT-beheer, cybersecurity, telecomdiensten, fysieke infrastructuur en gemeentelijke regie aantoonbaar op elkaar aansluiten.

Er is voldoende draagvlak voor een model met centrale service-integratie en één operationeel aanspreekpunt. Tegelijkertijd bestaat geen volledige marktconsensus over de vraag of alle dienstverlening in één integraal contract moet worden ondergebracht. Een brede SSI kan de operationele aansturing vereenvoudigen, maar kan ook de concurrentie beperken, afhankelijkheid vergroten en specialistische disciplines te veel bundelen. Een perceel- of hybride model kan meer marktwerking en specialistische diepgang bieden, maar stelt hogere eisen aan de regieorganisatie.

Op basis van de marktconsultatie lijkt daarom een hybride regiemodel het meest evenwichtig. Daarbij wordt één partij of functie expliciet verantwoordelijk gemaakt voor service-integratie, incidentcoördinatie, ketenrapportage en escalatie, terwijl specialistische diensten waar nodig afzonderlijk of via onderaannemers kunnen worden geleverd. De gemeente behoudt daarbij de strategische regie, het eigendom van data en documentatie en de verantwoordelijkheid voor architectuur, risicoacceptatie en investeringsbesluiten.

Voor een succesvolle aanbesteding zijn in ieder geval de volgende randvoorwaarden van belang:

1. Formuleer de uitvraag ketengericht en functioneel, met prestaties rond continuïteit, veiligheid, beheersbaarheid en samenwerking.

2. Leg de scope en demarcatie expliciet vast, inclusief de positie van telecomproviders, OT-leveranciers, civiele partijen en interne gemeentelijke teams.
3. Organiseer één herkenbaar punt voor ketenregie, ongeacht de uiteindelijke perceel- of contractstructuur.
4. Voer vooraf of bij aanvang een gevalideerde nulmeting uit van assets, configuraties, documentatie, contracten en afhankelijkheden.
5. Reserveer een realistische gefaseerde transitieperiode, gekoppeld aan acceptatiecriteria in plaats van uitsluitend een vaste einddatum.
6. Gebruik een hybride prijsmodel, met een vaste basisvergoeding en transparante eenheidstarieven voor groei, krimp en wijzigingen.
7. Maak onderscheid tussen beïnvloedbare prestaties en ketenafhankelijkheden bij SLA's, KPI's en aansprakelijkheid.
8. Beoordeel inschrijvers nadrukkelijk op OT-praktijkervaring, ketenregie en kennisborging, niet uitsluitend op certificeringen en prijs.
9. Borg cybersecurity, lifecyclemanagement en assetregistratie als structurele basisprocessen en niet als vrijblijvende opties.
10. Ontwerp de exitstrategie vanaf contractstart, met gemeentelijk eigendom en overdraagbaarheid van alle essentiële beheerinformatie.

De marktconsultatie geeft daarmee voldoende basis om de aanbesteding verder uit te werken. Wel is eerst een heldere keuze nodig over de gewenste ketenverantwoordelijkheid, het gemeentelijke regieniveau en de afbakening tussen integrale dienstverlening en specialistische onderdelen. De aanbestedingsvorm is uiteindelijk een middel. De bepalende succesfactor is een operating model waarin verantwoordelijkheden, informatie, mandaat en samenwerking gedurende de volledige contractperiode aantoonbaar zijn geborgd.

4. Vragen mondelinge ronde

4.1 Transitieperiode

Vraag 1: Welke informatie moet de gemeente in de aanbestedingsstukken meegeven, zodat het risico op een mislukte transitie voor u sterk afneemt en u kunt aanbieden op een overdracht van enkele maanden?

De markt beschouwt actuele configuraties, inzicht in de netwerkarchitectuur, afhankelijkheden en toegang tot de beheeromgeving als de belangrijkste voorwaarden voor een beheerste transitie. Daarnaast zijn een actueel assetregister, netwerk- en topologietekeningen, software- en firmwareversies, lifecycle- en supportstatus, accounts en rechten, storingshistorie, serviceafspraken en gegevens over ketenpartners van belang.

Volledige en betrouwbare informatie verkort de inventarisatie en beperkt risico-opslagen. Ontbrekende gegevens hoeven de transitie niet altijd te blokkeren, maar leiden doorgaans tot aanvullende validaties, schouwen, hogere kosten en meer onzekerheid. De markt adviseert daarom een nulmeting, due diligence of gap-analyse uit te voeren en vooraf vast te leggen hoe met ontbrekende informatie en meerwerk wordt omgegaan. Gevoelige technische informatie kan onder geheimhouding beschikbaar worden gesteld.

Vraag 2: Welke rol geeft u aan schaduwbeheer van de latende partij? Weegt u dat af tegen een werkwijze waarin de gemeente vooraf benoemde transitierisico's zelf aanvaardt, zodat een go- of no-go-besluit per fase op minder gegevens kan worden genomen?

Schaduwbeheer wordt gezien als een middel voor kennisoverdracht, verificatie en risicobeheersing. De gewenste duur varieert van een beperkte periode van circa twee weken tot een uitgebreidere periode van vier tot zes weken. Bij voldoende betrouwbare informatie kan schaduwbeheer worden beperkt en kan de opdrachtnemer ontbrekende gegevens tijdens de transitie verifiëren.

Een kortere of ontbrekende schaduwperiode vergroot het risico op onbekende afhankelijkheden, langere oplostijden bij de eerste incidenten, aanvullende inventarisaties en afhankelijkheid van kennisdragers bij de vertrekkende beheerder. De markt adviseert daarom een gefaseerde overdracht met go- of no-go-momenten per objectgroep, locatie of logisch cluster.

Vraag 3: Welke gegevens en documenten moeten in de transitiefase zelf nog worden opgeleverd, naast wat de gemeente in de aanbestedingsstukken meegeeft, om het dossier compleet te maken en het onderhoud te borgen?

Tijdens de transitie moet de beschikbare informatie worden omgezet in een gevalideerd en overdraagbaar beheerdossier. Dit dossier bevat in ieder geval:

- een gevalideerde assetregistratie en netwerktopologie;
- actuele configuraties en herstelbare back-ups;
- rollen, rechten, accounts en toegangsprocedures;
- incident-, wijzigings- en escalatieprocedures;
- afspraken en contactgegevens van ketenpartners;
- lifecycle-, onderhouds- en vervangingsinformatie;
- openstaande incidenten, risico's en afwijkingen;

- acceptatiecriteria en een formeel overdrachtsdocument;
- een actueel exitplan.

De gemeente moet eigenaar blijven van de primaire beheerinformatie. Daarmee wordt voorkomen dat bij een contractwisseling essentiële kennis, configuraties of gegevens verloren gaan.

4.2 24/7 ondersteuning

Vraag 1: Welke onderdelen van 24/7 ondersteuning heeft de gemeente nodig om aan de zorgplicht van de Cyberbeveiligingswet te voldoen, en welke gaan verder dan die zorgplicht vraagt?

De markt maakt onderscheid tussen bewaking, alarmering, triage en daadwerkelijke opvolging. Continue monitoring en automatische alarmering worden breed gezien als basisvoorzieningen. Triage is nodig om de impact, oorzaak en verantwoordelijke partij vast te stellen. Over de noodzaak van opvolging buiten kantoor tijd bestaan verschillende inzichten.

De algemene lijn is dat de Cyberbeveiligingswet om passende en evenredige maatregelen vraagt en niet automatisch om volledige 24/7 respons voor ieder object. De benodigde opvolging moet daarom worden bepaald op basis van een risicoanalyse en de maatschappelijke, operationele en veiligheidsimpact per objectcategorie. De grootste kostenfactor is niet de geautomatiseerde monitoring, maar de beschikbaarheid van specialisten die buiten kantoor uren bevoegd zijn om herstelmaatregelen uit te voeren.

Vraag 2: Welk deel van de diensten voert u lokaal uit, binnen het netwerk van de gemeente, en welke deel op afstand?

De markt verwacht dat het grootste deel van het beheer op afstand kan worden uitgevoerd. De genoemde indicaties liggen rond 70% tot 80% op afstand en 20% tot 30% lokaal. Monitoring, analyse, configuratiebeheer, rapportage en een groot deel van de wijzigingen kunnen op afstand plaatsvinden. Hardwarevervanging, kabelwerkzaamheden, locatie-inspecties en fysieke storingen vereisen lokale inzet.

Remote beheer moet plaatsvinden via een beveiligde en gecontroleerde toegangsarchitectuur, bijvoorbeeld met multifactor-authenticatie, een beveiligde verbinding, een jumpserver en gescheiden IT- en OT-zones. Essentiële beheer-, monitoring- en back-upvoorzieningen worden bij voorkeur binnen de gemeentelijke omgeving geplaatst en blijven eigendom van de gemeente. Leveranciersspecifieke monitoring of tooling kan bij contractbeëindiging wegvallen en moet daarom in het exitplan worden ondervangen.

4.3 Serviceniveaus en KPI's

Vraag 1: Welke normwaarden horen typisch bij een basisniveau op dit areaal?

De markt adviseert om serviceniveaus niet uniform voor het gehele areaal vast te stellen, maar te differentiëren naar kritikaliteit, risico, redundantie en maatschappelijke impact. De genoemde indicatieve

basisbeschikbaarheid ligt tussen 99,5% en 99,7%. Voor een verhoogd niveau wordt 99,9% tot 99,95% genoemd. Voor kritieke incidenten worden bij een basisniveau reactietijden van circa 30 tot 60 minuten en hersteltijden van 8 tot 12 uur genoemd. Bij een verhoogd niveau worden reactietijden van 15 tot 30 minuten en een hersteltijd van circa vier uur genoemd.

Deze waarden zijn slechts haalbaar wanneer de architectuur, redundantie, reserveonderdelen, toegang tot locaties en beschikbaarheid van specialisten daarop zijn ingericht. Een verhoogd serviceniveau kan volgens een marktpartij leiden tot circa 15% tot 30% hogere beheerkosten.

Vraag 2: Op welke prestaties wilt u worden afgerekend, en op welke niet?

De markt wil uitsluitend worden afgerekend op prestaties binnen de eigen beïnvloedingssfeer. Geschikte KPI's zijn:

- reactie- en hersteltijd per prioriteit;
- snelheid van functioneel herstel;
- beschikbaarheid per dienst of objectcategorie;
- tijdige alarmopvolging;
- preventief onderhoud;
- patch- en lifecyclemanagement;
- kwaliteit van wijzigingen;
- actualiteit van documentatie en assetdata;
- tijdige uitvoering van verbetermaatregelen;
- vermindering van herhalingsincidenten.

Functioneel herstel wordt belangrijker gevonden dan uitsluitend een beschikbaarheidspercentage. Bij complexe problemen kan onderscheid worden gemaakt tussen tijdelijk functieherstel en definitief technisch herstel. Verstoringen door telecomproviders, energievoorzieningen, gemeentelijke systemen of andere derden moeten afzonderlijk worden geregistreerd en mogen niet zonder meer aan de opdrachtnemer worden toegerekend.

Over bonus-malusregelingen verschillen de meningen. Service credits worden mogelijk geacht voor aantoonbare en beïnvloedbare tekortkomingen. Andere partijen geven de voorkeur aan reguliere contractsturing of een verlengingsoptie als prikkel voor goed presteren.

4.4 Vastleggen van assetdata

Vraag 1: Hoe legt u assetgegevens vast wanneer de registratie in een systeem van de gemeente plaatsvindt?

De markt onderschrijft dat de gemeente eigenaar en bronhouder van de assetdata moet blijven. Uitgangspunt is één centrale bron van waarheid. Leveranciers kunnen gegevens rechtstreeks in het gemeentelijke systeem verwerken of eigen beheer- en servicemanagementsystemen via een API of gecontroleerde gegevensuitwisseling koppelen.

Assetmutaties moeten onderdeel zijn van het wijzigingsproces. Relevante gegevens zijn onder meer asset-ID, locatie, type, serienummer, firmwareversie, IP-adres, netwerksegment, supportstatus, relaties

met andere assets en bijbehorende documentatie. De gegevensbehoefte verschilt tussen actieve netwerkcomponenten, passieve infrastructuur en connectiviteitsdiensten.

Vraag 2: Hoe stellen wij vast dat die gegevens actueel, betrouwbaar en volledig zijn?

De kwaliteit van assetdata kan worden gecontroleerd via een nulmeting, schouwen, steekproeven, vergelijking met monitoringdata en periodieke discrepantieanalyses. Genoemde indicatieve normen zijn:

- minimaal 90% van de wijzigingen binnen vijf werkdagen verwerkt;
- maximaal 5% afwijking tussen registratie en werkelijkheid;
- minimaal 95% van de verplichte velden gevuld;
- een halfjaarlijkse steekproef van circa 5% van de assets, of een jaarlijkse validatie afhankelijk van het aantal mutaties.

Volledig geautomatiseerd scannen kan in OT-omgevingen risico's veroorzaken. Daarom moet per objectcategorie worden beoordeeld of passieve monitoring, gecontroleerde detectie of een steekproef passend is. Bij contractbeëindiging moeten alle structurele assetgegevens, configuraties en relevante beheerinformatie beschikbaar blijven voor de gemeente.

5. Conclusie en rode draden analyse

5.1 Rode draden analyse

Uit de gesprekken komen de volgende rode draden naar voren:

- De kwaliteit van de uitgangsinformatie bepaalt de voorspelbaarheid van de opdracht.
- Een gefaseerde en risicogestuurde transitie heeft brede voorkeur.
- Het serviceniveau moet per objectcategorie worden vastgesteld.
- 24/7 monitoring is iets anders dan volledige 24/7 respons.
- Functioneel herstel en ketenregie zijn belangrijker dan uptime alleen.
- Gemeentelijk eigenaarschap beperkt leveranciersafhankelijkheid.
- De scope en demarcatie moeten expliciet worden gemaakt.

5.2 Conclusie mondelinge ronde

De markt acht een transitie binnen enkele maanden haalbaar, mits de gemeente vooraf voldoende inzicht biedt in de architectuur, configuraties, assets, toegangsvoorzieningen en ketenafhankelijkheden. Volledigheid van alle documentatie hoeft geen absolute voorwaarde te zijn, zolang ontbrekende informatie tijdens een gefaseerde transitie wordt gevalideerd en de bijbehorende risico's en kosten transparant worden verdeeld.

Voor de aanbesteding ligt een risicogestuurde inrichting voor de hand. Daarbij worden objecten geclassificeerd naar kritikaliteit, worden serviceniveaus en 24/7 ondersteuning per categorie vastgesteld en wordt gestuurd op functioneel herstel, incidentafhandeling, preventief onderhoud en datakwaliteit. Een nulmeting of due diligence, een beperkte schaduwperiode en duidelijke acceptatiemomenten kunnen de overdracht beheersbaar maken.

Tot slot is het van belang dat de gemeente eigenaar blijft van de essentiële asset- en beheerinformatie en dat monitoring, toegang, documentatie en exit vanaf de start overdraagbaar worden ingericht. Daarmee ontstaat een dienstverlening die niet alleen uitvoerbaar en betaalbaar is, maar ook bestuurbaar blijft bij wijzigingen in de leveranciersketen.

6. Conclusie totale marktconsultatie

Uit de schriftelijke reacties en de verdiepende gesprekken met de markt komt een consistent beeld naar voren. De voorgenomen uitbesteding wordt door de markt als haalbaar beschouwd, mits deze niet uitsluitend als een netwerkbeheercontract wordt benaderd. De centrale opgave ligt volgens de markt in het organiseren van een beheersbare OT-keten, waarin netwerkbeheer, OT-beheer, connectiviteit, cybersecurity, assetmanagement en gemeentelijke regie integraal samenwerken.

De markt spreekt zich vrijwel unaniem uit voor centrale ketenregie en één herkenbaar aanspreekpunt voor incidenten, escalaties en coördinatie. Tegelijkertijd bestaat geen volledige consensus over de wijze waarop dit contractueel moet worden ingericht. Sommige partijen zien voordelen in een integrale dienstverlening, terwijl anderen juist een hybride of perceelgerichte aanpak adviseren waarin specialistische disciplines afzonderlijk georganiseerd blijven. Wel bestaat brede overeenstemming dat de gemeente een sterke regierol moet behouden en eigenaar moet blijven van strategische besluitvorming, assetdata, documentatie en architectuurkeuzes.

Daarnaast blijkt dat OT-praktijkervaring door de markt als belangrijker wordt beschouwd dan algemene netwerkkennis. Leveranciers benadrukken dat de beheeropgave sterk afhankelijk is van kennis van OT-processen, afhankelijkheden tussen objecten en de impact van verstoringen op de openbare ruimte. Daarbij worden actuele assetdata, configuraties, documentatie en inzicht in ketenafhankelijkheden gezien als essentiële randvoorwaarden voor een succesvolle aanbesteding en beheertransitie.

Een tweede duidelijke rode draad is dat een gefaseerde en risicogestuurde transitie noodzakelijk wordt geacht. De markt geeft aan dat een overgang binnen enkele maanden haalbaar is, maar adviseert nadrukkelijk te werken met nulmetingen, validaties, acceptatiemomenten en een beperkte periode van kennisoverdracht of schaduwbeheer. Daarbij geldt dat ontbrekende informatie niet altijd een blokkade hoeft te vormen, mits risico's expliciet worden geaccepteerd en beheerst.

Op het gebied van dienstverlening ontstaat een breed beeld dat serviceniveaus, cybersecuritymaatregelen en 24/7 ondersteuning niet uniform moeten worden ingericht, maar afhankelijk moeten zijn van de kritikaliteit van de verschillende objectcategorieën. Monitoring, assetmanagement, lifecyclemanagement en cybersecurity worden daarbij niet gezien als afzonderlijke projecten, maar als structurele beheerprocessen gedurende de gehele contractduur. Ook wordt benadrukt dat hogere beschikbaarheidseisen direct leiden tot hogere kosten en dat differentiatie daarom wenselijk is.

Ten slotte bestaat brede overeenstemming dat overdraagbaarheid vanaf de start moet worden georganiseerd. Exit, eigenaarschap van data, documentatie, configuraties en beheerinformatie moeten vooraf worden ingericht om leveranciersafhankelijkheid te voorkomen en toekomstige contractwisselingen beheersbaar te houden.

Samenvattend geeft de marktconsultatie voldoende vertrouwen dat de aanbesteding succesvol kan worden uitgevoerd. De belangrijkste succesfactor ligt niet primair in de gekozen contractvorm, maar in een helder operating model waarin verantwoordelijkheden, regie, data-eigenaarschap, ketensamenwerking en overdraagbaarheid structureel zijn geborgd. Op basis van de marktconsultatie

lijkt een hybride model met centrale service-integratie, behoud van gemeentelijke regie en ruimte voor specialistische dienstverlening het beste aan te sluiten bij de behoeften en risico's van het gemeentelijke OT-landschap.