

## Samenvatting Marktconsultatie Digitale Werkplek

Algemeen en Strategie		Subvragen	Geanonimiseerde samenvatting
1	Hoe ziet volgens u de aanpak/planning eruit om van IST naar uw dienstverlening over te gaan. Beschrijf in maximaal 3x4 (aanpak, reikwijdte, integraties)		Alle leveranciers hanteren een gestructureerde transitieaanpak met fasen zoals voorbereiding, inventarisatie, kennisoverdracht en acceptatie, waarbij continuïteit en minimale impact voor eindgebruikers centraal staan. Er zijn verschillen in focus: sommige richten zich op technische overname ("as-is"), anderen combineren dit met transformatie en modernisering. De mate van governance en gebruikersgerichtheid varieert; enkele partijen leggen nadruk op adoptie en UX/XLA, terwijl anderen vooral technische integratie en procesborging benadrukken. Kernwaarden zoals risicobeheersing, flexibiliteit en toekomstgerichtheid (inclusief AI en cloudoplossingen) komen bij alle leveranciers terug.
2	Kunt u een referentieproject aangeven die aansluit bij de behoeftstelling van het Kadaster, voorzien van contactpersoon, e-mail en telefoonnummer?		Alle partijen hebben een referentie opgegeven.
3	Wat is volgens u de meest effectieve inkoopstrategie voor de hardware in deze opdracht, met inbegrip van keuzes zoals koop/lease, CYOD/BYOD, accessoires (zoals tasjes) en type apparatuur (tablets (Android/iOS), laptops, Mac Books, Surface Pro (of vergelijkbaar), mobiele telefoons (Android/ iOS), MFP's, plotters, scanners etc.)?		De meeste leveranciers adviseren Lease/DaaS voor voorspelbare kosten en eenvoudig beheer, al wordt opgemerkt dat lease duurder is dan koop. Koop wordt aanbevolen voor apparatuur met lange levensduur, zoals printers en AV-apparatuur; soms wordt een all-in maandprijs via een system integrator genoemd. CYOD (Choose Your Own Device) is breed aanbevolen, terwijl BYOD wordt afgeraden vanwege beheerrisico's. Het assortiment omvat laptops, tablets, MacBooks, smartphones en randapparatuur, afgestemd op gebruikersprofielen, met accessoires voor bescherming en mobiliteit. Leveranciers benadrukken standaardisatie, preferred suppliers, duurzaamheid en recycling als belangrijke aandachtspunten.
4	Hoe gaat u om met bestaande hardware van de opdrachtgever welke nog economische waarde heeft? Bent u bereid het beheer over te nemen, onder		ALLE partijen zijn bereid de hardware over te nemen ONDER VOORWAARDEN.
5	Acht u Due Dilligence bij een eventuele aanbesteding noodzakelijk, zo ja, hoe wilt u hiermee omgaan binnen de aanbesteding?		6 partijen achten een Due Dilligence noodzakelijk. De 2 partijen die het niet noodzakelijk achten kennen de actuele situatie.
6	Kunt u beschrijven hoe het beheer van een dergelijke omgeving wordt ingevuld. Bijvoorbeeld versiebeheer (updaten en upgraden)?		Alle partijen focussen voornamelijk op windows updates. Er zijn 2 partijen die LOB applicaties benoemt. Er is 1 partij die aangeeft het N-1 principe te hanteren. 5 partijen geven weer gebruik te maken van geautomatiseerde processen. Er is 1 partij die een dedicated klantenteam hanteert en aangeeft dat upgrades van microsoft producten is inbegrepen in werkplek prijs. Hierbij de kantekening dat deze partij eerder heeft aangegeven dat OS versie updates projectmatig ( additionele kosten) aangevlogen moet worden. 2 partijen geven duidelijk aan dat OS upgrades projectmatig worden uitgevoerd.2 partijen benoemen LOB applicaties.
7	<p>Perceelindeling: Het Kadaster overweegt om de opdracht op te delen in percelen. Een mogelijke indeling die momenteel in overweging is:</p> <p>Perceel 1: Beheer en levering van IT-hardware zoals laptops, tablets, mobiele telefoons, printers/plotters en accessoires. Inclusief het beheer en de levering van het totale applicatielandschap, zoals installatie, configuratie, updates, upgrades en selfservice-applicatieportaal, zie hiervoor ook bijlage 1.</p> <p>Perceel 2: Beheer, levering en installatie van audiovisuele middelen, zoals interactieve schermen, microfoons en overige AV-apparatuur, zie hiervoor ook bijlage 1.</p>	a. Wat is uw visie op de voorgestelde perceelindeling	<p>6 van de 8 partijen ondersteunen de voorgestelde splitsing in Perceel 1 (IT-hardware &amp; werkplekdiensten) en Perceel 2 (AV-middelen) als logisch en marktconform.</p> <p>2 partijen adviseren om de percelen juist te bundelen in één integraal perceel:</p> <p>Zij wijzen op de verwevenheid tussen AV en IT in de moderne werkplek.</p> <p>5 partijen benadrukken het belang van een centrale regierol of hoofdaannemer om bij een gesplitste aanpak integraliteit en samenhang te waarborgen.</p> <p>3 partijen noemen het risico op versnippering van verantwoordelijkheden en adviseren heldere afspraken over samenwerking, escalatie en integratie.</p>



11	Wat is uw visie op gebied van VDI en AVD?		Leveranciers zien VDI en Azure Virtual Desktop (AVD) als veilige, schaalbare en toekomstbestendige oplossingen voor de digitale werkplek, vaak gecombineerd met Windows 365 voor eenvoud en voorspelbare kosten. AVD wordt gepositioneerd als kostenefficiënt alternatief voor traditionele VDI-platformen en sluit goed aan bij hybride werken, BYOD en scenario's met hoge beveiligingseisen. De meeste partijen hanteren een hybride benadering waarin VDI en AVD elkaar aanvullen, met aandacht voor gebruiksgemak, performance en integratie met Microsoft 365. Aanvullend worden best practices zoals autoscaling, FSLogix, governance en securitymaatregelen genoemd om beheerbaarheid en compliance te waarborgen.
<b>MVOI Milieuaspecten</b>			
12	Welke maatregelen neemt u t.a.v. duurzaamheid? (bijv. ISO 14001, EPEAT, Energy Star)?		IT-dienstverleners integreren duurzaamheid structureel in hun bedrijfsvoering en dienstverlening, ondersteund door certificeringen zoals ISO 14001, 50001 en 27001. Maatregelen omvatten CO <sub>2</sub> -reductie, circulariteit, energie-efficiëntie en het gebruik van duurzame hardware, gecombineerd met cloudstrategieën en slimme werkplekinrichting om de ecologische voetafdruk te verkleinen. Organisaties stellen reductiedoelen op, rapporteren over emissies en stimuleren elektrisch rijden en hybride werken, terwijl ketenverantwoordelijkheid en samenwerking met leveranciers centraal staan. Duurzaamheid is verankerd in strategie en cultuur, met inzet van innovaties, trainingen en maatschappelijke initiatieven.
13	Kunt u een duurzaamheidsrapport of -beleid aanleveren? Hoe vaak wordt dit geüpdatet en wat wordt daarin gerapporteerd?		IT-organisaties hanteren formele duurzaamheids- en ESG-beleidskaders, vaak ondersteund door ISO-certificeringen en de CO <sub>2</sub> -Prestatieladder. Jaarlijkse rapportages geven inzicht in voortgang, KPI's en best practices op het gebied van milieu, sociale verantwoordelijkheid en governance. Doelstellingen zoals Net Zero en CO <sub>2</sub> -reductie zijn vaak gevalideerd via SBTi of vergelijkbare initiatieven. Beleid omvat thema's als circulaire economie, energie-efficiëntie, vitaliteit, inclusie en maatschappelijke impact. Rapportages zijn afgestemd op CSRD-, GRI- of URD-standaarden. Medewerkers worden betrokken via trainingen, bewustwording en MVO-activiteiten. ESG-governance is vaak verankerd in het managementsysteem en toegewezen aan specifieke rollen. Klantcontext en wetgeving worden meegenomen in de uitvoering. Transparantie en naleving staan centraal in de aanpak. Duurzaamheid is geïntegreerd in strategie, operatie en dienstverlening.
14	Welke maatregelen neemt u om de CO <sub>2</sub> -uitstoot te beperken?		Partijen nemen gerichte maatregelen om CO <sub>2</sub> -uitstoot te reduceren binnen hun organisatie, dienstverlening en keten. Doelstellingen zoals net-zero in 2040 of 2050 zijn vaak gevalideerd via SBTi en afgestemd op Europese klimaatdoelen. Maatregelen omvatten elektrificatie van wagenparken, gebruik van hernieuwbare energie, energiezuinige datacenters en circulaire hardwareverwerking. Cloudoplossingen en hybride werken dragen bij aan lagere uitstoot. Inkoop is gebaseerd op duurzaamheidscriteria, met monitoring van scope 1, 2 en 3-emissies. Jaarlijkse rapportages volgen standaarden zoals CSRD, GRI en het Greenhouse Gas Protocol. Medewerkers worden betrokken via mobiliteitsbeleid, trainingen en bewustwordingsacties. Innovaties zoals dashboards, GreenOps en maturity scans ondersteunen klanten bij verduurzaming. Duurzaamheid is verankerd in beleid, processen en klantoplossingen. Samenwerking met leveranciers versterkt de impact in de keten.
15	Hoe gaat u om met (verouderde) hardware (recycling, refurbishing, terugname of hergebruik)?		Partijen zetten sterk in op circulaire hardwareverwerking via hergebruik, refurbishing, recycling en veilige datavernietiging. Apparatuur krijgt een tweede leven binnen organisaties of via maatschappelijke initiatieven. Samenwerking met gecertificeerde partners garandeert dataveiligheid en milieuvriendelijke verwerking conform WEEE- en ISO-normen. Rapportages geven inzicht in CO <sub>2</sub> -besparing, hergebruikpercentages en sociale impact. Circulariteit is verankerd in beleid, inkoopcontracten en ketenbeheer. Cloudgebruik en modulaire hardware beperken e-waste en energieverbruik. Medewerkers worden betrokken via bewustwording, leeromgevingen en donatieprogramma's. Doelstellingen zoals "zero waste to landfill" en closed loop supply chains zijn leidend. Innovaties zoals dashboards en GreenOps ondersteunen klanten bij verduurzaming. De aanpak draagt bij aan maatschappelijke waarde en structurele CO <sub>2</sub> -reductie.
<b>MVOI Sociale aspecten</b>			
16	Hanteert u een IMVO-beleid (dat aansluit bij de OESO-richtlijnen of UNGP's)? Bent u daarnaast bekend met de toepassing van Internationale Sociale Voorwaarden (ISV) in Europese aanbestedingen en op welke wijze geeft u hier invulling aan (zoals het uitvoeren van due diligence of het indienen van een IMVO-zelfverklaring)		Leveranciers hanteren een IMVO-beleid dat aansluit bij OESO-richtlijnen en de UN Guiding Principles on Business and Human Rights. Due diligence wordt toegepast om risico's in de keten te identificeren en te mitigeren, met aandacht voor mensenrechten, arbeidsomstandigheden, milieu en ethiek. Leveranciers worden beoordeeld op naleving van gedragscodes; bij tekortkomingen volgen corrigerende maatregelen. IMVO-zelfverklaringen en toepassing van Internationale Sociale Voorwaarden (ISV) zijn gangbaar bij aanbestedingen. Transparantie, rapportage en stakeholderdialoog zijn belangrijke onderdelen van de aanpak. IMVO is geïntegreerd in inkoop, leveranciersmanagement en contractbeheer. Diverse organisaties nemen deel aan internationale initiatieven zoals het UN Global Compact. Medewerkers en partners worden betrokken via gedragscodes, meldsystemen en trainingen. IMVO is verankerd in strategie én praktijk. De aanpak draagt bij aan maatschappelijk verantwoord ondernemen en duurzame ketenverantwoordelijkheid.

17	Zijn uw leveranciers of productielocaties gecertificeerd op sociale aspecten (zoals bijv. SA8000, BSCI, Fair Trade of vergelijkbaar)? Zijn daarover auditrapportages of andere vormen van monitoring beschikbaar?		Partijen nemen sociale ketenverantwoordelijkheid serieus en hanteren beleid conform OESO-richtlijnen en UNGP's. Leveranciers worden beoordeeld op naleving van mensenrechten, arbeidsomstandigheden en ethische normen. Certificeringen zoals SA8000, BSCI, ISO 45001 en RBA worden toegepast, ondersteund door audits, gedragscodes en due diligence-processen. Bij afwijkingen worden verbetermaatregelen genomen; ernstige schendingen kunnen leiden tot beëindiging van samenwerking. Transparantie, monitoring en rapportage zijn structureel ingebed in leveranciersmanagement. Gedragscodes verplichten naleving van sociale normen in de hele keten. Sommige organisaties gebruiken tools zoals Ecovadis of leveranciersportalen voor risicobeoordeling. Circulariteit en verantwoord grondstoffengebruik zijn onderdeel van inkoopcriteria. Ethische inkoop is gekoppeld aan duurzaamheidsdoelen en maatschappelijke impact. De aanpak bevordert eerlijke, veilige en verantwoorde ketens wereldwijd.
18	Hoe geeft u invulling aan social return, diversiteit en inclusie?		Partijen bevorderen social return via samenwerking met maatschappelijke partners, begeleidingstrajecten en inclusieve werkplekken. Mensen met afstand tot de arbeidsmarkt krijgen kansen via stages, traineeships en jobcoaching. Diversiteit en inclusie zijn verankerd in beleid, HR-processen en gedragscodes. Organisaties werken met certificeringen, interne netwerken en trainingsprogramma's voor bewustwording en gelijke kansen. Social return wordt afgestemd op klantcontext en aanbestedingseisen, vaak via maatwerkafspraken. Donatie van hardware, maatschappelijke projecten en educatieve initiatieven versterken sociale impact. Monitoring en rapportage zorgen voor transparantie en continue verbetering. Inclusieve technologie en samenwerking met onderwijsinstellingen dragen bij aan structurele verandering. DE&I is onderdeel van strategie én dagelijkse praktijk. De aanpak verbindt maatschappelijke verantwoordelijkheid met technologische innovatie.
<b>Ricico's en haalbaarheid</b>			
19	Hoe gaat u om met externe ontwikkelingen in de markt, zoals veranderde regelgeving (bijvoorbeeld door geopolitieke ontwikkelingen)? En hoe verwerkt u dat in uw aanbieding.		Leveranciers hanteren een gestructureerde en adaptieve aanpak om externe ontwikkelingen zoals veranderende wet- en regelgeving en geopolitieke trends te integreren in hun dienstverlening. Dit gebeurt via continue monitoring, risicoanalyses, governance-frameworks en strategische samenwerking, vaak ondersteund door expertgroepen en compliance-modellen. Veel partijen benadrukken security- en compliance-by-design, anticiperen op regelgeving zoals NIS2, GDPR en BIO, en bieden flexibiliteit via cloud- en datasoevereine oplossingen. Innovatie, audits en klantgerichte roadmaps zorgen ervoor dat diensten toekomstbestendig blijven, met aandacht voor transparantie, risicobeheersing en samenwerking.
<b>Licentie en kosten</b>			
20	Om te kunnen budgetteren en om te bepalen welke aanbestedingsstrategie het beste past, vragen wij om een complete modulaire prijsstelling op te leveren (incl. afreken(licentie)model, beheer, support, upgrades, configuratie, opleiding gebruikers, specialisten, etc.).		De meeste leveranciers hanteren een modulaire prijsstructuur, vaak met onderscheid tussen vaste kosten en variabele componenten (bijvoorbeeld P*Q-modellen). Sommige partijen geven indicatieve prijscomponenten of bandbreedtes, terwijl anderen aangeven prijzen pas in een latere fase te delen of verwijzen naar bestaande afspraken. Er wordt regelmatig flexibiliteit geboden via toelichtende gesprekken en aanvullende opties.
21	Hanteert u licentievoorwaarden (zoals EULA)? Waarop hebben deze exact betrekking?		De meeste leveranciers hanteren licentievoorwaarden, vaak gebaseerd op standaardvoorwaarden van softwareleveranciers zoals Microsoft, Oracle of Adobe. Deze voorwaarden hebben betrekking op gebruik, intellectuele eigendomsrechten, beveiliging, updates en aansprakelijkheid. Sommige partijen beperken hun voorwaarden tot eigen ontwikkelde producten, terwijl anderen ondersteuning bieden bij licentiebeheer via tools of advies. Enkele leveranciers geven aan dat details later of mondeling worden toegelicht, maar er is brede consensus over het belang van transparantie en compliance.
22	Is een grote upgrade naar een opvolgend besturingssysteem inbegrepen in de prijsstelling? Zo niet, hoe definieert u het verschil tussen updates en (grote) upgrades en hoe worden de kosten in rekening gebracht?		Leveranciers geven aan dat reguliere updates, zoals beveiligingspatches en kleine verbeteringen, standaard zijn inbegrepen in de dienstverlening. Grote upgrades, zoals de overgang naar een nieuw besturingssysteem, worden meestal als aparte projecten behandeld vanwege hun impact op hardware, applicaties en gebruikers. Kosten voor deze upgrades zijn afhankelijk van migratie-inspanningen, licentievoorwaarden en eventuele hardware-aanpassingen, en worden vaak apart geoffreerd. Sommige partijen bieden de mogelijkheid om deze kosten vooraf als optiepost op te nemen voor meer voorspelbaarheid.
<b>AI</b>			

23	Past u AI of algoritmes toe in uw oplossing? Hoe borgt u transparantie, governance en naleving (bv. AI-verordening)?	De meeste leveranciers geven aan AI of algoritmes toe te passen, vaak in de vorm van Microsoft Copilot, generatieve AI of intelligente agents voor IT-serviceprocessen (incidentafhandeling, monitoring, automatisering). Transparantie en governance worden geborgd via interne AI-governance frameworks, registers, risicoclassificatie en documentatie. Meerdere leveranciers noemen expliciet DPIA's, audit trails, explainable AI en menselijke controle. Compliance: De meeste leveranciers verwijzen naar naleving van de EU AI Act, AVG/GDPR en ethische richtlijnen. Sommigen hebben eigen frameworks (bijv. Responsible AI Framework, GAIA-model) en benoemen technische borging via Microsoft Purview, RBAC en auditlogging. Training en bewustwording: Verschillende leveranciers bieden workshops, richtlijnen en AI-geletterdheidstrajecten om verantwoord gebruik te waarborgen.
24	Aan welke nationale/internationale AI-richtlijnen kunt u voldoen?	EU AI Act wordt door vrijwel alle leveranciers genoemd als primair kader, inclusief risicoclassificatie en transparantie-eisen. AVG/GDPR is standaard onderdeel van compliance, vooral bij verwerking van persoonsgegevens. Internationale kaders zoals OECD AI Principles, ISO/IEC 42001, NIS2 en soms UNESCO-richtlijnen worden door meerdere leveranciers genoemd. Enkele leveranciers verwijzen naar nationale toezichhouders (bijv. Autoriteit Persoonsgegevens) en interne governance boards. Sommige leveranciers geven aan actief deel te nemen aan Europese initiatieven zoals het AI Pact of kennisdeling binnen internationale netwerken.
25	In hoeverre is AI, bijvoorbeeld in de vorm van Microsoft Copilot, onderdeel van uw visie op de digitale werkplek? En hoe ondersteunt u organisaties bij de adoptie hiervan?	Alle leveranciers zien AI als een integraal onderdeel van de moderne digitale werkplek en noemen Microsoft Copilot expliciet als belangrijke tool. AI wordt gepositioneerd als middel om productiviteit, automatisering en gebruikerservaring te verbeteren, vaak gecombineerd met maatwerkagents en integratie in Microsoft 365. Adoptieondersteuning: Leveranciers bieden workshops, training, change management, e-learning en governance-advies. Sommige hanteren frameworks zoals Prosci/ADKAR of eigen adoptieprogramma's. Technische ondersteuning: Meerdere leveranciers bieden assessments (bijv. AI Readiness), tenantconfiguratie, security checks en integratie met bestaande processen. Enkele leveranciers benadrukken hybride of soevereine AI-architecturen voor datacontrole en compliance.
<b>Technologie en implementatie</b>		
26	Wat zijn volgens u de belangrijkste randvoorwaarden ten aanzien van resourceplanning voor soepele, technische implementaties gedurende een beheerperiode?	1) Langetermijnplanning: Voorkomt verstoringen door duidelijke planning en samenwerking met de business 2) Correcte intake: Zorgt voor efficiënte vertaling van functionele vragen naar technische oplossingen 3) Kennis van klant en omgeving: Een dedicated beheerteam met diepgaande kennis is cruciaal
27	Welke adoptieactiviteiten neemt u op zich bij de invoering van uw oplossing en wat verwacht u van het Kadaster?	Alle partijen hebben hun adoptieaanpak toegelicht, waarbij een aantal partijen inzetten op trainingen, communicatie en monitoring met actieve betrokkenheid van het Kadaster. Twee partijen hanteren een gestructureerde veranderaanpak met nadruk op pilots en change-activiteiten. Eén partij ziet beperkte adoptie-inspanningen als voldoende vanwege bestaand draagvlak binnen het Kadaster.
28	Hoe organiseert u gebruikerssupport en wat is uw ervaring met adoptie van werkplekken incl. M365, audiovisuele middelen en printers?	Zes partijen hebben hun supportaanpak toegelicht, waaronder persona-gebaseerde ondersteuning, regieorganisaties, Techbars, en ADKAR-gebaseerde adoptie. Eén partij gaf aan dit onderwerp liever mondeling toe te lichten, en één partij benoemde audiovisuele middelen en printers niet expliciet, maar impliceerde deze binnen bredere dienstverlening. Meerdere partijen hebben ervaring met M365, AV-middelen en printers, vaak ondersteund door gespecialiseerde partners.
<b>AVG</b>		
29	Kun u een voorstel doen voor een verwerkersovereenkomst.	Zes partijen hebben bevestigd dat zij een verwerkersovereenkomst aanbieden of kunnen opstellen, waarbij sommigen aanvullende maatregelen of maatwerkopties benoemen. Eén partij verwijst naar een apart bestand dat niet is opgenomen in het document. Eén partij stelt voor om de bestaande overeenkomst als basis te gebruiken en samen met de opdrachtgever te evalueren en aan te passen.
30	Kan uw dienst overweg met een de Rijksbrede verwerkersovereenkomst, waar het Kadaster een eigen versie van hanteert?	Vier partijen hebben bevestigd dat zij kunnen werken met de Rijksbrede verwerkersovereenkomst, eventueel inclusief Kadaster-specifieke aanpassingen. Twee partijen staan open voor de overeenkomst, maar willen eerst verduidelijking of beoordeling van specifieke versies. Eén partij lijkt flexibel en ervaren, wat suggereert dat aansluiting mogelijk is, hoewel dit niet expliciet is bevestigd.
<b>Security</b>		

31	Welke rol speelt security in uw visie op de inrichting van een digitale werkplek voor organisaties zoals het Kadaster? (toelichting: in het kader van gebruiksvriendelijkheid versus veiligheid?)		Security wordt door alle leveranciers gezien als een fundamenteel onderdeel van de digitale werkplek, gebaseerd op principes zoals security by design en Zero Trust. Er wordt gestreefd naar een balans tussen veiligheid en gebruiksvriendelijkheid, met toegangsbeheer op basis van identiteit, apparaatstatus en context, ondersteund door technologieën zoals MFA, Intune en Azure AD. Moderne oplossingen zoals cloud-native monitoring worden ingezet voor realtime detectie en respons, aangevuld met compliance volgens normen als ISO27001, BIO en AVG. Daarnaast is er aandacht voor bewustwording, training en samenwerking binnen integratiemodellen zoals SIAM om regie en grip op security te behouden.
32	Wat is uw aanpak bij incidentmanagement, zoals een (dreigend) datalek of systeeminbreuk? (Hoe verloopt detectie, melding, opvolging?)		Leveranciers hanteren een gestructureerde aanpak voor incidentmanagement met proactieve detectie via SIEM-technologie, gedragsanalyse en 24/7 monitoring vanuit SOC's. Respons verloopt volgens gestandaardiseerde frameworks zoals ITIL of ISO 27035, met registratie en prioritering in ITSM-tools zoals ServiceNow of TOPdesk. Samenwerking binnen SIAM-structuren zorgt voor snelle coördinatie, gevolgd door herstelmaatregelen, root cause-analyses en beleidsupdates. Preventie wordt geborgd via Security- en Privacy-by-Design, gedragsmonitoring en machine learning, met naleving van normen zoals ISO 27001, BIO en AVG en duidelijke rapportages voor continue verbetering.
<b>SIAM, SLA, support en beheer</b>			
33	Heeft u ervaring in het werken in een SIAM-ecosysteem, hoe positioneert u zich binnen zo'n ecosysteem en op welke wijze draagt u bij aan de samenwerking?		Alle leveranciers hebben ruime ervaring met werken binnen SIAM-ecosystemen en positioneren zich als actieve samenwerkingspartners. Hun aanpak richt zich op integratie, governance, transparantie en het faciliteren van samenwerking tussen meerdere leveranciers, vaak inclusief multi-vendor management en procesafstemming. Er wordt nadruk gelegd op communicatie, gezamenlijke doelstellingen en continue verbetering, ondersteund door tooling zoals ServiceNow en frameworks voor regie en rapportage. Leveranciers bieden daarnaast kennis van technologie en processen, training en ondersteuning om soepele samenwerking en een consistente gebruikerservaring te waarborgen.
34	Welke technische middelen op de gebruikersapparaten kunnen worden ingezet om de gebruikerservaring (XLA) te meten?		Leveranciers meten en verbeteren de gebruikerservaring (XLA) met Digital Experience Monitoring-tools en vaak aangevuld met dashboards en feedbacksystemen. AI, automatische foutdetectie en UX-analysetools worden ingezet om prestaties, stabiliteit en netwerkvertragingen te monitoren. Sommige partijen combineren dit met persona-gebaseerde benaderingen, design thinking en journey-analyses om gerichte verbeteringen door te voeren. Ondersteuning vindt plaats via servicedesks, selfserviceportalen en adoptieprogramma's, met focus op continue optimalisatie van de digitale werkplek. 3 leveranciers noemen aanvullende beveiligingsmaatregelen zoals privileged access, zero trust policies, subnetsegmentatie of SIEM-integratie.
<b>Hosting</b>			
35	Wat is een gangbare manier van hosting en worden alle componenten door uzelf gehost?		Leveranciers hanteren overwegend een hybride hostingstrategie, waarbij combinaties van private cloud, public cloud (zoals Azure, AWS, Google Cloud) en on-premises infrastructuur worden ingezet. Hosting wordt afgestemd op klantbehoeften, compliance-eisen en regievoorkeuren, met opties voor soevereine cloudoplossingen en integratie met bestaande omgevingen. Sommige partijen bieden eigen cloudplatformen of edge-hosting, terwijl anderen optreden als integrator en samenwerken met gespecialiseerde hostingpartners. Flexibiliteit, schaalbaarheid en veiligheid staan centraal, met aandacht voor datalocatie, kostenbeheersing en exitstrategieën.
<b>Contractering en exitstrategie</b>			
36	Hoe ziet een exit-strategie eruit, inclusief data-overdracht en afbouw van diensten en wat zijn de kosten en risico's.		Alle leveranciers hanteren een exit-strategie die continuïteit en overdraagbaarheid vanaf de start waarborgt. Dit gebeurt via een contractueel of projectmatig geborgd exitplan, waarin overdracht van data, documentatie, rechten en kennis centraal staat, vaak gefaseerd en met validatiemomenten. Kosten worden vooraf inzichtelijk gemaakt, meestal op basis van vaste afspraken of ratecards, zodat financiële consequenties voorspelbaar zijn. Risico's zoals vendor lock-in, incomplete documentatie of verstoring van kritieke diensten worden geminimaliseerd door standaardisatie, planning, risicologboeken en betrokkenheid van ervaren specialisten. Alle strategieën benadrukken transparantie, samenwerking en beveiliging tot het einde van het proces.
<b>Flexibiliteit</b>			
37	Is uw oplossing standaard, open source of is er sprake van maatwerk, en maakt u gebruik van "open standaarden" (bv. ISO/IEC 19941:2017)? Licht toe. Wij vragen dit omdat wij zoveel mogelijk gebruik maken van vendor-agnostische koppelingen.		Alle leveranciers bieden oplossingen die modulair, gestandaardiseerd en interoperabel zijn, met beperkte inzet van maatwerk om overdraagbaarheid en continuïteit te waarborgen. Open standaarden zoals ISO/IEC 19941:2017 en protocollen (bijv. SAML, OpenID Connect, RESTful API's) worden breed toegepast om vendor-agnostische koppelingen en integratie met andere systemen mogelijk te maken. Veel oplossingen zijn gebaseerd op commerciële platformen zoals Microsoft 365, Azure Virtual Desktop, aangevuld met open source componenten waar nodig. Flexibiliteit, schaalbaarheid en toekomstbestendigheid staan centraal, waarbij vendor lock-in wordt voorkomen door standaardisatie en transparantie. Alle strategieën ondersteunen een digitale werkplek die eenvoudig kan integreren met andere leveranciers en systemen.

Overige		
38 Welke aanvullende onderwerpen, signalen, kansen of risico's zijn volgens u van belang maar niet aan bod gekomen? Licht toe met relevantie voor het Kadaster.		Leveranciers benadrukken het belang van een sterke focus op gebruikerservaring en adoptie, ondersteund door XLA's, structurele feedback en continu verandermanagement, vooral bij invoering van AI en nieuwe werkwijzen. Governance, integrale regie en uniforme security-kaders zijn cruciaal om versnippering en compliance-risico's te voorkomen, met aandacht voor NIS2, BIO en ISO-normen. Er wordt gepleit voor interactieve dialoogsessies, duidelijke beoordelingscriteria (kwaliteit boven prijs), en flexibele contracten die ruimte bieden voor innovatie, duurzaamheid en maatschappelijke verantwoordelijkheid. Tot slot wordt gewezen op risico's rond exitstrategieën, tooling-overname en de noodzaak van samenwerking in Agile/DevOps-teams om wendbaarheid en continuïteit te waarborgen.