Ref.	Onderwerp	Vraag	Antwoord	Beantwoord op	Beantwoord door
1	Prijzenblad	In het prijzenblad vraagt u om een "Totaalbedrag Licenties Reserveringssysteem (eindgebruikers)". Wij hanteren een licentie op basis van reserveerbare eenheden (werkplek). Kunt u aangeven om hoeveel reserveerbare eenheden het gaat.	Het gaat om 220 werkplekken en omstreeks 35 vergaderruimtes.	9-10-2025	Corrien
2	Programma van Eisen	In het Programma van Eisen maakt u bij 1.14 en 1.15 duidelijk dat er in elke ruimte aanwezigheidssensoren zijn/geplaatst moeten worden. In 1.16 geeft u aan dat er Yealink aanwezigheidssensoren in de ruimtes zijn. Zijn alle 50 ruimtes, waarvoor u in het Prijzenblad een roomdisplay een prijs aanvraagt voorzien van Yealink aanwezigheidsensoren.	De huidige ruimtes zijn voorzien van Yealink video-conferentie systemen, welke Yealink Mtouch 2 panelen bezitten waarin een ingebouwde presence sensor zit. Het is voor ons niet duidelijk of deze sensoren gebruikt kunnen worden. Er zijn géén aparte Yealink Roomsensoren aanwezig.	9-10-2025	Tymen/Frank
3	Prijzenblad	Indien wij eigen sensoren willen installeren, kunnen wij de kosten van de sensoren optellen bij het onderwerp Roomdisplay op het Prijzenblad?	Ja, dat klopt.	13-10-2025	Tymen
4	Prijzenblad	In het Prijzenblad wenst u een totaalbedrag voor "Aanschaf NFC Stickers tbv werkplekreservering". In het Programma van Eisen bij 1.7 meldt u dat de medewerkers moeten kunnen inloggen met QR-Stickers. Kunnen wij ervan uitgaan dat u in het Prijzenblad QR-Stickers bedoelt?	Ja dat klopt. QR codes, dan wel NFC stickers zijn beide prima.	9-10-2025	Corrien
5	Programma van Eisen	Beschikt u al over een narrowcastingsysteem waarbinnen wij de interactieve plattegrond moet integreren of vraagt u ons ook een narrowcastingsysteem aan te bieden?	Opdrachtgever heeft op dit moment geen narrowcastingsysteem.	9-10-2025	Corrien
6	Plattegronden	Om een goede aanbieding te kunnen maken, hebben wij meer informatie nodig over uw pand(en). Om hoeveel panden gaat dit, met hoeveel verdiepingen? Dit in verband met het bepalen van het aantal sensoren en het juiste aantal licenties. Kunt u plattegronden delen?	Het gaat om 2 panden. Deze panden liggen hemelsbreed een paar honderd meter uit elkaar	9-10-2025	Corrien
7	1.16 | Bijlage 1 pakket van eisen	Er wordt naar integratie van Yealink teams rooms system gevraagd. - Kunt u bevestigen dat er in iedere ruimte een Yealink RoomSensor beschikbaar is?	De huidige ruimtes zijn voorzien van Yealink video-conferentie systemen, welke Yealink Mtouch 2 panelen bezitten waarin een ingebouwde presence sensor zit. Het is voor ons niet duidelijk of deze sensoren gebruikt kunnen worden. Er zijn géén aparte Yealink Roomsensoren aanwezig.	9-10-2025	Tymen/Frank
8	Bijlage 5 | Prijzenblad	Bij 1.16 uit bijlage 1 'pakket van eisen' is er een keuze tussen integratie van bestaande sensoren of het aanbieden van nieuwe sensoren. Waar kan de aanschaf van nieuwe sensoren in het prijzenblad worden ingevuld?	De kosten van de ruimtesensoren kunt u invullen bij 'aanschaf roomdisplays'		
9	1.30 | bijlage 1 pakket van eisen	Kunt u de eis rondom de koppeling met power BI verduidelijken?	Wij zijn voornememens rapportage middels powerbi hiermee te maken		
10	Wensenlijst	Dienen de wensen die met een 'ja' zijn beantwoord daadwerkelijk geïmpementeerd te worden?	Nee, niet alle wensen hoeven direct geimplementeerd te worden.	9-10-2025	Corrien
11	Offerteaanvraag	U geeft in dit document aan dat kwaliteit erg belangrijk is en dat een soepel lopend project erg belangrijk is. Aan de andere kant is de factor prijs 60% van de gunningscriteria. Kunt u uitleggen waarom voor dit onderscheid is gekozen en overweegt u om deze verdeling aan te passen naar 60-40 ipv 40-60?	Opdrachtgever gaat hier niet mee akoord.	9-10-2025	Corrien
12	Bijlage 5: Prijzenblad	In het prijzenblad spreekt u van een NFC sticker, in het PVE wordt gesproken over een QR code. Dit zijn in onze optiek 2 verschillende onderdelen. Wat is leidend in deze?	Beide zijn prima, ofwel een NFC sticker, ofwel een QR code.	9-10-2025	Corrien

13	Bijlage 5: Prijzenblad	Wij hanteren een licentie structuur op basis van software, gebruikers en Hardware. Gaat de Gemeente Heerenveen ermee akkoord dat de leverancier de verschillende licentielijnen opnemen in het Prijzenblad zodat de Gmeente Heerenveen een goed vergelijk kan maken tussen de verschillende aanbieders?	Opdrachtgever gaat hier niet mee akkoord. Opdrachtgever is erbij gebaat dat iedereen het op dezelfde manier invult, zodat we een deugdelijke vergelijking kunnen maken. Het prijzenblad vervult in deze wens.	9-10-2025	Tymen
14	PVE 3.7 en 3.8	U geeft in deze eisen aan waar de Hardware aan moet voldoen. In hoeverre wil de gemeente Heerenveen ook de werkplekken voorzien van bezettingssensoren?	Werkplekken hoeven op dit moment niet voorzien te worden van bezettingssensoren.	9-10-2025	Corrien
15	PVE 3.7 en 3.8	U geeft in deze eisen aan waar de Hardware aan moet voldoen. Is het voor de gemeente Heerenveen voldoende als de bezetting van de vergaderruimtes gemeten wordt of wil de gemeente Heerenveen ook de benutting meten?	Het is voor opdrachtgever voldoende dat de bezetting gemeten wordt.	9-10-2025	Corrien
16	GIBIT 2020	U heeft Bijlage 3B GIBIT 2020 toegevoegd in uw aanbestedingsdocumenten. Hoe verhoudt dit zich tot de GIBIT 2023 die op dit moment leidend is?	Opdrachtgever heeft de voorwaarden gewijzigd naar de Gibit 2023		
17	GIBIT 2023 art 24.14	Wij achten het redelijk om deze bepaling wederkerig te maken.	Opdrachtgever gaat hiermee akoord		
18	GIBIT 2023 art 24.1	Wij achten het redelijk om deze bepaling wederkerig te maken.	Opdrachtgever gaat hiermee akoord		
19	GIBIT 2023 art 20.5	Wij voegen hier graag aan toe dat Opdrachtgever zich zal onthouden van enige toegevingen betreffende de (mogelijke) aansprakelijkheid van de Leverancier en de inbreuk niet te wijten zal zijn aan de Opdrachtgever zelf.	Opdrachtgever gaat hiermee akoord		
20	GIBIT 2023 art 20.3	Om enig misverstand te vermijden voegen wij hier graag aan toe dat het gaat om een niet-exclusief en niet-overdraagbaar gebruiksrecht.	Opdrachtgever gaat hiermee akoord		
21	GIBIT 2023 art 16.1	Het is gebruikelijk dat contractspartijen in commerciële overeenkomsten hun aansprakelijkheid beperken tot directe schade, met uitsluiting van enige aansprakelijkheid voor indirecte schade, gevolgschade of enige derving van winst. Graag zien wij dit aangepast.	Opdrachtgever gaat hiermee niet akkoord.		
22	GIBIT 2023 art 10.14 (ii)	Het is redelijk om meerkosten voor onderhoud meteen of binnen een redelijke termijn in rekening te kunnen brengen indien deze te wijten zijn aan het achterlopen op of weigeren van een Update en/of Upgrade door de Opdrachtnemer en niet pas na 18 maanden. Gelieve de verwijzing naar 18 maanden te willen schrappen, dan wel te willen wijzigen in 6 maanden (redelijke termijn).	Opdrachtgever gaat hiermee akoord		
23	Bijlage 2: Conceptovereenkomst	In uw conceptovereenkomst zijn door de Gemeente Heerenveen meerdere opmerkingen opgenomen aangaande inkoop leveringen en inkoop diensten. Volgens Pagina 5 zouden de Algemene inkoopvoorwaarden onder Bijlage 2 zijn opgenomen. Bijlage 2 is echter de concept overeenkomst. Kunt u dit verduidelijken en indien nodig de juiste documenten beschikbaar stellen?	De Gibit 2023 is van toepassing. Deze zijn bijgevoegd in bijlage 3.		
24	Bijlage 2: Conceptovereenkomst	6.1: U geeft aan dat facturering volgens het betalingsschema zoals gebruikelijk in de branche verloopt. Dit schema is niet toegevoegd aan de conceptovereenkomst. Wij factureren onze Licenties jaarlijks vooruit en onze Hardware direct na levering. Uren worden na uitvoering aan u doorbelast. Gaat u hiermee akkoord?	Opdrachtgever gaat hiermee akoord.		
25	Offerteaanvraag	In uw uitvraag spreekt u over 200 werkplekken en minimaal 20 vergaderruimtes. Daarnaast geeft u aan dat het systeem gebruikt moet kunnen worden door alle medewerkers van de gemeente Heerenveen die hiervoor in aanmerking komen. Om tot een passende aanbieding te komen is het van belang om inzichtelijk te krijgen wat de juiste aantallen zijn. Graag ontvangen wij dan ook het exacte aantal vergaderruimtes, verdiepingen en medewerkers.	220 werkplekken en omstreeks 35 vergaderruimtes. Verdeeld over 2 panden. Het ene pand heeft 3 etages, het andere pand 4. Opdrachtgever heeft ongeveer 500-600 medewerkers in dienst die wellicht het systeem gaan gebruiken.	9-10-2025	Corrien

26	PvE 5.29 Thycotic-eis voor beheer	In eis 5.29 wordt Thycotic als vereiste genoemd voor beheerderstoegang. Dit is vendor-specifiek. Kunt u bevestigen dat een vendor-neutrale PAM-oplossing (bijv. Delinea/Thycotic, CyberArk, BeyondTrust) óf SSO + MFA met least-privilege en auditeerbare sessies ook wordt geaccepteerd, zodat we kunnen aansluiten op de bestaande IAM-inrichting van de opdrachtgever? Voorstel tekstwijziging (compact): "Voor beheerderstoegang wordt gebruikgemaakt van een PAM-voorziening met credential-vaulting, JIT/JEA, logging en (indien beschikbaar) session recording. Vendor-neutraal (o.a. Delinea/Thycotic, CyberArk, BeyondTrust) en te integreren met SSO + MFA. Het noemen van Thycotic is voorbeeld en geen verplichte tooling."	Opdrachtgever laat eis vervallen.	9-10-2025	Frank/Tymen
27	PvE 5.9 Technisch Dossier voor gunning	In eis 5.9 wordt gevraagd om vóór gunning een technisch dossier met o.a. testresultaten van de laatste 12 maanden, inclusief pentest-/fuzzingrapport(en) en remediate-status. Dit is pre-award zeer vertrouwelijk/IP-gevoelig. Kunt u bevestigen dat bij inschrijving een samenvatting op hoofdlijnen volstaat en dat het volledige dossier na gunning en onder NDA wordt aangeleverd (eventueel gefaseerd tijdens implementatie)? Voorstel tekstwijziging (compact): "Bij inschrijving levert inschrijver een functionele/security-samenvatting (architectuur op hoofdlijnen, maatregelen, risico's/mitigaties). Na gunning en onder NDA levert inschrijver het volledige technisch dossier incl. recente testresultaten/pentest-/fuzzingrapport(en) en remediate-status; aanlevering mag gefaseerd plaatsvinden gedurende de implementatie."	Wij kunnen niet akkoord gaan met het voorstel om bij inschrijving uitsluitend een samenvatting op hoofdlijnen aan te leveren en het volledige technisch dossier pas na gunning beschikbaar te stellen. Als opdrachtgever hebben wij vóór gunning, onder NDA, inzage nodig in de volledige testresultaten, inclusief pentest-/fuzzingrapporten en de bijbehorende remediate-status. Deze inzage is noodzakelijk om niet alleen de kwaliteit en volwassenheid van de oplossing te kunnen beoordelen, maar ook om inzicht te krijgen in hoe de inschrijver omgaat met bevindingen en kwetsbaarheden. Dit is een belangrijk aspect van cybersecurity governance en risicobeheersing, en moet meegewogen kunnen worden in de gunning. Daarnaast biedt een samenvatting op hoofdlijnen van architectuur, beveiligingsmaatregelen en risico's/mitigaties onvoldoende diepgang om te kunnen voldoen aan de eisen die wij vanuit wet- en regelgeving hebben ten aanzien van informatiebeveiliging en risicobeoordeling. Wij begrijpen dat het aanleveren van een volledig technisch dossier voorafgaand aan gunning een belasting kan vormen. Daarom bieden wij de mogelijkheid om deze inzage – onder NDA – te organiseren via een whiteboard-sessie met uw specialisten. Dit biedt ruimte voor toelichting en interactie, zonder dat direct het volledige dossier hoeft te worden overgedragen, en kan de administratieve last beperken.	13-okt	

28	PvE 2.24 Jaarlijkse technische testen door der	In eis 5.24 staat dat alle (sub)leveranciers hun oplossing "aantoonbaar jaarlijks getest" moeten hebben. Voor COTS-hardware en standaard clouddiensten van derden is dit niet proportioneel en veelal buiten onze beïnvloedingssfeer. Kunt u bevestigen dat deze eis beperkt is tot onze eigen SaaS/backend en publiek toegankelijke API's, en dat voor derde partijen wordt volstaan met: actieve monitoring en opvolging van vendor-security-advisories en CVE's, het overleggen van relevante certificeringen/attestaties (bijv. ISO/IEC 27001, SOC 2) waar beschikbaar, en een patch-/updatebeleid conform afgesproken SLA's? Voorstel tekstwijziging: "Inschrijver voert jaarlijks onafhankelijk technisch testen (o.a. pentest) uit op de eigen SaaS/backend en publiek toegankelijke API's. Voor COTS-componenten en derde-partijdiensten borgt inschrijver risicogebaseerd beheer: monitoring en opvolging van vendor-advisories/CVE's, overleg van beschikbare certificeringen/attestaties en patchmanagement conform SLA. Waar directe beïnvloeding ontbreekt, geldt een redelijke inspanningsverplichting."	Wij kunnen niet akkoord gaan met het voorstel om de eis tot aantoonbaar jaarlijks testen uitsluitend te beperken tot de eigen SaaS/backend en publiek toegankelijke API's. Hoewel wij begrijpen dat COTS-componenten en standaard clouddiensten van derden vaak buiten directe beïnvloeding vallen, is het voor ons als aanbestedende dienst essentieel om vóór gunning inzicht te krijgen in hoe deze onderdelen worden geborgd binnen het totale beveiligingsproces. De voorgestelde aanpak — risicogebaseerd beheer, monitoring van vendor-advisories en CVE's, certificeringen en patchbeleid — kan een proportionele invulling zijn, mits deze onderbouwd wordt met een risico-inschatting en procesbeschrijving. Wij willen deze onderbouwing vóór gunning kunnen beoordelen, zodat we dit aspect kunnen meewegen in de gunning en niet pas na contractsluiting geconfronteerd worden met lacunes in de ketenbeveiliging. Daarnaast willen we benadrukken dat deze eisen mede voortkomen uit de BIO2 en andere relevante wet- en regelgeving, waarin van verwerkers wordt verlangd dat zij niet alleen hun eigen beveiliging op orde hebben, maar ook die van hun sub- en sub-subleveranciers in kaart brengen en aantoonbaar beheersen. Als verantwoordelijke partij moeten wij dit kunnen aantonen richting toezichthouders. Om de administratieve belasting te beperken, staan wij open voor een pragmatische invulling, bijvoorbeeld via een whiteboard-sessie met uw specialisten waarin het risicobeheerproces en de borging van derde-partijdiensten worden toegelicht. Dit biedt ons voldoende inzicht zonder dat direct alle documentatie hoeft te worden overgedragen.		
29	5.22 Onafhankelijke pentest ≤12 mnd op bac	Dit is voor COTS-devices niet realistisch. Voorstel: beperken tot SaaS/backend & API; voor devices vendor-attestaties en hardening-richtlijnen.	Wij kunnen niet akkoord gaan met het voorstel om de eis tot onafhankelijke pentest binnen 12 maanden uitsluitend te beperken tot de eigen SaaS/backend en publiek toegankelijke API's. Hoewel wij begrijpen dat COTS-devices vaak buiten directe beïnvloeding vallen, is het voor ons als aanbestedende dienst essentieel om voorafgaand aan gunning inzicht te krijgen in hoe deze componenten worden geborgd binnen het totale beveiligingsproces. Net als bij eerdere vragen staan wij open voor een proportionele invulling op basis van een risicogebaseerd beheer. Dit betekent dat wij vóór gunning willen kunnen beoordelen hoe de leverancier omgaat met de beveiliging van devices, inclusief de onderbouwing van keuzes zoals het gebruik van vendor-attestaties en hardening-richtlijnen. Daarbij willen we benadrukken dat termen als "hardening-richtlijnen" in de praktijk sterk uiteen kunnen lopen. Waar de ene leverancier een HTTPS-verbinding als voldoende beschouwt, verwacht de andere een gedetailleerde onderbouwing van gebruikte cyphers, configuratieparameters en firmwarebeheer. Juist daarom is het van belang dat deze aanpak voorafgaand aan gunning in voldoende diepgang wordt besproken en beoordeeld, zodat wij als opdrachtgever kunnen vaststellen of de gekozen maatregelen proportioneel én effectief zijn in het licht van onze verplichtingen onder de BIO2 en andere relevante wet- en regelgeving. Om de administratieve belasting te beperken, staan wij ook hier open voor een pragmatische invulling, bijvoorbeeld via een whiteboard-sessie met uw specialisten waarin het risicobeheerproces en de borging van device-beveiliging worden toegelicht.		

30	PvE 5.35 en 5.36 Aanleveren (updates) SBOM	5.35 en 5.36: wij leveren hier standaard hardware (COTS), geen maatwerksoftware. Voor dergelijke producten zijn SBOM's (SPDX/CycloneDX) doorgaans niet beschikbaar en het delen daarvan kan botsen met IP-/vertrouwelijkheidsafspraken van de fabrikant. Kunt u bevestigen dat deze eisen niet van toepassing zijn op COTS-hardware en daarom vervallen? Als alternatief kunnen wij per product model- en firmwareversies, onze CVE-monitoringsprocedure en verwijzingen naar security-advisories van de fabrikant aanleveren.	Wij begrijpen dat het aanleveren van een SBOM (in SPDX of CycloneDX) voor standaard hardware (COTS) op dit moment niet altijd gangbare praktijk is, en dat dit voor leveranciers en hun fabrikanten nieuw, complex of zelfs als gevoelig kan worden ervaren. Tegelijkertijd willen we benadrukken dat deze eisen niet optioneel zijn: ze vloeien voort uit de verplichtingen onder de NIS2-richtlijn en de BIO2, waarin van verwerkers wordt verlangd dat zij inzicht en controle hebben over de gehele keten — inclusief componenten van sub- en sub-subleveranciers. Het doel van deze eisen is nadrukkelijk niet om broncode of intellectueel eigendom op te vragen, maar om machineleesbare metadata te verkrijgen over gebruikte componenten en versies. Dit is essentieel om snel en adequaat te kunnen reageren op kwetsbaarheden zoals die in Log4J, waarbij het ontbreken van keteninzicht leidde tot grote vertragingen en risico's in de respons. Wij erkennen dat SBOM's voor COTS-devices niet altijd beschikbaar zijn. Daarom staan wij open voor een risicogebaseerde invulling, waarbij de leverancier per product inzicht geeft in model- en firmwareversies, CVE-monitoringsprocedures en verwijzingen naar security-advisories van de fabrikant. Belangrijk is wel dat deze aanpak voorafgaand aan gunning wordt toegelicht en beoordeeld, zodat wij kunnen vaststellen of deze proportioneel en effectief is in het licht van onze verplichtingen. Juist in deze fase is het waardevol dat de leverancier beschrijft hoe zij — ook richting haar eigen leveranciers — toewerkt naar compliance met toekomstige kaders zoals de Cyber Resilience Act, die vanaf 2027 van kracht wordt. Een dergelijke beschrijving, in combinatie met een risicogebaseerde aanpak, vormt voor ons een passend en werkbaar antwoord op deze eisen.		
31	PvE 5.15 Algoritmen	In de eis staat: "Gebruik van algoritmen in de oplossing … wordt vooraf open en transparant aan de opdrachtgever voorgelegd, waarna de opdrachtgever kan beoordelen of deze mogen worden toegepast." Kunt u specificeren welke categorieën algoritmen dit betreft? Gaat het om: AI/ML-modellen die (mogelijk) besluiten over personen beïnvloeden, beveiligingsmechanismen (zoals encryptie/hashing), of operationele algoritmen (planning, zoek-/matchinglogica, optimalisatie)? Inzage in broncode en detailontwerp is doorgaans onverenigbaar met vertrouwelijkheid en intellectuele eigendomsrechten. Bedoelt u in plaats daarvan een functionele beschrijving van algoritmen die persoonsgegevens verwerken of materiële impact hebben op de dienstverlening? Graag verduidelijking van scope, diepgang (welke documentatie), en moment van aanleveren (bij ingebruikname / bij materiële wijziging).	Dank voor uw vraag en verzoek tot verduidelijking. Eis 5.15 heeft specifiek betrekking op het gebruik van AI-algoritmen, waaronder machine learning-modellen die (mogelijk) besluiten over personen beïnvloeden of impact hebben op processen en dienstverlening. Het gaat hierbij niet om beveiligingsmechanismen zoals encryptie of hashing, noch om puur operationele algoritmen zoals zoek-, plannings- of optimalisatielogica, tenzij deze algoritmen persoonsgegevens verwerken of materiële impact hebben op de dienstverlening. De toetsing die wij als opdrachtgever willen uitvoeren, richt zich in eerste instantie op de functionele beoordeling van het algoritme: wat doet het, welke data worden verwerkt, en wat is de impact op personen of processen? Daarbij is het niet noodzakelijk om inzage te krijgen in broncode of detailontwerp. Een functionele beschrijving volstaat, mits deze voldoende inzicht biedt in de werking en toepassing. Wanneer een algoritme onder de hoog risico-categorie valt (zoals gedefinieerd in de AI Act), gelden aanvullende verplichtingen. In dat geval moet de leverancier kunnen aantonen dat: Er een risicomanagementsysteem is opgezet om risico's te identificeren, verminderen en monitoren. Er een conformiteitsbeoordeling is uitgevoerd (bijv. CE-markering). Er voldoende documentatie beschikbaar is, zoals technische details, gebruikshandleiding en logbestanden. Er een Fundamental Rights Impact Assessment (FRIA) is uitgevoerd, waarin risico's voor grondrechten zijn geanalyseerd. Er sprake is van transparantie, zoals uitleg over de werking, automatische logging en labeling van output. Er menselijk toezicht is ingericht (bijv. human-in-the-loop of nauw toezicht). Er data governance wordt toegepast, inclusief waarborging van datakwaliteit, representativiteit en rechtmatigheid.		
32	Offerteaanvraag - algemeen	Kunt u het aantal werkplekken specificeren? Bijvoorbeeld aantal werkplekken, aantal belcellen, overlegruimtes.	220 werkplekken en omstreeks 35 vergaderruimtes.	9-10-2025	Corrien
33	Offerteaanvraag - algemeen	Kunt u plattegronden aanleveren?	Ja, deze gaan we aanleveren.	13-okt	Corrien

34	Prijzenblad	U geeft aan dat optioneel ruimtesensoren kunnen worden aangeboden. Er is geen ruimte voor op het Prijzenblad. Kunt u aangeven hoe we dit in de prijs kunnen verwerken?	De kosten van de ruimtesensoren kunt u invullen bij 'aanschaf roomdisplays'		
35	PvE 5.14 auditverklaring	In de eis staat: "De ISO27001 wordt jaarlijks door en auditverklaring als een ISAE3402 type 2 of SOC 2 aan te leveren." Kunt u toelichten wat hiermee precies wordt bedoeld? Is een geldige ISO/IEC 27001-certificering voldoende, of verlangt u daarnaast óók een ISAE 3402 type 2 of SOC 2-rapportage? Daarnaast: ISAE 3402 ziet op interne beheersing rond financiële verslaggeving (ICFR). Wij zien geen relatie met onze dienstverlening. Wilt u bevestigen dat ISAE 3402 en/of SOC 2 niet van toepassing is en de eis te laten vervallen of aan te passen?	De eis om jaarlijks een auditverklaring zoals een ISAE3402 type II of SOC 2 aan te leveren bij een ISO27001-certificering is geen harde eis, maar een nadrukkelijke wens vanuit de opdrachtgever. Deze wens vloeit voort uit het feit dat een ISO27001-certificering vooral aantoont dat procedures en beheersmaatregelen formeel zijn ingericht. Tijdens een ISO-audit worden deze maatregelen echter slechts steekproefsgewijs beoordeeld, en dat doorgaans eens per vier jaar. Hierdoor ontstaat het risico dat de certificering weliswaar geldig is, maar onvoldoende zegt over de daadwerkelijke werking van de maatregelen in de praktijk over een langere periode. Een auditverklaring zoals een ISAE3402 type II of SOC 2 biedt juist dat aanvullende inzicht: het toont aan dat de organisatie niet alleen beschikt over de juiste procedures, maar dat deze ook structureel en aantoonbaar worden nageleefd. Dat geeft ons als opdrachtgever meer zekerheid dat informatiebeveiliging niet alleen op papier staat, maar ook daadwerkelijk wordt toegepast. Een beeldspraak die dit illustreert: een ISO-certificaat is als een rijbewijs — het toont aan dat iemand bevoegd is om te rijden. Maar het zegt niets over hoe goed of veilig iemand daadwerkelijk rijdt. Een auditverklaring is dan als een rijvaardigheidstest over een langere periode: het laat zien hoe iemand zich in de praktijk gedraagt. Wij staan open voor een risicogebaseerde aanpak, waarbij de leverancier toelicht hoe zij invulling geeft aan de borging van de ISO27001-maatregelen in de praktijk. Een beschrijving van dit proces, inclusief hoe monitoring, interne audits of externe toetsing worden ingezet, kan voor ons een passend alternatief vormen en worden meegenomen in de beoordeling.		
36	PvE 3.6 Displays voor vergaderplekken	U geeft aan dat voeding via 230V moet verlopen. Betekent dat u niet over een PoE aansluiting beschikt bij de vergaderruimten? Dit staat wel expliciet vermeld bij 3.8 Ruimtesensoren. Als u niet over PoE beschikt zijn er bij alle ruimten aparte stroompunten beschikbaar?	Ja, dat klopt.	9-10-2025	Tymen/Frank
37	Programma van Eisen 1.16	U geeft aan dat er sensoren beschikbaar zijn. Zijn deze sensoren in alle vergaderruimten geinstalleerd? Kunt u exacte specificatie van deze sensoren aanleveren (type, firmware versie).	De huidige ruimtes zijn voorzien van Yealink video-conferentie systemen, welke Yealink Mtouch 2 panelen bezitten waarin een ingebouwde presence sensor zit. Het is voor ons niet duidelijk of deze sensoren gebruikt kunnen worden. Er zijn géén aparte Yealink Roomsensoren aanwezig.	9-10-2025	Tymen/Frank
38	Eis 3.1 PvE	Aanbestedende dienst vermeld dat de leverancier de technische implementatie verzorgt. Bedoeld aanbestedende dienst hiermee dat dit niet mag worden uitgevoerd door een derde partij?	Een derde partij is ook prima, de leverancier blijft aanspreekpunt en verantwoordelijk.	9-10-2025	Corrien
39	Eis 1.32 PvE	Aanbestedende dienst vraagt naar 4 beeldschermen, waarop de bezetting van werkplekken en ruimtes inzichtelijk wordt gemaakt. Gaat het in dit geval alleen om inzicht te krijgen van de bezetting van de werkplekken en ruimtes of wenst aanbestedende dienst ook aan dit beeldscherm een vrije ruimte of werkplek te kunnen reserveren?	Het gaat in dit geval om het krijgen van inzicht.	9-10-2025	Corrien

40	Prijzenblad	Kan de aanbestedende dienst bevestigen dat het invullen van de prijslijst (cel A17) voor de aanschaf van overzichtsschermen minimaal de volgende producten en kosten dient te omvatten: - Display conform eisen PVE - Wandbeugel - Benodigde bekabeling - Configuratiekosten - Installatie- en implementatiekosten overzichtsschermen	Opdrachtgever kan dit bevestigen	9-10-2025	Corrien
41	Prijzenblad	Kan de aanbestedende dienst bevestigen dat het invullen van de prijslijst (cel A16) voor de aanschaf van NFC-stickers minimaal de volgende producten en kosten dient te omvatten: - NFC-sticker - Designsticker met Heerenveen-logo, waarop de NFC-sticker wordt geplaatst ter verbetering van zichtbaarheid en herkenning bij het scannen - Custom Design kosten - Configuratiekosten - Installatie- en implementatiekosten van de NFC-sticker	Dit zal per aanbieder anders zijn. We gaan er wel van uit dat er een werkende NFC sticker, dan wel QR code wordt opgeleverd en dat de kosten om deze werkend te krijgen bij het product inzitten.	13-10-2025	Corrien
42	Prijzenblad	Kan de aanbestedende dienst bevestigen dat het invullen van de prijslijst (cel A15) voor de aanschaf van roomdisplays minimaal de volgende producten en kosten dient te omvatten: - 10" RoomDisplay (conform de eisen uit de aanbesteding) -Wand- of glasbeugel -Configuratiekosten -Installatie- en implementatiekosten	Eens	13-10-2025	Corrien
43	Planning	Inschrijver werkt al met veel gemeenten samen en heeft ruime ervaring met de aangeboden SaaS-oplossing, maar merken dat het onderdeel Informatieveiligheid in dit PvE uitzonderlijk uitgebreid is. Juist omdat Inschrijver dit belangrijk vindt, wilt Inschrijver de tijd nemen om alle eisen grondig te bestuderen. Zo kan Inschrijver scherpe, inhoudelijke vragen stellen die bijdragen aan een heldere en zorgvuldige inschrijving. Gaat de aanbestedende dienst ermee akkoord dat er tot en met vrijdag 10 oktober om 17.00 uur vragen kunnen worden gesteld ten behoeve van Nota van Inlichtingen 1?	Opdrachtgever gaat hier niet mee akkoord.		
44	Eis 5.10 PvE	De inschrijver biedt conform de uitvraag een SaaS-platform aan. Kan de aanbestedende dienst toelichten waar eis 5.10 specifiek betrekking op heeft?	Ook voor een SaaS oplossing is het belangrijk dat we terug kunnen vallen op een roll-back omgeving en dat er een duidelijke manual is.		
45	Eis 1.23 PvE	De voorgestelde inrichting leidt tot veel beheerslast. Het is efficiënter om op ruimteniveau te bepalen of catering geboekt kan worden. Indien een gebruiker bevoegd is om een ruimte te boeken, ligt het voor de hand dat hij ook de bijbehorende services kan reserveren. Neemt aanbestedende dienst dit advies over?	Nee, dat nemen wij niet over. Wij gaan in ons cateringbeleid inregelen dat niet iedereen bv een lunch of een koffiehap kan aanvragen. Dat willen we ingeregeld hebben in het reserveringssysteem.	13-10-2025	Corrien
46	Prijzenblad	De aangeboden SaaS-oplossingen voor werkplekreservering worden gelicentieerd op basis van het aantal werkplekken, en niet per medewerker/eindgebruiker. Kan de aanbestedende dienst toelichten hoe de inschrijver in dit geval het prijzenblad dient in te vullen, aangezien het huidige prijzenblad is ingericht op basis van het aantal eindgebruikers?	Opdrachtgever heeft het prijzenblad aangepast. Er is een optie tot werkplekreservering toegevoegd. Opdrachtnemer kan licentie of werkplekreservering invullen		

47	Eis 5.29 PvE	In de aangeboden SaaS-omgeving is het mogelijk om de beheerders toegang te geven via SSO op basis van EntraID. In de omgeving kan de authorisatie gescheiden worden tussen beheerders en gebruikers. Voldoet dat voor aanbestedende dienst?	Ja, dit voldoet.		