Dit bestand bevat nota van inlichtingen 1. d.d. 12 februari 2026 voor de Europees openbare aanbesteding SIEM/SOC - Steenwijkerland met referentienummer: 2025-028781

Indien u naar aanleiding van deze nota van inlichtingen nog vragen heeft kunt u deze stellen tot 26 februari 2026.

Vraag	Document	Pagina	Paragraaf/artikel	Vraag	Motivatie vraag	Antwoord
1	Uitnodiging tot inschrijving SIEM-SOC	4	Inleiding	Is er momenteel sprake van een bestaande Incident Response-voorziening, en zo ja, wanneer eindigt dit contract?	Aanbestedingswet, gelijkheids- en transparantiebeginsel	Nee, er is momenteel geen bestaand Incident Response-voorziening.
2	Uitnodiging tot inschrijving SIEM-SOC	4	Inleiding	Kan opdrachtgever aangeven of er in de afgelopen 12 maanden cybersecurity-incidenten hebben plaatsgevonden (zonder detail), en zo ja, op hoofdlijnen hoe hiermee is omgegaan en welke afdelingen of externe partijen hebben geholpen met het herstel?	Aanbestedingswet, gelijkheids- en transparantiebeginsel	Er zijn geen incidenten geweest in de afgelopen 12 maanden.
3	Uitnodiging tot inschrijving	7	Paragraaf 1.3.1	Heeft gemeente al ervaring met een SOC dienstverlening op basis van een SIEM oplossing in combinatie met Microsoft Sentinel? Zo ja, welke?		Nee, de gemeente heeft hier geen ervaring mee.
4	Uitnodiging tot inschrijving SIEM-SOC	1.3	7	U geeft aan dat Defender for Server actief is. Kunt u aangeven waar deze voor gebruikt wordt? Dit i.v.m. het feit dat volgens bijlage 12 de virtuele servers beveiligd zijn met Palo Alto Cortex als endpoint-security oplossing.		Vanwege einde contract wordt Palo Alto Cortex vervangen door Microsoft Defender for Server. Huidige bijlage 12 wordt verwijderd en vervangen door een nieuwe bijlage 12. Zie het antwoord op vraag 316 voor meer informatie.
5	Uitnodiging tot inschrijving SIEM-SOC	1.3	1	In het overzicht van actieve Defender onderdelen ontbreken Defender for Office en Defender for Cloud Apps. Is dit bewust? M.a.w. zijn deze onderdelen nog niet actief? Zo niet, staat de activering ervan op een routekaart? En dienen deze onderdelen als te koppelen logbon te worden meegenomen?	Het antwoord helpt ons om de gewenste scope correct te duiden.	De door uw genoemde onderdelen vallen niet binnen de scope van de opdracht.
6	Uitnodiging tot inschrijving SIEM-SOC	1.3	1	U geeft aan dat de virtuele servers zijn beveiligd zijn met Palo Alto Cortex. Is dit ook uw wens voor de gewenste situatie? M.a.w. dient Palo Alto Cortex als logbron gekoppeld te worden aan Microsoft Sentinel? Of wordt Palo Alto Cortex vervangen voor Microsoft Defender for Servers?	Het antwoord helpt ons om de gewenste scope correct te duiden.	Vanwege einde contract wordt Palo Alto Cortex vervangen door Microsoft Defender for Server.
7	Uitnodiging tot inschrijving	7		Wordt de huidige Microsoft omgeving inclusief Sentinel beheerd door de gemeente zelf of een externe partner?	Een goed beeld van de Ist situatie draagt bij aan de inschatting van de werkzaamheden voor de onboarding.	De gehele Microsoft omgeving wordt door de gemeente zelf beheerd.
8	Uitnodiging tot inschrijving SIEM-SOC	7	1.3.1.2	Een SOC-dienst is niet op genomen de definitielijst op bladzijde 5. Een SCO.is in de basis gericht op detectie en het vergroten van de weerbaarheid, maar leidt op zichzelf niet automatisch tot structurele versterking van de securitypositie op de langere termijn. Hiervoor zijn doorgaans aanvullende verbeterprocessen nodig, zoals advies, consultancy en structurele optimalisatie. In de huidige aanbesteding missen wij expliciete eisen of ruimte voor een gezamenlijk partnership gericht op continue verbetering en groei in securityvolwassenheid gedurende de looptijd, bijvoorbeeld in de vorm van een volwassenheidstraject naast de SOC-dienstverlening. Is dit wenselijk voor opdrachtgever en kan de uitvraag hierop worden aangepast, zodat dergelijke aanvullende dienstverlening expliciet kan worden meegenomen in de inschrijving?	Om zorg te dragen dat de digitale weerbaarheid structureel en met name continue verbeterd wordt tijdens de gehele looptijd (max 10 jaar), en niet eenmalig door toepassen SOC. Aanvrager doet zich mogelijk te kort door hier geen eisen en uitleg over te vragen aan Inschrijvers.	Dit is geen onderdeel van deze aanbesteding en zal daarmee ook niet in deze opdracht worden opgenomen. Uiteraard is het belangrijk, maar dit valt niet onder de verantwoordelijkheid van Technisch Beheer en daarmee deze opdracht.
9	Uitnodiging tot inschrijving SIEM-SOC	7	1.3.1.2	Kunt u uitweiden wat u bedoelt (wat is in scope) voor : Incident Response (CERT): coördineren van respons bij beveiligingsincidenten, het uitvoeren van forensisch onderzoek, het adviseren over herstelmaatregelen, en delen kennis t.a.v. dreigingen. Deze staan nergens beschreven (niet op genomen in definitielijst) en daarom zijn deze verschillend te interpreteren.	Is dit additionel dienstverlenig naast het SOC?	Incident Response valt binnen de scope van deze opdracht. Aanbestedende dienst heeft eis 4.17 aangepast om meer helderheid te geven in de gevraagde dienstverlening rondom Incident Response: De opdrachtnemer levert een Incident Response (IR) retainer waarmee de opdrachtgever 24/7 directe toegang heeft (via een dedicated noodnummer, telefonisch) tot een team van cyberbeveiligingsexperts, met vooraf vastgestelde reactietijden en tarieven, teneinde schade te beperken en herstel te versnellen. De retainer biedt gegarandeerde beschikbaarheid bij incidenten, inclusief directe telefonische ondersteuning en een overeengekomen starttijd voor het onderzoek. De opdrachtnemer stelt gespecialiseerde expertise beschikbaar voor onder meer digitaal forensisch onderzoek, juridische ondersteuning en begeleiding bij communicatie met toezichthouders en verzekeraars. Daarnaast omvat de retainer proactieve voorbereidende diensten, zoals het helpen van de opdrachtnemer bij het opstellen of actualiseren van een Incident Response-plan, afgestemd op de organisatie van de opdrachtgever, en het verzorgen van trainingen (minimaal één IR-oefening of training per jaar voor relevante medewerkers), met als doel het beperken van financiële, reputatie- en juridische schade. De opdrachtnemer stelt gespecialiseerde expertise beschikbaar voor: 1) digitaal forensisch onderzoek (inclusief loganalyse, malware-onderzoek en vaststelling van de oorzaak en impact); 2) mitigatie- en herstelmaatregelen; 3) rapportage: de opdrachtgever ontvangt na afronding van een incident een schriftelijk incidentrapport, inclusief tijdlijn, bevindingen, genomen maatregelen en aanbevelingen.
10	Uitnodiging tot inschrijving SIEM-SOC/Bijlage 12 - Huidige situatie	7	Uitnodiging tot inschrijving SIEM-SOC 1.3.2./Bijlage 12 - Huidige situatie blz.1	In de uitnodiging tot inschrijving wordt gesproken over Defender for Server, terwijl in de beschrijving van de huidige situatie Palo Alto Cortex XDR wordt genoemd als Endpoint tool op de servers. Worden beide tools naast elkaar gebruikt of is het de bedoeling dat Defender for Server de plaats van Palo Alto Cortex XDR in gaat nemen. Kan hier duidelijkheid gegeven worden?		Zie antwoord op vraag 6.
11	Uitnodiging tot inschrijving SIEM-SOC	8	1.3.2	Hier wordt gesproken over "Advies en ondersteuning bij de inrichting, het beheer en de optimalisatie van technische beveiligingsoplossingen". Wat wordt hier precies bedoeld? Gaat dit over beheer en inrichting in relatie tot het (aanleveren van logging aan het) SIEM of het daadwerkelijk inrichten van de tooling zelf?		Het gaat om de daadwerkelijke inrichting van de tooling.
12	Uitnodiging tot inschrijving	8	1.3.3	Heeft de gemeente al ervaringen met SOC-dienstverlening of monitoring en wat zijn de eventuele lessons learned?	Een goed beeld van de Ist situatie draagt bij aan de inschatting van de werkzaamheden voor de onboarding.	Nee, de gemeente heeft hier geen ervaring mee.
13	Uitnodiging tot inschrijving SIEM-SOC	8	1.3.3	Kunt u bevestigen dat een aanbiedig met een prijs boven € 850.000 over een looptijd van 10 jaar, exclusief indexering, terzijde zal worden gelegd? Of geldt er in geheel geen plafond	Geldt er een fataal financieel plafond?	Voor implementatiekosten geldt een plafondbedrag van €50.0000. Voor exploitatiekosten is dit €850.000. Indien uw inschrijfprijs in één of beide onderdelen hoger is dan het plafodbedrag, dan leidt dit tot het terzijde leggen van de inschrijving.
14	Uitnodiging tot inschrijving SIEM-SOC	8	1.3.3	Welke SOC oplossing en/of van welke leverancier wordt er momenteel gebruikt (indien)	Aanbestedingswet, gelijkheids- en transparantiebeginsel	Er wordt nog geen soc dienstverlening gebruikt. Wel heeft aanbestedende dienst op dit moment Microsoft Sentinel. Bij uitvoering van de opdracht moet opdrachtnemer gebruik maken van deze omgeving.

15	Uitnodiging tot inschrijving	8	1.3.5 Doelstellingen	In paragraaf 1.3.5 wordt gesproken over het realiseren van een “samenhangende aanpak voor monitoring, detectie, incidentrespons en technische beveiligingsondersteuning“. a) Kunt u toelichten welke concrete onderdelen en werkzaamheden u bedoelt onder “samenhangende aanpak“, bijvoorbeeld welke onderdelen van de ICT-organisatie en welke processen hierbij betrokken zijn? b) Kunt u aangeven welke verwachtingen u heeft ten aanzien van de samenwerking tussen de verschillende onderdelen (zoals monitoring, detectie, incidentrespons en technische beveiligingsondersteuning) bij het realiseren van deze samenhangende aanpak?	Deze vraag zorgt voor helderheid over wat er precies wordt verwacht van een samenhangende aanpak en voorkomt dat er misverstanden ontstaan over de verwachtingen en de betrokken onderdelen.	Antwoord op a): "Met een 'samenhangende aanpak' doelt de opdrachtgever op een integrale keten waarin security-informatie niet op zichzelf staat, maar leidt tot gerichte actie. De concrete onderdelen en werkzaamheden omvatten: Monitoring & Detectie: Het continu analyseren van logdata uit de bronnen tegen actuele dreigingsbeelden. Incident Response: Een naadloze overgang van 'alert' naar 'actie', waarbij het SOC adviseert over de te nemen isolatie- en herstelmaatregelen. Technische Beveiligingsondersteuning: Het proactief adviseren over het verbeteren van de technische weerbaarheid (hardening), bijvoorbeeld door het fine-tunen van Microsoft Defender-instellingen op basis van waargenomen trends. De betrokken onderdelen binnen de gemeentelijke organisatie zijn de CISO (strategisch/tactisch), de Functionaris Gegevensbescherming/Privacy Officer (bij datalekken) en het team IT-beheer (operationele uitvoering van wijzigingen en herstelacties)." Antwoord op b): "De verwachting is dat de opdrachtnemer fungeert als de 'waakvlam' en de 'expert-adviseur'. Omdat de gemeente momenteel geen specifiek Incident Response Plan (IRP) voor de SOC-dienstverlening heeft, verwacht de opdrachtgever dat de opdrachtnemer tijdens de implementatiefase het voortouw neemt in het opstellen van dit plan en de bijbehorende playbooks/draaiboeken. Hierin moet de samenwerking als volgt worden geborgd: Het SOC is verantwoordelijk voor de initiële triage en het vaststellen van de ernst (impact/urgentie). Bij incidenten met een hoge prioriteit voert het SOC de regie op de technische analyse en geeft concrete instructies/adviezen aan het IT-beheerteam van de gemeente voor de inperking (containment). Er wordt een nauwe samenwerking verwacht waarbij periodiek de effectiviteit van de detectie wordt getoetst aan de veranderende ICT-infrastructuur van de gemeente.
16	Uitnodiging tot inschrijving SIEM-SOC	8	1.3.6	Het in de toekomst toevoegen van logbronnen (categorie A, B en C) of de groei vban data ingest per logbron zal binnen Microsoft Sentinel doorgaans leiden tot aanvullende kosten. Kunt u aangeven hoe deze toekomstige kosten moeten worden meegenomen bij het opstellen van een totaal TCO-overzicht?	Onduidelijhied over kosten TCO exrta logbronen of extra log ingest per logbron.	Zie het vernieuwde prijzenblad.
17	Uitnodiging tot inschrijving SIEM-SOC	8	1.3.6	Over het algemeen geldt een SROI niet regiogebonden. Iedereen in NL kan profijt hebben in de participatie, of moet er gebruik worden gemaakt van het regionale Expertisepunt Social Return (ESR) van het Werkbedrijf regio Zwolle?	Graag verduidlijking reikwijdte.	Of u de SROI-invulling doet met een leerling uit Dokkum of uit Roermond, dat is aan u. De woonplaats van uw medewerker die onder een SROI-doelgroep valt, is inderdaad niet van belang. De gastles over deze opdracht die u verzorgt bij een opleidingsinstituut mag in Steenwijkerland plaatsvinden, maar Harderwijk vindt de aanbestedende dienst ook goed. De SROI is in eerste instantie opdrachtgebonden. Uiteraard wordt het gewaardeerd wanneer u de sociaal-maatschappelijke meerwaarde in Steenwijkerland realiseert. De wijze van invulling (en de keuzes daarin) is aan u als opdrachtnemer. De bouwblokken zijn hier leidend in. Het ESR en de Werkgeversdienstverlening van de gemeente Steenwijkerland adviseren u hier kosteloos in. Zij helpen u ook op weg met het op te stellen Plan van Aanpak, de verantwoording, etc.
18	Uitnodiging tot inschrijving	10	1.9 Planning	In de planning wordt aangegeven dat het voornemen tot gunning op dinsdag 31 maart 2026 wordt bekendgemaakt. a) Kunt u bevestigen dat u ons op de hoogte zult brengen indien er wijzigingen in deze planning plaatsvinden, zodat we op tijd kunnen reageren op eventuele vertragingen of andere aanpassingen? b) Indien u niet van plan bent om inschrijvers te informeren bij wijzigingen in de planning, kunt u toelichten waarom dit niet is toegestaan, gezien het belang van transparantie en goede communicatie in de aanbestedingsprocedure?	Deze vraag zorgt voor helderheid over de communicatie bij wijzigingen in de planning en voorkomt dat je onterecht wordt benadeeld door een vertraging of aanpassing die niet wordt gecommuniceerd.	Indien de planning om welke reden dan ook aangepast moet worden, dan probeert de aanbestedende dienst dit tijdig te communiceren met geïnteresseerde partijen. Naar aanleiding van Nota van Inlichtingen 1 is de planning aangepast, waardoor de voorlopige gunning is gepland op vrijdag 8 mei 2026.
19	Uitnodiging tot inschrijving	11	1.10 Inlichtingen	Na het publiceren van de 1ste nota van inlichtingen biedt u de mogelijkheid om vragen te stellen over de 1ste nota van inlichtingen. Kunt u toelichten hoe de aanbestedende dienst omgaat met nieuwe vragen die inschrijvers stellen en hoe u ervoor zorgt dat de duidelijkheid en transparantie gewaarborgd blijven in de aanbestedingsprocedure?	Deze vraag zorgt voor helderheid over het omgaan met nieuwe vragen en voorkomt dat je onterecht wordt uitgesloten door een onduidelijke interpretatie van de documenten.	Elke ingediende vraag in de Nota van Inlichtingen 2 wordt beoordeeld door de aanbestedende dienst. Vragen die noodzakelijk zijn voor het vervolg van de aanbesteding worden beantwoord.
20	Uitnodiging tot inschrijving	11	1.10 Inlichtingen	In de tweede vragenronde biedt u inschrijvers de mogelijkheid om vragen te stellen over de 1ste nota van inlichtingen. Verzoeken wij u vriendelijk om ook nieuwe vragen te beantwoorden. Zo niet, kunt u dan uw motivatie geven waarom u geen nieuwe vragen toelaat, gezien het belang en de wens van partnerschap in de aanbestedingsprocedure?	Deze vraag zorgt voor helderheid over het beantwoorden van nieuwe vragen en voorkomt dat je onterecht wordt uitgesloten door een onduidelijke interpretatie van de documenten.	Zie antwoord op vraag 19.
21	Uitnodiging tot inschrijving SIEM-SOC	13	1.12.5	U verlangt een (rechtsgeldig ondertekende) aanbiedingsbrief. Kunt u aangeven of u specifieke verwachtingen heeft van / eisen stelt aan de inhoud van deze brief?	Voor de duidelijkheid. Hoewel een aanbiedingsbrief voor een inschrijver altijd een optie is, is het niet gebruikelijk dat een aanbiedingsbrief wordt vereist. Het belang van rechtsgeldige ondertekening wordt ook meestal benadrukt met betrekking tot de ondertekening van de UEA.	De eis van een aanbiedingsbrief komt te vervallen.
22	Uitnodiging tot inschrijving	16	Paragraaf 1.15	Kan deze alinea buiten komen te vervallen?	In het geval dat er een kort geding aanhangig is gemaakt stelt u dat de winnende inschrijver in kortgeding moet interveniëren. Dit lijkt een omissie te zijn. Immers, op grond van de Aanbestedingswet is een dergelijk geschil in beginsel tussen de gemeente als Aanbestedende dienst en de partij die het kort geding heeft ingesteld. Dit valt primair buiten de verantwoordelijkheid van de winnende inschrijver. Daarnaast heeft de winnende inschrijver niet alle informatie voorhanden om deugdelijk te kunnen interveniëren en is zij ook niet de partij die zich dient te verantwoorden.	Niet akkoord. De winnende inschrijver dient in de kort gedingprocedure te interveniëren, op straffe van verval van recht om – nadien – nog op te mogen komen tegen een eventueel gewijzigde gunningsbeslissing.
23	Uitnodiging tot inschrijving SIEM-SOC	16	1.15	Is er een mogelijkheid bij bezwaar van een gunning om eerst gehoord te worden voordat er direct een kort geding procedure dient te worden opgestart?	Mogelijk voorkomen van kort geding kosten	Niet akkoord. De afgewezen inschrijver heeft wanneer hij zich niet kan vinden in de gunningsbeslissing het recht om binnen 20 kalenderdagen na mededeling van de gunningsbeslissing een kort geding aanhangig te maken bij de bevoegde rechter.

24	Uitnodiging tot inschrijving	17	Paragraaf 1.16	Kan de gemeente de paragraaf op basis hiervan aanpassen?	Leverancier acht het redelijk dat in het geval deze situatie zich voortdoet er uitsluitend geen recht op schadevergoeding bestaat in het geval er in het geheel nog geen werkzaamheden door Leverancier zijn verricht, dan wel in het geval dat de ontbinding aan de inschrijving van Leverancier als winnende partij kan worden toegerekend. In het geval de gerechtelijke beslissing echter een gevolg is van handelen dat aan de gemeente kan worden verweten, en Inschrijver al werkzaamheden onder de overeenkomst heeft uitgevoerd, dan acht Inschrijver het wel redelijk dat zij recht heeft op schadevergoeding. Immers, in dat geval gaat het om een situatie waarop zij geen enkele invloed heeft gehad en welke situatie volledig in de risicosfeer van de gemeente ligt.	Niet akkoord. De opdrachtnemer heeft in beginsel geen recht op een schadevergoeding, indien uit een uitspraak van een rechter volgt dat de gunningsbeslissing of overeenkomst onrechtmatig is. Alleen in het geval dat de onrechtmatigheid toe te rekenen is aan de opdrachtgever, kan worden besloten de opdrachtnemer een schadevergoeding toe te kennen.
25	Uitnodiging tot inschrijving SIEM-SOC	20	2.1.2	Kunt u aangeven of een inschrijver terzijde wordt gelegd indien deze bewijsstukken niet binnen vijf dagen kunnen worden aangeleverd? Inplaats van het nu gestelde: kan de inschrijver worden uitgesloten van verdere deelname aan de aanbestedingsprocedure...	Geen onduidelijke juridische ruimte toelaten in het correct volgen van aanbestedingsprocedures.	Het uitgangspunt is dat het niet binnen vijf dagen aanleveren van de bewijsstukken leidt tot uitsluiting van verdere deelname aan de aanbestedingsprocedure. Echter, er kunnen zich onvoorziene omstandigheden voordoen waardoor het niet aanleveren van bewijsmiddelen binnen vijf dagen niet per direct leidt tot uitsluiting van verdere deelname.
26	Uitnodiging tot inschrijving SIEM-SOC		2.1.4	Klopt het dat er in deze aanbesteding alleen voor de verzekeringseis eventueel een beroep hoeft te worden gedaan op de economische- en financiele financiele van een derde?	Ter bevestiging van de eigen conclusie omdat er ondanks de bescheiden eis bepaalde nadruk wordt gelegd op de concernverklaring en of de 403-verklaring.+F27	Inschrijver beoordeelt zelf of hij een beroep moet doen op de draagkracht van een derde. U verwijst naar paragraaf 2.1.4. Indien u een beroep doet op de draagkracht van het concern om te voldoen aan een geschiktheidseis, geldt hetgeen is beschreven in paragraaf 2.1.4. Het kan gaan om economische en financiële draagkracht of om eisen met betrekking tot technische en beroepsbekwaamheid.

27	Uitnodiging tot inschrijving SIEM-SOC		2.1.5	Inschrijver is een met name genoemde Medeverzekerde op het verzekeringscertificaat dat de moedermaatschappij noemt als Verzekeringsnemer. Dit verzekeringscertificaat is het beoogd bewijsstuk om aan te tonen dat we voldoen aan de eis onder 2.1.5. Kwalificeert u dit als een situatie waarbij Inschrijver een beroep doet op de Economische en financiele draagkracht van de moedermaatschappij (als derde)?	Onze eerste aanname is dat geschetste situatie geen beroep op draagkracht inhoudt. Maar dat is een aanname. Zonder duidelijkheid van uw kant zouden we op dit punt een verkeerde inschrijving kunnen doen.	De geschetste situatie kwalificeert niet als een beroep op een derde om te voldoen aan één of meerdere eisen met betrekking tot economische en financiële draagkracht. Vereist is dat inschrijver aantoonbaar verzekerd is, en daaraan wordt voldaan indien inschrijver als meeverzekerde op het certificaat voorkomt.
28	leidraad	22	2.1.6.	In de uitvraag wordt verzocht om een referentie van een overheidsinstantie. Kunt u bevestigen dat een referentie uit een semi-overheidsorganisatie ook voldoet aan de referentie-eis?	We willen zekerheid over de interpretatie van de referentie-eis om uitsluiting te voorkomen. Semi-overheidsorganisaties zijn vaak gelijkwaardig qua governance en relevantie.	Zie antwoord op vraag 356.
29	Uitnodiging tot inschrijving	23	2.2 Gunningscriteria	In de aanbestedingsdocumenten staat dat het lettertype Arial en de lettergrootte minimaal 10 is voor de tekst in het plan van aanpak. a) Kunt u bevestigen dat afbeeldingen (zoals schema's, diagrammen of visuele planningen) mogen worden gebruikt met een ander lettertype of lettergrootte, zolang de inhoud leesbaar is en duidelijk blijft? b) Indien dit niet is toegestaan, kunt u toelichten waarom een ander lettertype of lettergrootte in afbeeldingen niet is toegestaan, gezien het belang van leesbaarheid en duidelijkheid van visuele elementen in het plan van aanpak?	Deze vraag zorgt voor helderheid over de toegestane variatie in lettertype en -grootte voor afbeeldingen, en voorkomt dat je onterecht wordt uitgesloten door een te strikte interpretatie van de regels.	Ja, dat bevestigen wij.
30	Uitnodiging tot inschrijving	24	2.2.1 Inschrijfprijs	In de leidraad wordt aangegeven dat een inschrijving boven het plafondbedrag "kan leiden tot het terzijde leggen van de inschrijving". a) Kunt u toelichten onder welke omstandigheden het overschrijden van het plafondbedrag leidt tot het terzijde leggen van de inschrijving en wanneer dit niet het geval is? b) Kunt u aangeven welke criteria of overwegingen u hanteert bij het besluit om een inschrijving boven het plafondbedrag al dan niet terzijde te leggen?	Wij stellen deze vraag om helderheid te krijgen over de gevolgen van het overschrijden van het plafondbedrag, zodat we onze inschrijving correct kunnen invullen en weten wat de gevolgen zijn voor onze kansen op gunning.	Dit is een omissie van de aanbestedende dienst. Indien een inschrijver een inschrijving indient boven een van de plafondbedragen, leidt dit tot terzijdelegging van de inschrijving. Dit houdt in dat bij overschrijding van het plafondbedrag de inschrijving in alle gevallen terzijde wordt gelegd. De aanbestedende dienst heeft hierbij geen keuzevrijheid.
31	Uitnodiging tot inschrijving SIEM-SOC	24	2.2.1	In de uitvraag wordt aangegeven dat voor de implementatiekosten een plafondbedrag van € 50.000,- exclusief btw geldt en dat voor de exploitatiekosten een plafondbedrag van € 850.000,- exclusief btw van toepassing is, waarbij wordt vermeld dat overschrijding kan leiden tot uitsluiting. Deze formulering is voor ons niet geheel eenduidig. Kunt u bevestigen of overschrijding van één of beide plafondbedragen daadwerkelijk leidt tot directe uitsluiting, of dat hier sprake is van beoordelingsruimte?	Onduidelijk juridisch kader tbv regels Aanbestedingswet.	Zie antwoord op vraag 30.
32	Uitnodiging tot inschrijving	25	2.2.2 Kwaliteitscriterium 1: Partnerschap	Kun je toelichten wat je verwacht onder "overdraagbaarheid en toekomstbestendigheid" van de oplossing, bijvoorbeeld of er een bepaalde documentatie of handover-procedure vereist is bij het overdragen van de dienstverlening aan een opvolgende leverancier?	Wij stellen deze vraag om helderheid te krijgen over wat er precies wordt verwacht onder 'overdraagbaarheid en toekomstbestendigheid', zodat we onze inschrijving correct kunnen invullen en er geen misverstanden ontstaan bij de beoordeling, conform het gelijkheids- en proportionaliteitsbeginsel.	Onder overdraagbaarheid verstaat de aanbestedende dienst dat de dienstverlening aan het einde van de looptijd zonder verlies van historisch inzicht of actueel detectievermogen kan worden voortgezet door de gemeente zelf of door een derde partij. Hiertoe wordt minimaal verwacht: Documentatie: Een actueel 'As-Built' dossier van de SIEM-inrichting, een register van alle actieve use cases (gebaseerd op het MITRE ATT&CK-framework) en bijbehorende logische schema's. Handover-procedure: Opdrachtnemer dient een beknopt exit-plan op te stellen waarin de overdracht van autorisaties, kennisoverdrachtsessies voor beheerders en de de-onboarding van eventuele eigen tooling van de opdrachtnemer zijn beschreven. Onder toekomstbestendigheid verstaat de opdrachtgever: De inzet van open standaarden en de volledige benutting van de roadmap-ontwikkelingen binnen het Microsoft Sentinel-ecosysteem. Een modulaire opzet van de dienstverlening, waardoor het toevoegen of wijzigen van logbronnen (cloud of on-premise) en het updaten van detectielogica eenvoudig en zonder architecturale wijzigingen mogelijk blijft. De bereidheid van de opdrachtnemer om tijdens de looptijd proactief te adviseren over nieuwe dreigingen en technologische verbeteringen in de markt. In lijn met de GIBIT 2023-voorwaarden wordt van de opdrachtnemer verwacht dat deze loyale medewerking verleent aan een soepele overdracht aan het einde van de overeenkomst.
33	Uitnodiging tot inschrijving	25	2.2.2 Kwaliteitscriterium 1: Partnerschap	In paragraaf 2.2.2 wordt aangegeven dat u als de opdrachtgever zich inspant om een goede opdrachtgever te zijn en verwacht ditzelfde partnerschap en professionaliteit van de opdrachtnemer. Kunt u toelichten welke concrete inspanningen u als opdrachtgever uitvoert om een "goede opdrachtgever" te zijn in deze opdrascht, bijvoorbeeld op het gebied van communicatie, beschikbaarheid, besluitvorming, of ondersteuning tijdens de uitvoering van de opdracht?	Wij stellen deze vraag om helderheid te krijgen over welke concrete maatregelen en inspanningen u als opdrachtgever neemt om een goede opdrachtgever te zijn, zodat we als opdrachtnemer onze verwachtingen en voorbereidingen hierop kunnen afstemmen en er geen misverstanden ontstaan over de samenwerking tijdens de uitvoering van de opdracht.	De gemeente Steenwijkerland erkent dat een effectieve SOC-dienstverlening een gedeelde verantwoordelijkheid is. Om een goede opdrachtgever te zijn, zet de gemeente de volgende concrete middelen en structuren in: Governance & Beschikbaarheid: De gemeente wijst een vast tactisch aanspreekpunt aan (TISO) voor de aansturing van de overeenkomst en periodiek overleg. Voor de dagelijkse operatie is het team IT-beheer gedurende kantoortijden beschikbaar voor technische ondersteuning en de uitvoering van wijzigingen. Incidentmanagement: Er wordt een escalatiematrix opgesteld waarin ook de bereikbaarheid van de gemeente buiten kantoortijden voor Prio-1-incidenten wordt vastgelegd. De gemeente spant zich in om binnen de in het Incident Response Plan (IRP) afgesproken termijnen besluiten te nemen over voorgestelde isolatiemaatregelen. Informatievoorziening: De gemeente draagt zorg voor de noodzakelijke autorisaties binnen de eigen Azure-tenant voor de opdrachtnemer en stelt documentatie over de relevante infrastructuur proactief ter beschikking. Partnerschap: De gemeente hanteert een transparante communicatiestijl en staat open voor proactief advies van de opdrachtnemer om de securitybaseline gezamenlijk naar een hoger plan te tillen. De gemeente verwacht van de opdrachtnemer dat deze in de implementatiefase aangeeft welke specifieke input of medewerking op welk moment cruciaal is, zodat de gemeente haar capaciteit hierop kan inplannen.
34	Uitnodiging tot inschrijving	25	2.2.2 Kwaliteitscriterium 1: Partnerschap (maximaal 35 punten)	U vraagt de inschrijver in (max. 4 A4) partnerschap te beschrijven. Dit onderdeel vormt een belangrijk onderdeel voor de dienstverlening (dit wordt ook bevestigd door uw weging op dit onderdeel). Onze ervaring is dat minimaal 7 A4 benodigd is om gedegen antwoord te kunnen geven op uw vragen. Bent u akkoord met het verhogen van het aantal A4 naar 6?	Dit geeft inschrijvers de mogelijkheid een onderscheidend antwoord te formuleren	Aanbestedende dienst is akkoord met het verhogen van het aantal pagina's voor kwaliteitscriterium 1 Partnereschap naar maximaal 6 A4.
35	Uitnodiging tot inschrijving	25	2.2.2 Kwaliteitscriterium Partnerschap	Kunt u toelichten hoe het gunningscriterium 'Partnerschap' concreet wordt beoordeeld? Welke concrete aspecten worden gewogen en wat onderscheidt een score "voldoende" (6 punten) van "goed" (8 punten)?		Zie paragraaf 2.2.5 voor de beoordelingscriteria voor Partnerschap. In deze paragraaf treft u eveneens een toelichting op het onderscheid tussen een voldoende (6) en een goed (8).

36	Uitnodiging tot Inschrijving	25	2.2.3	Bij onze klanten zien we dat de dienstverlening rondom forensisch onderzoek vaak door 3de partijen worden uitgevoerd om zo objectief mogelijk onderzoek te kunnen doen. Onze vraag is of de gemeente mee kan in deze best practice, en het forensisch onderzoek zelf buiten scope van de uitvraag ziet.		De aanbestedende dienst maakt een onderscheid tussen de operationele incidentrespons en diepgaand forensisch onderzoek: Incident Response: De opdrachtnemer is volledig verantwoordelijk voor de technische incidentrespons (containment en recovery) om directe schade te beperken. Hierbij wordt nauw samengewerkt met de TISO van de gemeente. De gemeente Steenwijkerland zal bij significante incidenten tevens de IBD (Informatiebeveiligingsdienst) inschakelen voor een adviserende en coördinerende rol op landelijk niveau. Van de opdrachtnemer wordt verwacht dat deze de technische bevindingen proactief deelt met de TISO ten behoeve van de afstemming met de IBD. Forensisch onderzoek: Indien na een incident diepgaand forensisch onderzoek noodzakelijk is (bijv. voor bewijsvoering in een juridisch traject), erkent de opdrachtgever dat dit als specialistische dienst buiten de primaire scope van de vaste exploitatiekosten kan vallen. De opdrachtnemer heeft hierin echter een cruciale faciliterende rol: Het borgen van de integriteit van logdata (chain of custody) conform BIO-richtlijnen. Het onverwijld verlenen van technische medewerking aan een eventuele derde partij of de IBD door het beschikbaar stellen van data en analyses. De opdrachtgever behoudt zich het recht voor om te allen tijde een onafhankelijke derde partij of de IBD te consulteren voor een second opinion of forensisch onderzoek.
37	Uitnodiging tot inschrijving SIEM-SOC	25	2.2.3	Kwaliteitscriterium 2. Sprake van leveren van incident response. Definitie IR (verwachting) en kader scope ontbreekt. Wat moet er geleverd worden bij een incident? Bijvoorbeeld onsite ondersteuning, Incident Response plan? IR portal voor de IR project plan en planning bij onberiekbaarheid omgeving door het incident etc.?	Gaarne verduidelijking of er een volledige IR gervaagd wordt als onderdeel.	Zie antwoord op vraag 9 voor een verduidelijking van Incident Response (IR). De aanbestedende dienst nodigt inschrijvers uit om in hun uitwerking van Kwaliteitscriterium 2 specifiek in te gaan op de wijze waarop zij de regie voeren en welke tooling zij inzetten om de communicatie tijdens een kritiek incident te waarborgen.
38	Uitnodiging tot inschrijving SIEM-SOC	25	2.2.3	Kunt u een uitsluitende opsomming geven met alle beveiligingsmaatregelen en oplossingen die momentneel aanwezig/gebruikt worden om te voldoen aan het aspect: integratie met bestaande beveiligingsmaatregelen?	Er bestaat onduidelijkheid over de huidige, reeds aanwezige beveiligingsmaatregelen. Dit kan leiden tot een ongelijk speelveld binnen de aanbesteding, aangezien sommige inschrijvers mogelijk meer inzicht hebben in de bestaande beveiligingsmaatregelen dan anderen. Kunt u toelichten welke beveiligingsmaatregelen momenteel zijn ingericht, zodat alle inschrijvers over dezelfde uitgangspositie beschikken?	De aanbestedende dienst is zich bewust van het belang van een gelijk speelveld, maar stelt de veiligheid van de gemeentelijke infrastructuur voorop. Een gedetailleerd overzicht van de specifieke beveiligingsmaatregelen, versies en configuraties wordt beschouwd als vertrouwelijk. Conform de procedure beschreven in de aanbestedingsstukken is de gedetailleerde informatie over de huidige technische situatie (Bijlage 12) uitsluitend beschikbaar voor geïnteresseerde partijen. Zie ook het antwoord op vraag 316. Inschrijvers die deze verklaring hebben ingediend, beschikken hiermee over de volledige en uitsluitende lijst van beveiligingsoplossingen (waaronder Identity Management, Endpoint Protection, firewalling en vulnerability management) die noodzakelijk is voor een kwalitatief goede inschrijving. De aanbestedende dienst verwijst voor de inhoudelijke details naar dit beveiligde document.
39	Uitnodiging tot inschrijving SIEM-SOC	26	2.2.3	Is het aanbieden van een Incident Response Retainer (IR) een verplicht onderdeel van de uitvraag? Kunt u de verwachte scope van deze IR-retainer toelichten en aangeven of dit een integraal onderdeel is van de SIEM/SOC-dienstverlening of een separaat te prijzen component? Daarnaast ontvangen wij graag verduidelijking over de wijze van aanbieden: wordt een all-in jaarprijs verwacht, een prijs per uur, per incident, fair use / maximum inzet, of een andere prijsstructuur?	Onduidelijk of en hoe IR in de aanbieding moet komen te staan.	De aanbestedende dienst verwacht geen separate 'Incident Response Retainer' in de vorm van een beschikbaarheidsvergoeding (stand-by fee). De verwachtingen ten aanzien van Incident Response zijn als volgt verdeeld: Integraal onderdeel (vaste prijs): De initiële respons, triage, technische analyse en het adviseren over inperkingsmaatregelen (containment) maken integraal onderdeel uit van de SIEM/SOC-dienstverlening. Hiervoor wordt een all-in maandprijs verwacht binnen de exploitatiekosten. Aanvullende IR-ondersteuning (separaat): Voor grootschalige ondersteuning bij de afhandeling van complexe incidenten die de reguliere scope overstijgen, dient de opdrachtnemer in de prijstabel (Bijlage 3) uurtarieven op te geven voor relevante rollen (zoals IR-specialist, forensisch analist). Prijsstructuur: Er wordt dus gewerkt op basis van 'nacalculatie tegen vooraf vastgestelde uurtarieven' voor de inzet die buiten de reguliere monitoring en initiële respons valt. Een 'all-in jaarprijs' voor onbeperkte IR is niet vereist, tenzij de inschrijver dit als onderdeel van een 'fair use'-policy binnen hun standaarddienstverlening aanbiedt. De opdrachtgever verwacht dat de opdrachtnemer in de SLA vastlegt binnen welke termijnen zij deze specialistische IR-capaciteit kan garanderen na escalatie van een incident.
40	Uitnodiging tot inschrijving	26	2.2.4 Kwaliteitscriterium 3: Implementatie	U vraagt de inschrijver in (max. 6 A4) een plan van aanpak te beschrijven. Onze ervaring is dat minimaal 7 A4 benodigd is om gedegen antwoord te kunnen geven op uw vragen. Bent u akkoord met het verhogen van het aantal A4 naar 7?	Dit geeft inschrijvers de mogelijkheid een onderscheidend antwoord te formuleren	Zie antwoord op vraag 34.
41	Uitnodiging tot inschrijving	26	2.2.4 Kwaliteitscriterium 3: Implementatie	In paragraaf 2.2.4 "Kwaliteitscriterium 3: Implementatie" is bepaald dat het plan van aanpak maximaal 6 A4 mag beslaan. Voor de leesbaarheid en duidelijkheid van onze planning en fasering zouden wij graag een visuele planning (bijvoorbeeld in de vorm van een tijdlijn of Gantt-chart) als aparte bijlage op A3-formaat willen toevoegen. Deze bijlage zou uitsluitend de planning visualiseren en geen aanvullende inhoud bevatten ten opzichte van het plan van aanpak op de 6 A4. a) Kunt u bevestigen dat het is toegestaan om, naast het plan van aanpak van maximaal 6 A4, één extra bijlage op A3-formaat met een visuele planning (tijdlijn/Gantt-chart) mee te sturen, die uitsluitend ondersteunend is aan de toelichting in het plan van aanpak? b) Indien dit niet is toegestaan, verzoeken wij u kort toe te lichten waarom een dergelijke visualisatie niet is toegestaan, gezien het belang dat u hecht aan een heldere fasering, mijlpalen en samenwerking tijdens de implementatie.	Wij stellen deze vraag om de leesbaarheid en duidelijkheid van onze planning te waarborgen, en om te voorkomen dat we worden benadeeld door een te strikte interpretatie van de paginalimiet, terwijl een visuele bijlage juist bijdraagt aan het belang dat u hecht aan een heldere fasering en samenwerking.	Ja, hier gaat de aanbestedende dienst mee akkoord.
42	Uitnodiging tot inschrijving	26	Paragraaf 2.2.5	Welke rollen / personen zitten in de beoordelingscommissie?		Er zitten vier medewerkers vanuit Gemeente Steenwijkerland in de beoordelingscommissie. Deze medewerkers hebben de volgende functies: ontwikkelaar, systeembeheerder en securityspecialist.
43	Uitnodiging tot inschrijving	26	2.2.5 Beoordeling onderdeel kwaliteit	Kun je toelichten uit hoeveel leden de beoordelingscommissie bestaat en welke functies deze leden vervullen?	Wij stellen deze vraag om transparantie en gelijkheid te waarborgen bij de beoordeling, en om te voorkomen dat we worden benadeeld door onduidelijkheid over de samenstelling en deskundigheid van de beoordelingscommissie.	Er zitten vier medewerkers vanuit Gemeente Steenwijkerland in de beoordelingscommissie. Deze medewerkers hebben de volgende functies: ontwikkelaar, systeembeheerder en securityspecialist.

44	Uitnodiging tot inschrijving	26	2.2.5 Beoordeling onderdeel kwaliteit	Kun je toelichten op basis waarvan blijkt dat de leden van de beoordelingscommissie voldoende ervaring en materiedeskundigheid bezitten voor het beoordelen van de inschrijvingen in deze aanbesteding?	Wij stellen deze vraag om te waarborgen dat de beoordeling objectief en op basis van relevante expertise plaatsvindt, en om te voorkomen dat we worden benadeeld door een commissie die niet voldoende deskundig is.	De beoordelingscommissie werkt op de afdeling Technisch Beheer en beschikt over technische kennis van systemen en security. Daarmee hebben zij voldoende materiedeskundigheid om de inschrijvingen voor deze aanbesteding te beoordelen.
45	Uitnodiging tot inschrijving	26	2.2.5 Beoordeling onderdeel kwaliteit	In de aanbestedingsdocumenten wordt niet duidelijk gemaakt of er externen (bijvoorbeeld externe adviseurs, consultants of derden) betrokken zijn bij het beoordelen van inschrijvingen of bij het opstellen van het programma van eisen. a) Kunt u bevestigen dat uitsluitend medewerkers in dienst van de aanbestedende dienst betrokken zijn bij deze aanbesteding, inclusief het beoordelen van inschrijvingen en het opstellen van het programma van eisen? b) Indien externe partijen alsnog worden betrokken, kunt u toelichten op basis waarvan blijkt dat hun belangen transparant zijn en dat er geen belangenverstrengeling optreedt?	Wij stellen deze vraag om transparantie en integriteit te waarborgen in de aanbestedingsprocedure, en om te voorkomen dat we worden benadeeld door een onduidelijke of niet-objectieve beoordeling, conform het gelijkheidsbeginsel en de aanbestedingswetgeving.	Externe adviseurs ondersteunen deze aanbesteding procesmatig (o.a. planning, documentbeheer, procedurele advisering en coördinatie). Het inhoudelijk programma van eisen is vastgesteld door de aanbestedende dienst. De beoordeling van kwaliteitscriterium 1, 2 en 3 van de inschrijvingen wordt uitsluitend uitgevoerd door medewerkers van de aanbestedende dienst. Externe adviseurs nemen geen deel aan de beoordelingscommissie, hebben geen stemrecht en bepalen geen scores. Wel begeleiden externe adviseurs het beoordelingsproces.
46	Uitnodiging tot inschrijving SIEM-SOC	27	2.2.5	Indien een inschrijver meer functionaliteit of aanvullende dienstverlening kan aanbieden dan expliciet is uitgevraagd in het PvE, op welke wijze kan dit worden meegenomen in de beoordeling? Kunnen hiermee extra punten worden behaald, of worden uitsluitend de expliciet benoemde eisen en criteria beoordeeld, ongeacht aanvullende dienstverlening die aansluit op de doelstellingen?	Mogelijk extra beoordelingspunten bij mogelijke extra functionaliteit en kwaliteit tbv publieke gelden.	Inschrijvers worden beoordeeld op hetgeen is uitgevraagd en is opgenomen in het document Uitnodiging tot inschrijving en bijlagen. Niet-uitgevraagde extra functionaliteit of aanvullende dienstverlening wordt niet apart gescoord en kan geen extra punten opleveren.
47	Uitnodiging tot inschrijving	27	2.2.5 Beoordeling onderdeel kwaliteit	Op pagina 27 van de uitnodiging tot inschrijving wordt het beoordelingskader beschreven, waarbij het verschil tussen "goed" (8 punten) en "uitstekend" (10 punten) wordt gemaakt op basis van de mate waarin de aanpak volledig of goed aansluit bij de doelstelling en het criterium. a) Kunt u toelichten wat precies het verschil is tussen een beantwoording die "goed aansluit" en een beantwoording die "volledig aansluit", bijvoorbeeld aan de hand van concrete kenmerken of criteria? b) Kunt u een voorbeeld geven van een beantwoording die als "uitstekend" zou worden beoordeeld, zodat inschrijvers duidelijk weten wat er precies van hen verwacht wordt om het maximum aantal punten te behalen?	Wij stellen deze vraag om helderheid en gelijkheid te waarborgen bij de beoordeling, en om te voorkomen dat we worden benadeeld door een onduidelijke of subjectieve interpretatie van het beoordelingskader.	a) Een beantwoording die “goed” (8 punten) kenmerkt zich doordat: - alle gevraagde onderdelen van het betreffende subgunningscriterium zijn behandeld; - de aanpak duidelijk, logisch en realistisch is; - de voorgestelde werkwijze in algemene zin aansluit bij de doelstellingen van de aanbestedende dienst en het criterium; - de beantwoording concreet is, maar op onderdelen nog ruimte laat voor nadere invulling, aannames of toelichting; - de inschrijving nauwelijks vragen oproept, maar niet alle aspecten volledig is uitgewerkt. Een beantwoording die “uitstekend” (10 punten) kenmerkt zich doordat: - alle relevante aspecten van het subgunningscriterium volledig, integraal en samenhangend zijn uitgewerkt; - de aanpak specifiek is toegesneden op de doelstellingen en context van de opdracht; - de beantwoording concreet, realistisch en SMART is (specifiek, meetbaar, acceptabel, realistisch en tijdsgebonden); - verantwoordelijkheden, processen, borging en samenhang expliciet zijn beschreven; - de aanpak geen openstaande vragen of interpretatieruimte laat bij de beoordelingscommissie. b) De aanbestedende dienst kan hiervan geen voorbeeld geven. Dit is aan de inschrijver.
48	Bijlage 2	1	Kerncompetentie 3	Contactpersoon en telefoonnummer en tevredenhiedsverklaring graag pas na (voorlopige) gunning delen ter verificatie.	Dit ter onnodige voorkoming van administratie en het beleg leggen op tijd en inspanningen van huidige klanten. Door de vele refentie aanvragen wordt dit als onnodige storend ervaren. We behoeden graag onze klanten hiertegen. Dank voor het begrip.	Nee, wij gaan hier niet mee akkoord. Het is voor aanbestedende dienst van belang dat de implementatie van de oplossing en uitvoering van dienstverlening naar tevredenheid is uitgevoerd. Een tevredenheidsverklaring is hierin belangrijk. De aanbestedende dienst is van mening dat de tevredenheidsverklaring niet leidt tot een disproportionele verhoging van de administratieve lasten.
49	Bijlage 3 Prijsinvulformulier			Voor het aansluiten van nieuwe logbronnen kan een eenmalig bedrag worden opgegeven. Waar kan leverancier de benodigde additionele uren voor analyse (per categorie) door het SOC kwijt op het prijzeninvulformulier?		Er is een nieuw prijzenblad toegevoegd. In het prijzenblad dient inschrijver onderscheid te maken in categorie A-, B- of C-logbronnen die later aangesloten kunnen worden. Per soort logbron dient inschrijver eenmalige implementatiekosten en exploitatiekosten per maand op te geven. Eventuele additionele uren voor analyse zijn verdisconteerd in de eenmalige implementatiekosten of exploitatiekosten.
50	Bijlage 3 Prijsinvulformulier	1	1	Wij hanteren aanvullende kosten per use case, waarbij de hoogte afhankelijk is van het aantal use cases. Kunt u aangeven op welke plaats in het prijsformulier deze kosten kunnen worden opgenomen?	Geen plek voor extra usecases.	Zie eis 3.1 van het programma van eisen. Use cases voor het SIEM dienen standaard meegeleverd en onderhouden te worden door de opdrachtnemer, zonder extra kosten voor het gebruik van de betreffende use cases.
51	Bijlage 3 Prijsinvulformulier	1	1	Wij hanteren één all-in prijs voor zowel de SIEM-dienstverlening als de SOC-dienstverlening. Kunt u aangeven of het is toegestaan om in dat geval één van beide regels in het prijsformulier leeg te laten?	Waar in te vullen?	Er is een nieuw prijzenblad toegevoegd. Inschrijver dient alle geel gearceerde cellen in te vullen. Het nieuwe prijzenblad maakt bij exploitatiekosten geen onderscheid in SIEM- en SOC-diensten. Inschrijver dient een eenheidsprijs (exploitatiekosten) per asset in te dienen waarin SIEM- en SOC-dienstverlening verdisconteerd is.
52	Bijlage 3 Prijsinvulformulier			Voor het aansluiten van een nieuwe logbron is een plafondbedrag van Eur 1.000 opgenomen. Voor categorie C is dit plafond niet realistisch. Leverancier gaat er vanuit dat voor Categorie C het plafondbedrag niet van toepassing is. Derhalve het verzoek van leverancier om dit onderdeel in het prijsinvulformulier niet in te vullen. Gaat gemeente hiermee akkoord?	Dit betreft maatwerk en is volledig afhankelijk van de complexiteit van de logbron. De kosten zullen hoger zijn dan Eur 1.000. Prijs zal op basis van de scope worden bepaald.	Er is een nieuw prijzenblad toegevoegd. Inschrijver dient alle geel gearceerde cellen in te vullen. Aanbestedende dienst acht het prijsplafond voor categorie C realistisch. Het prijsplafond voor koppeling van categorie C blijft gehandhaafd.
53	Bijlage 3 Prijsinvulformulier			Het prijzenblad is vrij summier van opzet. Staat gemeente toe dat leverancier een prijsonderbouwing meestuurt met de beantwoording van de uitvraag?	Hierdoor krijgt de gemeente een helder inzicht in de afzonderlijke prijsopbouw van de aangeboden dienstverlening wat bijdraagt aan meer transparantie.	Nee, dat staat de aanbestedende dienst niet toe. Er is een nieuw prijzenblad toegevoegd.
54	Bijlage 3 Prijsinvulformulier	1	1	Cellen uit het Excel Bijlage 3 - prijzeninvulformulier F10, F11, F12 lijken niet mee genomen te worden in de berekening van de totale TCO van de aanbieding (Cell: G17)	Fout in Ecel sheet.	Zie antwoord op vraag 83. Er is een nieuw prijzenblad toegevoegd.
55	Bijlage 3 Prijsinvulformulier	1	1	Het prijsinvulformulier onderscheidt drie categorieën logbronnen (A, B, C) met maximumprijs €1.000 per logbron. Kunt u een definitie/omschrijving geven van wat onder categorie A, B en C wordt verstaan (bijvoorbeeld op basis van complexiteit, datavolume, of type bron)?		Dit is gespecificeerd in tabblad 'Toelichting' van het nieuwe prijzenblad. Zie antwoord op vraag 83.
56	Bijlage 3 - Prijsinvulformulier	1	Prijsonderdeel 2 Exploitatiekosten	In bijlage 3 – Prijsinvulformulier wordt onderscheid gemaakt tussen 'levering SIEM-dienstverlening' en 'levering 24/7 SOC-dienstverlening'. Kan de Aanbestedende Dienst toelichten waarom dit onderscheid is gemaakt?	Om duidelijkheid te verkrijgen over de prijsopbouw en een correcte invulling van het prijsformulier te waarborgen.	Er is een nieuw prijzenblad toegevoegd waarin dit onderscheid niet meer is gemaakt.

57	Bijlage 3		Prijs per logbron	U heeft 3 categorieen opgegeven als logbron (rij 10, 11 en 12). Kunt u aangeven wanneeer u hier gebruik van gaat maken? En zijn dit de eenmalige kosten voor het aansluiten?		Ten aanzien van de logbronnen in categorie 10, 11 en 12 geldt de volgende toelichting: Timing van aansluiting: De opdrachtgever verwacht dat de kritieke bronnen (zoals benoemd in de implementatiefase van het PvE) binnen de eerste 3 maanden operationeel zijn. De overige categorieën dienen uiterlijk binnen 6 maanden na gunning volledig ontsloten en gemonitord te worden. De exacte volgorde van aansluiting wordt in overleg met de TISO vastgelegd in het implementatieplan. Kostenonderbouwing: De kosten voor deze categorieën in de prijstabel dienen als volgt te worden opgegeven: De eenmalige kosten voor de technische inrichting, configuratie en validatie van de koppeling (onboarding). De maandelijkse exploitatiekosten voor het monitoren, triageren en beheren van de alerts voortvloeiend uit deze bronnen dienen te zijn inbegrepen in de vaste maandprijs voor de SOC-dienstverlening. Inschrijvers dienen er rekening mee te houden dat de aanbestedende dienst een volledige dekking van de benoemde bronnen wil om de gewenste integrale monitoring te kunnen realiseren.
58	Bijlage 3		Exploitatiekosten	Bij een toename van logbronnen nemen ook de exploitatiekosten toe. Wij kunnen dit nu niet kwijt in het prijzenblad. Hoe wenst de gemeente hier mee om te gaan?		Dit is opgenomen in het nieuwe prijzenblad. Zie antwoord op vraag 83.
59	Bijlage 3		Implementatie	Kunt u aangeven of alle logbronnen in de huidige oplossing al zijn aangesloten? Zo nee, welke ontbreken dan nog?		Voor april willen we alle servers over hebben naar Defender for Server. Andere logbronnen zijn nog niet aangesloten op onze Sentinel-omgeving.
60	Bijlage 3 - Prijsinvulformulier		Implementatiekosten	Hoe wordt omgegaan met additionele kosten voor complexe logbronnen die substantieel meer inspanning vereisen?		Aanbestedende dienst heeft in de aanbestedingsstukken een zo volledig mogelijk beeld geschetst van de huidige infrastructuur en de aan te sluiten bronnen. De aanbestedende dienst verwacht van potentiële opdrachtnemers dat zij op basis van deze informatie een integrale aanbieding doen, inclusief de benodigde inspanning voor de koppeling van de genoemde bronnen. Bestaande scope: Voor de in de uitvraag benoemde bronnen worden geen additionele kosten geaccepteerd buiten de opgegeven eenmalige implementatiekosten en de vaste maandelijkse exploitatiekosten. Het risico voor de complexiteit van de koppeling van deze bronnen ligt bij de opdrachtnemer. Nieuwe bronnen: Indien de gemeente Steenwijkerland gedurende de looptijd van de overeenkomst besluit om nieuwe, thans niet voorziene bronnen toe te voegen die buiten categorie A, B of C vallen, zal dit via de overeengekomen wijzigingsprocedure (Change Management) worden afgehandeld. Dit gebeurt enkel na akkoord van opdrachtgever. Hiervoor kunnen de in de prijstabel opgenomen uurtarieven voor incident response worden gehanteerd.
61	Bijlage 3		Exploitatiekosten	Bij een toename of afname van het aantal devices of servers heeft dit ook gevolgen voor de exploitatiekosten. Wij kunnen dit nu niet kwijt in het prijzenblad. Hoe wenst de gemeente hiermee om te gaan?		Dit is opgenomen in het nieuwe prijzenblad. Zie antwoord op vraag 83.
62	PvE	alle	alle	Wordt volledige Microsoft 365 E5-telemetrie verwacht binnen Sentinel?	Dit geeft inzicht in scope en datavolume. Het bepaalt of extra configuratie nodig is voor compliance en of er performance- en kostenimplicaties zijn.	Ja, dat bevestigd aanbestedende dienst.
63	PvE	alle	alle	Heeft het SOC mandaat tot actieve respons bij P1-incidenten?	Het mandaat beinvloedt de inrichting van processen en tooling. Actieve respons vereist specifieke playbooks, autorisaties en mogelijk integratie met endpoint- of netwerkcontrols.	Ja, dat bevestigd aanbestedende dienst.
64	PvE	alle	alle	Zijn de genoemde retentietermijnen leidend voor alle logdata?	Retentie heeft directe impact op storage-architectuur, kosten en compliance. We moeten weten of afwijkingen per bron mogelijk zijn of dat uniforme termijnen gelden.	De aanbestedende dienst heeft in het document Detailinformatie bijlage 12 (zie antwoord op vraag 316) een gedetailleerd overzicht gegeven van de aanwezige infrastructuur en de aan te sluiten bronnen. Deze bijlage is uitsluitend beschikbaar voor inschrijvers en kan worden opgevraagd via TenderNed (berichtenmodule). Opdrachtnemer verklaart dat het verstrekte document uitsluitend zal worden gebruikt ten behoeve van het voorbereiden en indienen van een inschrijving in het kader van deze aanbesteding. Opdrachtnemer zal het document niet aan derden verstrekken, noch geheel of gedeeltelijk kopiëren of anderszins gebruiken voor andere doeleinden. Na afronding van de aanbestedingsprocedure, ongeacht de uitkomst daarvan, zal opdrachtnemer het document onverwijld vernietigen. De aanbestedende dienst verwacht van de potentiële opdrachtnemer dat zij op basis van de informatie in deze vertrouwelijke bijlage een integrale aanbieding doet, inclusief de benodigde inspanning voor de koppeling van de daarin genoemde bronnen: Bestaande scope: Voor de in de uitvraag benoemde bronnen worden geen additionele kosten geaccepteerd buiten de opgegeven eenmalige implementatiekosten en de vaste maandelijkse exploitatiekosten. De inschrijver wordt geacht de complexiteit van deze koppelingen te hebben ingeschat op basis van de verstrekte vertrouwelijke informatie. Nieuwe bronnen: Indien de gemeente gedurende de looptijd van de overeenkomst besluit om nieuwe bronnen toe te voegen die op dit moment nog niet aanwezig zijn of niet zijn vermeld, zal dit via de overeengekomen wijzigingsprocedure (Change Management) worden afgehandeld, waarbij de prijzen voor het koppelen van categorie A-, B- en C-bronnen worden gehandhaafd.
65	PvE	alle	alle	Is gebruik van AI toegestaan uitsluitend voor analyse en triage?	Dit bepaalt of we geavanceerde AI-modellen kunnen inzetten voor detectie en prioritering. Het beinvloedt innovatie en de mate van automatisering binnen het SOC.	Ja, dit is toegestaan.
66	PvE	alle	alle	Moet volledige overdraagbaarheid van use-cases en configuraties worden gegarandeerd?	Dit raakt aan exit-strategie en vendor lock-in. We willen weten of configuraties exporteerbaar moeten zijn om continuiteit bij contractwissel te waarborgen.	Ja, dat moet worden gegarandeerd.
67	PVE	alle	alle	Zijn er aanvullende compliance-eisen boven BIO2/NIS2?	Extra eisen (bijv. AVG, sector-specifiek) beinvloeden architectuur, logging en rapportage. Dit is essentieel om non-compliance risico's te vermijden.	Ook dient de opdracht te worden uitgevoerd met inachtneming van de AVG-wetgeving.
68	PvE	alle	alle	Is de huidige technische situatie leidend en dient deze intact te blijven? (producten)	Dit bepaalt of er ruimte is voor optimalisatie of vervanging van bestaande componenten. Het beinvloedt ontwerpkeuzes, integratiecomplexiteit en kostenraming.	Ja, de huidige technische situatie dient intact te blijven, wel mogelijk tot uitbreiding binnen Sentinel/Defender.

69	Bijlage 5 Programma van eisen	1	Pve eerste rij	In kolom B van het Programma van Eisen staan de eisen geformuleerd ten aanzien van de oplossing waarmee de inschrijver de opdracht invult. Kunt u toelichten of deze eisen als uitvoeringseisen moeten worden gezien en of het dus om eisen gaat die tijdens de uitvoering van de opdracht moeten worden nageleefd, of dat het om eisen gaat die alleen bij inschrijving moeten worden aangetoond?	Deze vraag zorgt voor helderheid over het karakter van de eisen en voorkomt dat je onterecht wordt uitgesloten door een onduidelijke interpretatie van de documenten.	In het programma van eisen staan eisen met betrekking tot de uitvoering van de opdracht. Het gaat om eisen die tijdens de uitvoering van de opdracht moeten worden nageleefd. Bij inschrijving bevestigt de inschrijvende partij dat hij vanaf de start van de overeenkomst voldoet aan het programma van eisen.
70	Bijlage 5 Programma van Eisen	Algemeen	2.1	Kunt u bevestigen (als Knock Out eis) dat de volgende logbronnen aangesloten en verwerkt moeten worden binnen de SIEM/SOC-dienstverlening:	Graag verduidelijking omdat niet elka Inschrijver elk onderdeel goed kan aansluiten.	We hebben de bedrijfsgevoelige informatie uit uw vraag gefilterd. Zie antwoord op vraag 316. Opdrachtnemer dient te voldoen aan eis 2.1 waarin staat opgenomen dat de SIEM oplossing een minimaal aantal typen logbronnen of aansluiten ondersteunt.
71	Programma van Eisen (Bijlage 5)	1-2	2.1 - 3.13	Hoe definieert opdrachtgever precies een “logbron” voor het prijzenblad: per asset, per connector, per dienst (bijv. Microsoft 365/Defender) of per cluster (bijv. firewall active/passive)?	Om interpretatieverschillen te voorkomen en prijsvergelijking mogelijk te maken.	Ten behoeve van de eenduidige invulling van het prijzenblad hanteert de aanbestedende dienst de volgende definitie van een 'logbron': Per logische dienst/platform: Een samenhangende set aan data die via één centrale koppeling of connector wordt ontsloten. Voorbeeld: De volledige Microsoft 365/Defender-suite (inclusief alle onderliggende Defender-producten) wordt beschouwd als één logbron. Per cluster/opstelling: Een redundante opstelling (bijv. een active-passive firewallcluster) wordt beschouwd als één logbron, aangezien deze een integrale set aan beveiligingslogs genereert voor hetzelfde netwerksegment. Serverinfrastructuur: Voor de monitoring van servers wordt uitgegaan van de ontsluiting via de centrale Microsoft Sentinel-agent/connector. De inschrijver dient hierbij uit te gaan van de in Detailinformatie bijlage 12 (zie antwoord op vraag 316) genoemde aantallen servers als één collectieve bronomgeving, tenzij er voor specifieke applicatielogging separate connectoren noodzakelijk zijn. De aanbestedende dienst vraagt inschrijvers om in hun prijsstelling uit te gaan van de functionele scope in het prijzenblad en Detailinformatie bijlage 12. Indien een inschrijver afwijkt van deze logische groepering, dient dit expliciet en gemotiveerd te worden vermeld.
72	Bijlage 5 Programma van Eisen	Algemeen	3.1	Moet er ondersteuning geboden worden met kant en klare compliance-rapportage conform ISO 27001, NIST en CIS.	Handig en toegevoegde waarde maar is het een eis? Zonet dan ook niet relevant	Het leveren van rapportages over compliance is een eis, waarbij de focus ligt op de Nederlandse context: BIO als uitgangspunt: De primaire rapportageverplichting is gebaseerd op de BIO (Baseline Informatiebeveiliging Overheid). De opdrachtnemer dient periodiek (bijv. maandelijks/kwartaal) rapportages te leveren die inzicht geven in de effectiviteit van de technische beheersmaatregelen die binnen de scope van het SIEM/SOC vallen. ENSIA-ondersteuning: De rapportages moeten de TISO en CISO ondersteunen bij de jaarlijkse ENSIA-verantwoording. Dit betekent dat data over incidenten, kwetsbaarheden en logging-integriteit herleidbaar moet zijn naar de relevante BIO-controls. Aanvullende standaarden: Hoewel rapportages conform NIST of CIS als waardevolle aanvulling worden gezien voor technisch beheer, zijn deze ondergeschikt aan de BIO-rapportage. De aanbestedende dienst verwacht dat de opdrachtnemer in het plan van aanpak toelicht welke standaardrapportages beschikbaar zijn en hoe deze specifiek worden gemapt op de BIO-beheersmaatregelen.
73	Programma van Eisen (Bijlage 5)	2	3.10 / 3.11	Indien microsoft sentinel gebruikmaakt van AI functionaliteit binnen Azure, valt de toetsing aan de EU AI Act volledig onder verantwoordelijkheid van opdrachtnemer?	Dit om verantwoordelijkheden rondom AI-governance helder te krijgen.	De verantwoordelijkheid rondom AI-governance en de EU AI Act is een gedeelde verantwoordelijkheid, waarbij de aanbestedende dienst de volgende kaders stelt: Platform (provider): Voor de AI-functionaliteiten binnen de Microsoft Azure/Sentinel-omgeving is de platformleverancier (Microsoft) primair verantwoordelijk voor de compliance van de onderliggende technologie aan de EU AI Act. Inrichting en gebruik (deployer): De opdrachtnemer is verantwoordelijk voor de wijze waarop zij AI-functionaliteiten (zoals Copilot for Security of geautomatiseerde analyses) configureert, inzet en beheert ten behoeve van de SOC-dienstverlening. De opdrachtnemer dient te garanderen dat de door hen ingerichte AI-processen voldoen aan de geldende wet- en regelgeving, inclusief transparantie en menselijk toezicht (human-in-the-loop). Governance (user): De gemeente Steenwijkerland voert als eigenaar van de data de regie en toetst of de inzet van AI past binnen het eigen ethische en juridische kader (zoals de AVG). De opdrachtnemer kan de verantwoordelijkheid voor de eigen werkwijze en configuratie van AI-tools dus niet volledig bij de opdrachtgever neerleggen. De opdrachtgever verwacht dat de opdrachtnemer in staat is om aan te tonen hoe zij op een verantwoorde wijze met AI omgaat binnen het SOC.
74	Bijlage 5 Programma van Eisen	Algemeen	3.12	Bij de inzet van Network Detection & Response (NDR)-componenten – wat gezien de detectiemogelijkheden voor geavanceerde aanvallen en kwetsbaarheden vaak sterk wordt aanbevolen – is in de praktijk regelmatig sprake van hardware- of sensorplaatsing binnen het netwerk. Kunt u aangeven of de inzet van hardware (of virtuele sensoren) ten behoeve van NDR is toegestaan binnen de kaders van deze aanbesteding, mede in relatie tot de eis dat er geen hardwarecomponenten op de infrastructuur van opdrachtgever mogen worden geïnstalleerd?	Network Detection & Response (NDR) lijkt momenteel nog geen expliciete eis te zijn binnen de uitvraag. Gezien de lange looptijd van de overeenkomst (10 jaar) en het belang van continue verbetering van de dienstverlening volgens actuele en toekomstige securityrichtlijnen, ligt het voor de hand om dergelijke moderne detectiemogelijkheden mee te nemen.	De aanbestedende dienst herkent de toegevoegde waarde van Network Detection & Response (NDR) in een volwassen security-architectuur. Ten aanzien van de technische invulling gelden de volgende kaders: Geen fysieke hardware: De eis dat er geen fysieke hardwarecomponenten in de infrastructuur van de gemeente geplaatst mogen worden, blijft onverkort van kracht. Dit geldt ook voor NDR-appliances. Virtuele sensoren: De inzet van virtuele sensoren (bijvoorbeeld als VM binnen de bestaande VMware-omgeving) is toegestaan, mits de impact op de performance en het beheer vooraf door de opdrachtnemer is aangetoond en geaccordeerd door de TISO. Integratie: Een eventuele NDR-oplossing dient volledig geïntegreerd te zijn met de Microsoft Sentinel-omgeving van de gemeente. Alerts en relevante metadata moeten centraal in Sentinel landen, zodat er één integraal dashboard voor de analisten ontstaat. Optioneel: NDR is in de huidige uitvraag geen harde eis, maar wordt gewaardeerd als onderdeel van de visie op continue verbetering (Continuous Improvement). Inschrijvers die NDR aanbieden, dienen de kosten hiervoor separaat en transparant in de prijstabel te vermelden. Kortom: NDR is toegestaan mits virtueel en volledig geïntegreerd, maar fysieke hardwareoplossingen zijn niet toegestaan.

75	Programma van Eisen (Bijlage 5)	2	3.12	Worden virtuele collectors, software agents of cloud-based oplossingen gezien als hardwarecomponenten en daarmee uitgesloten?	Om interpretatieverschillen over architectuurkeuzes te voorkomen.	De aanbestedende dienst verduidelijkt hiermee de definitie van hardwarecomponenten in relatie tot de uitsluiting: Hardware (uitgesloten): Onder de uitsluiting vallen uitsluitend fysieke apparaten (fysieke appliances, servers, sensoren) die fysiek in de datacenters of op locaties van de gemeente geplaatst zouden moeten worden. Virtuele collectors (toegestaan): Virtuele appliances of collectors (bijv. een Linux-VM voor syslog-ingestie) die binnen de bestaande virtualisatieomgeving van de gemeente kunnen worden uitgerold, worden niet als hardware aangemerkt en zijn derhalve toegestaan. Software-agents (toegestaan): Softwarematige agents (zoals de Azure Monitor Agent) worden niet als hardware aangemerkt. Het gebruik van standaard Microsoft-agents heeft de voorkeur. Cloudbased oplossingen (toegestaan): Oplossingen die volledig cloud-native of als SaaS worden geleverd, vallen buiten de uitsluiting van hardware. Kortom: De uitsluiting is enkel van toepassing op fysieke hardware. Virtuele en softwarematige componenten zijn toegestaan, mits deze voldoen aan de gestelde eisen op het gebied van beheerlast, veiligheid en architectuur.
76	Bijlage 5 - Programma van Eisen		3.3	Wat wordt bedoeld met de ruleset voor netwerkdetectie gezien netwerksensoren niet in scope zijn?		Met de 'ruleset voor netwerkdetectie' doelt de aanbestedende dienst op de verzameling van detectielogica en correlatieregels die binnen het SIEM (Microsoft Sentinel) worden toegepast op de binnengekomen netwerklogbestanden. Hoewel er geen fysieke of virtuele netwerksensoren voor volledige packet inspection (NDR) in de basis-scope zitten, genereren de in Detailinformatie bijlage 12 genoemde netwerkcomponenten (zoals de firewalls en netwerkapparatuur) rijke logbestanden (o.a. syslog, IPFIX/NetFlow, API-logs). De opdrachtnemer wordt geacht een ruleset te leveren en te onderhouden die op basis van deze logs verdacht gedrag signaleert.
77	Programma van Eisen (Bijlage 5)	2 en 8	3.5 en 10	Moeten correlatieregels en use cases bij beëindiging van de overeenkomst ook buiten Microsoft Sentinel herbruikbaar en overdraagbaar zijn?	In relatie tot exit, kennisborging en herbruikbaarheid.	Ja, de door de opdrachtnemer ingerichte correlatieregels en use-cases in de Microsoft Sentinel-tenant van de gemeente Steenwijkerland moeten bij beëindiging van de overeenkomst volledig beschikbaar, overdraagbaar en functioneel blijven.
78	Programma van Eisen (Bijlage 5)	2	3.9	Wordt Microsoft Sentinel beschouwd als een oplossing die een afhankelijkheid richting Microsoft creëert, en zo ja, welke eisen stelt opdrachtgever aan de bijbehorende exitstrategie?	Om helderheid te krijgen over vendor lock-in en exitneutraliteit.	De keuze voor Microsoft Sentinel als technisch platform is een strategische beslissing van de gemeente Steenwijkerland, die past binnen haar bredere cloud- en architectuurbeleid. De afhankelijkheid van Microsoft als platformleverancier is voor de gemeente een geaccepteerd gegeven en valt buiten de scope van deze aanbesteding. De eisen met betrekking tot de exitstrategie en vendor lock-in (zoals geformuleerd in o.a. eis 3.9) richten zich specifiek op de dienstverlening en de inrichting: Dienstverlener-neutraliteit: De gemeente stelt als eis dat zij te allen tijde moet kunnen overstappen naar een andere SOC-leverancier, met behoud van de inrichting, historie en intelligentie (query's, playbooks) binnen haar eigen Sentinel-tenant. Geen extra barrières: De opdrachtnemer mag geen eigen 'laag' of propriëtaire tooling toevoegen die het onmogelijk maakt voor een opvolgende partij om de dienstverlening op het Sentinel-platform voort te zetten. Datasouvereiniteit: De verzamelde data en de configuratie in de tenant zijn en blijven eigendom van de gemeente. Kortom: De exitstrategie dient gericht te zijn op het borgen van continuïteit bij een wisseling van de wacht tussen SOC-aanbieders, waarbij het platform (Sentinel) als constante factor wordt beschouwd.
79	Programma van Eisen (Bijlage 5)	3-4	4.1 / 4.2	Wordt verwacht dat nieuwe Microsoft Sentinel-functionaliteiten proactief worden geïmplementeerd door opdrachtnemer zonder aanvullende kosten?	Ter verduidelijking van doorontwikkeling binnen de dienstverlening.	De aanbestedende dienst verwacht dat de opdrachtnemer de dienstverlening proactief actueel houdt met de technologische ontwikkelingen van het Microsoft Sentinel-platform. Inbegrepen (continue verbetering): Nieuwe functionaliteiten die door Microsoft binnen de bestaande licenties beschikbaar worden gesteld en die bijdragen aan de effectiviteit, efficiëntie of kwaliteit van de afgesproken monitoring (bijv. verbeterde detectie-algoritmes, nieuwe visualisaties of efficiëntere parsers), dienen proactief en zonder aanvullende kosten te worden geïmplementeerd. Dit valt onder de 'Continuous Improvement'-verplichting van de opdrachtnemer. Uitzondering (scopewijziging): Indien een nieuwe functionaliteit leidt tot een substantiële uitbreiding van de functionele scope (bijv. het ontsluiten van een compleet nieuw type bron dat voorheen technisch niet mogelijk was) of indien er sprake is van additionele licentiekosten vanuit Microsoft, vindt implementatie plaats in overleg en via de wijzigingsprocedure. De aanbestedende dienst verwacht van een strategische partner dat deze adviseert over de roadmap van het platform en zorgdraagt dat de gemeente Steenwijkerland altijd beschikt over een state-of-the-art SIEM/SOC-oplossing.
80	Programma van Eisen (Bijlage 5)	4	4.11	Wanneer de SIEM als dienst wordt geleverd, blijft opdrachtgever zelf beheerrechten houden binnen Microsoft Sentinel, of ligt het volledige beheer exclusief bij opdrachtnemer?	Om verantwoordelijkheden en governance duidelijk af te bakenen.	De gemeente Steenwijkerland behoudt te allen tijde het volledige eigendom en de uiteindelijke beheerrechten over de eigen Microsoft Azure-tenant en de Sentinel-omgeving. Het beheer wordt ingericht op basis van het principe van gedeelde toegang (co-management): Operationeel beheer: De opdrachtnemer krijgt de noodzakelijke rechten (bijv. via Azure Lighthouse of een vergelijkbare veilige methode) om de SIEM/SOC-dienstverlening volledig en zelfstandig uit te voeren. Dit omvat het configureren van regels, het beheren van incidenten en het inrichten van automatisering. Toegang opdrachtgever: De TISO en relevante beheerders van de gemeente behouden (minimaal) leesrechten op de gehele omgeving voor auditdoeleinden en regievoering. Daarnaast behoudt de gemeente de 'Owner'-rol op de tenantonderdelen om de continuïteit bij een eventuele exit te waarborgen. De aanbestedende dienst verwacht dat de opdrachtnemer adviseert over de optimale RBAC-inrichting (Role-Based Access Control) die zowel de effectiviteit van het SOC als de controlebehoefte van de gemeente dient.

81	Programma van Eisen (Bijlage 5)		4.12	Eis 4.12 stelt dat opdrachtnemer de bestaande Microsoft Sentinel omgeving gebruikt. Naast de auditlog-bewaring (eis 9.5) kent Microsoft Sentinel ook substantiële kosten voor reguliere data ingestion en opslag. Zijn deze Azure data ingestion/storage kosten voor alle logs (niet alleen auditlogs) onderdeel van de geoffreerde exploitatiekosten, of worden deze rechtstreeks door opdrachtgever aan Microsoft betaald?		De Azure-kosten voor data-ingestion en data-opslag binnen Microsoft Sentinel (de zogenaamde 'Azure Consumption Costs') maken geen onderdeel uit van de geoffreerde exploitatiekosten van de opdrachtnemer. De gemeente Steenwijkerland beschikt over een eigen Microsoft-overeenkomst (bijv. EA of CSP) en zal de verbruikskosten voor het Sentinel-platform rechtstreeks aan Microsoft voldoen. Van de opdrachtnemer wordt echter wel verwacht dat zij: Adviseert over kostenoptimalisatie: Proactief adviseren welke logbronnen en tabellen kritiek zijn en welke (gezien de kosten) buiten de scope kunnen blijven of naar 'Archive Storage' verplaatst kunnen worden. Monitoring van verbruik: Het bewaken van onverwachte pieken in data-ingestion om budgetoverschrijdingen te voorkomen. Inschrijvers dienen hun prijsstelling dus uitsluitend te baseren op hun eigen dienstverlening (managementfee, analisten, inrichting, etc.) en niet op de onderliggende Azure-consumptie.
82	Programma van Eisen (Bijlage 5)	3	4.12	Wordt een SIEM oplossing met kosteloze dataopslag en native integraties met Microsoft Defender en Microsoft 365 uitgesloten wanneer dit geen Microsoft Sentinel betreft?	Om vast te stellen of kosten en functioneel gunstige alternatieven zijn uitgesloten.	Ja, oplossingen die niet gebaseerd zijn op Microsoft Sentinel zijn uitgesloten. De gemeente heeft strategisch gekozen voor Microsoft Sentinel als technisch platform om maximale synergie, integratie en regie binnen de bestaande Microsoft-omgeving te waarborgen. Inschrijvers dienen hun SIEM/SOC-dienstverlening volledig op dit platform aan te bieden.
83	Bijlage 5 - Programma van Eisen		4.17	Klopt het dat deze tarieven nergens kunnen worden opgenomen in het prijzenblad?		Per abuis is er geen prijsonderdeel opgenomen voor Incident Response (IR) retainer zoals omschreven in eis 4.17. Er is een nieuw prijzenblad toegevoegd aan de nota van inlichtingen waarin inschrijver een uurtarief kan indienen voor uitvoering van Incident Response (IR).
84	Bijlage 5 Programma van Eisen	Algemeen	4.3	Wij zijn een internationale leverancier met medewerkers die in meerdere talen werken. De vaste contactpersoon en het reguliere (verbeter en rapportage) overleg met opdrachtgever vinden in het Nederlands plaats. Ook met een Nederlande partner (Consultants engineers) . Bij lopende detecties of technische afstemming kan het echter voorkomen dat een Engelstalige engineer wordt betrokken. Kunt u aangeven of hiermee wordt voldaan aan de taaleis, of dat de eis zodanig kan worden geïnterpreteerd of aangepast dat regulier contract- en voortgangsoverleg Nederlandstalig is, terwijl incidentele technische ondersteuning ook in het Engels mag plaatsvinden?	Overall Nederlands alleen in incidenten 24x7 kan Engelstalig.	De aanbestedende dienst gaat akkoord met deze invulling onder de volgende voorwaarden: Vaste contactpunten: De vaste contactpersoon (Service Manager), de Lead-analist en de consultants die de periodieke overleggen en rapportages verzorgen, dienen de Nederlandse taal machtig te zijn (minimaal B2-niveau). Technische ondersteuning: Voor ad-hoc technische afstemming of specialistische ondersteuning (bijv. tijdens een incident of complexe wijziging) is het gebruik van de Engelse taal toegestaan. Rapportage: Alle officiële documentatie, zoals maandrapportages, incidentverslagen (post-mortem) en de inrichtingsdocumentatie, dient in de Nederlandse taal te worden opgeleverd. Hiermee wordt de eis geoperationaliseerd zonder de inzet van specialistische internationale expertise te belemmeren.
85	Bijlage 5	3	4.4	Hoe ziet het proces rondom een P1 er op dit moment uit wanneer deze zich buiten kantoortijden voordoet(eventueel ook in relatie tot eventuele 3de partijen)?	Nodig om goede inschatting te kunnen maken over de hoeveelheid werk	Buiten kantoortijden is het proces als volgt ingericht: Melding: Het SOC stelt een P1 vast en onderneemt direct actie conform de vooraf afgestemde playbooks (bijv. isoleren van een endpoint). Alarmering: Het SOC belt de bereikbaarheidsdienst van de gemeente (TISO/piketbeheerder). Coördinatie: De gemeente fungeert als centrale regisseur. Indien nodig schakelt de gemeente zelf andere derde partijen (bijv. de infra-beheerder) in voor herstelwerkzaamheden. Opschaling: Indien de ernst dit vereist, wordt de Incident Response-dienstverlening van de opdrachtnemer geactiveerd. De exacte invulling van de samenwerking en communicatielijnen met specifieke derde partijen wordt tijdens de implementatiefase in het Operationeel Handboek vastgelegd.
86	Bijlage 5 Programma van Eisen	3	Eis 4.4	Kan de gemeente bevestigen dat met deze toelichting afdoende aan deze eis wordt voldaan?	Leverancier hanteert een risicogebaseerde aanpak waarbij p1 en p2 incidenten uiteraard 24/7 worden opgelost binnen de SLA. Voor lagere gevallen, (p3 en p4) hanteert zij standaard een 8x5 service window. Enerzijds verlaagt dit de kosten drastisch voor de gemeente, terwijl dit anderszijds niet leidt tot een vermindering van het beveiligingsniveau. Dit is overigens ook gebruikelijk in de markt.	Nee, de aanbestedende dienst kan dit niet bevestigen. De eis voor 24/7-dienstverlening heeft betrekking op de volledige scope van monitoring, triage en incidentafhandeling. Hoewel de aanbestedende dienst begrijpt dat de intensiteit van de opvolging kan variëren op basis van prioriteit (SLA-tijden), dient de initiële beoordeling (triage) van alle meldingen 24/7 plaats te vinden om te voorkomen dat incidenten met een lage initiële prioriteit onopgemerkt escaleren.
87	Bijlage 5 Programma van Eisen	Algemeen	4.6	De gangbare internationele industriestandaard voor detectie- en responstijden ligt rond de 15 minuten. Kan opdrachtgever aangeven of wordt overwogen om deze norm aan te passen, bijvoorbeeld door strengere responstijden te hanteren, indien dit leidt tot een betere kwaliteit van de aanbestedde dienstverlening?	Aanbestedende dienst doet zich mogelijk te kort	De aanbestedende dienst hanteert de reactietijden zoals gedefinieerd in de aanbestedingsstukken. Deze tijden worden beschouwd als passend voor de risicoprofielen van de gemeente en de gewraagde kwaliteit van de dienstverlening. Hoewel inschrijvers vrij zijn om in hun plan van aanpak scherpere tijden aan te bieden als onderdeel van hun kwaliteitsbelofte, zal de aanbestedende dienst de gestelde eisen op dit moment niet naar boven of beneden bijstellen. De kwalitatieve beoordeling vindt plaats op basis van de in de gunningsleidraad genoemde criteria.
88	Bijlage 5 Programma van Eisen	3	eis 4.6	Kan de gemeente akkoord gaan met een vrijwaringsverklaring, althans deze na eventuele gunning afstemmen met Leverancier? Deze zal dan onderdeel worden van de aanbieding van Leverancier.	Leverancier kan uiteraard op basis van mandaat in actie komen. Wel geldt dan dat zij een vrijwaringsverklaring vereist voor eventuele nevenschade die mogelijk kan ontstaan bij een dergelijke mandaatactie. Deze vrijwaring ziet uiteraard enkel de situatie dat Leverancier binnen de kaders van het mandaat en conform de overeenkomst heeft geacteerd.	Ja, aanbestedende dienst staat ervoor open om na definitieve gunning in samenspraak met opdrachtnemer een vrijwaringsverklaring op te stellen.
89	Bijlage 5 Programma van Eisen	4	eis 4.16, eis 11.9	Kan de gemeente bevestigen dat met deze toelichting aan deze eis wordt voldaan?	Leverancier hanteert standaard een beschikbaarheid van 99.5%.	Nee, de gemeente kan dit niet bevestigen. De gemeente houdt vast aan de gestelde eisen in het Programma van Eisen. Een beschikbaarheid van 99,5% wordt voor een cruciale veiligheidsdienst (24/7-monitoring) als onvoldoende beschouwd. Inschrijvers worden geacht hun dienstverlening en bijbehorende SLA in te richten conform de gestelde eisen.

90	Programma van eisen	3	4,6	Bij de hoogste classificatie (prio 1) geldt een mandaat actie dat binnen 30 minuten na bekendheid van het incident moeten worden uitgevoerd. Dit zal ook direct vermeld moeten worden aan de opdrachtgever. Overige prio's worden in overleg met elkaar afgestemd.Kunt u nader toelichten wat de definitie mandaat actie inhoudt?	Een verduidelijking is nodig om een goede inschatting te maken wat u van inschrijver verwacht.	Onder een 'mandaat actie' wordt verstaan: een dwingende technische interventie die de opdrachtnemer zonder voorafgaand overleg mag (en moet) uitvoeren om verdere schade bij een P1-incident te beperken. Voorbeelden hiervan zijn: - Het isoleren van een besmet endpoint van het netwerk. - Het tijdelijk blokkeren van een gecompromitteerd gebruikersaccount. - Het blokkeren van een kwaadaardig IP-adres op de firewall. De specifieke kaders en de lijst met toegestane acties worden tijdens de implementatiefase per scenario vastgelegd in 'Playbooks'. Na uitvoering van een mandaat actie dient de opdrachtgever direct (binnen het gestelde tijdslot) te worden geïnformeerd.
91	Bijlage 5	4	4.9	Kun u een overzicht delen van welke bronnen en welke usecases er op dit moment actief zijn in het soc? Eventueel na het ondertekenen van een NDA.		De aanbestedende dienst stelt een overzicht van de huidige logbronnen (inclusief benamingen en aantallen servers/clients) beschikbaar. Deze bijlage is uitsluitend beschikbaar voor inschrijvers en kan worden opgevraagd via TenderNed (berichtenmodule). Opdrachtnemer verklaart dat het verstrekte document uitsluitend zal worden gebruikt ten behoeve van het voorbereiden en indienen van een inschrijving in het kader van deze aanbesteding. Opdrachtnemer zal het document niet aan derden verstrekken, noch geheel of gedeeltelijk kopiëren of anderszins gebruiken voor andere doeleinden. Na afronding van de aanbestedingsprocedure, ongeacht de uitkomst daarvan, zal opdrachtnemer het document onverwijld vernietigen. Wat betreft de use cases: de opdrachtgever vraagt inschrijvers om een eigen standaardset aan detectieregels (use cases) voor te stellen die aansluit bij de geboden logbronnen en specifiek is afgestemd op een gemeentelijke organisatie (conform BIO/MITRE ATT&CK). De exacte afstemming en fijnmazige inrichting van deze use cases zal plaatsvinden tijdens de implementatiefase.
92	Bijlage 5	4	4.11	Kunt u bevestigen of in uw Azure-tenant uitsluitend Microsoft Sentinel wordt gebruikt voor SIEM, of dat daarnaast andere (security)diensten en componenten actief zijn binnen dezelfde tenant?	juiste afbakening scope	De aanbestedende dienst bevestigt dat Microsoft Sentinel de centrale SIEM-oplossing is voor deze opdracht. Binnen de Azure-tenant zijn daarnaast de verschillende Microsoft Defender-componenten actief (zoals Defender for Endpoint, Identity en Office 365), die als primaire bronnen voor Sentinel fungeren. De scope van deze aanbesteding richt zich op de inrichting, het beheer en de 24/7-opvolging binnen Microsoft Sentinel, inclusief de integratie met de genoemde Defender-diensten. Eventuele specifieke aanvullende securitycomponenten van derden die relevant zijn voor de logingestie, zijn opgenomen in de bronnenlijst die na ondertekening van de NDA beschikbaar wordt gesteld.
93	Programma van Eisen		4.13 Incidentafhandeling	In 4.13 wordt gesproken over afhandeling van incidenten. Kunt u verduidelijken of deze paragraaf uitsluitend ziet op SOC-activiteiten (detectie, analyse en escalatie), of dat hieronder ook volledige Incident Response-activiteiten vallen zoals forensisch onderzoek en herstelondersteuning?		De werkzaamheden in paragraaf 4.13 hebben betrekking op de reguliere SOC-activiteiten: detectie, triage, analyse en de eerste maatregelen tot indamming (containment). Voor volledige Incident Response-activiteiten, zoals diepgaand forensisch onderzoek en grootschalige herstelondersteuning na een significante inbreuk, dient de opdrachtnemer wel de capaciteit en expertise beschikbaar te hebben. Deze specialistische inzet valt echter buiten de vaste maandelijkse dienstverleningskosten en zal, indien nodig, op basis van vooraf overeengekomen tarieven (nacalculatie) worden ingezet zoals aangegeven in het vernieuwde prijzenblad.
94	Programma van eisen	4	4,13	Opdrachtnemer levert een gedetailleerd post-incident rapport en adviseert verbeteringen in de door opdrachtnemer beheerde ict-omgeving en -processen om toekomstige incidenten te voorkomen. Daarnaast worden er aanbevelingen richting opdrachtgever gedaan over het oplossen van organisatiekwetsbaarheden die "buiten de invloedsfeer" van de opdrachtnemer vallen. Kunt u nader toelichten wat u bedoelt met "organisatiekwetsbaarheden buiten de invloedsfeer van de opdrachtnemer vallen"?	Een verduidelijking is nodig om een goede inschatting te maken wat u van inschrijver verwacht.	Met 'organisatiekwetsbaarheden buiten de invloedsfeer van de opdrachtnemer' worden zaken bedoeld die de opdrachtnemer niet direct zelf technisch kan oplossen, maar die wel uit de incidentanalyse naar voren komen. Denk hierbij aan: -Procesmatig: Een incident dat ontstaat doordat autorisaties niet tijdig worden ingetrokken bij uitdiensttreding - (instroom-doorstroom-uitstroomproces). -Beleid: Het ontbreken van een clean-desk-policy waardoor inloggegevens fysiek zijn buitgemaakt. -Bewustwording: Herhaaldelijke succesvolle phishingincidenten binnen een specifieke afdeling die vragen om extra security-awarenesstraining. -Technisch (extern): Kwetsbaarheden in applicaties van derde partijen waar de opdrachtnemer geen beheer op voert. De aanbestedende dienst verwacht dat de opdrachtnemer deze patronen herkent en de gemeente hierover proactief adviseert om de algehele weerbaarheid te verhogen.
95	Programma van Eisen (Bijlage 5)	4	4.17	U geeft aan dat de retainer het verzorgen van trainingen omvat. Kunt u aangeven hoe vaak u die trainingen verwacht af te nemen en voor hoeveel personen?		De trainingen hebben in de initiële fase primair tot doel het bevorderen van een effectieve samenwerking tussen opdrachtgever en opdrachtnemer. In het kader van de implementatie en kennisoverdracht dient de opdrachtnemer gedurende de looptijd van de overeenkomst maandelijks een overleg en/of training te verzorgen. De trainingen zijn bestemd voor maximaal drie (3) deelnemers per sessie.
96	Programma van Eisen (Bijlage 5)	4	4.17	Wat is het verschil tussen CERT-functionaliteit (operationeel SOC) en IR-retainer uit eis 4.17? Welke activiteiten vallen onder basis exploitatiekosten en welke onder IR-retainer met separate tarieven? Hoeveel uur forensisch onderzoek per jaar moet in exploitatiekosten?		De aanbestedende dienst hanteert de volgende verdeling: SOC-functionaliteit (basis exploitatiekosten): Omvat 24/7-monitoring, triage, analyse en de eerste maatregelen tot indamming (containment, bijv. isoleren van een endpoint). Dit is de reguliere dienstverlening. IR-retainer (separate tarieven): Dit betreft de beschikbaarheid van specialistische kennis voor complexe escalaties. De werkzaamheden (zoals diepgaand forensisch onderzoek, root-causeanalyse van complexe infecties en grootschalige herstelondersteuning) vallen onder deze retainer en worden op basis van nacalculatie verrekend tegen de in de offerte genoemde tarieven.
97	Programma van Eisen (Bijlage 5)	4	4.9	Betekent het vereiste inzicht in use cases en IoC's dat alle Sentinel analytics rules volledig inzichtelijk en overdraagbaar moeten zijn?	Ter verduidelijking van transparantie- en overdraagbaarheidseisen.	Ja, de aanbestedende dienst bevestigt dat alle in de Sentinel-omgeving van de gemeente geconfigureerde analytics rules volledig inzichtelijk en overdraagbaar moeten zijn. Aangezien de gemeente eigenaar is van de data en de gebruikte SIEM-omgeving, is volledige transparantie over de actieve detectielogica essentieel voor de verantwoording (compliance) en de continuïteit van de beveiliging. Bij beëindiging van de overeenkomst blijven de geconfigureerde regels en instellingen in de tenant van de gemeente aanwezig.
98	Bijlage 5 - Programma van Eisen		5.1	Kan aangegeven worden dat opdrachtnemer niet verantwoordelijk kan worden gehouden voor deze eisen voor zover dit de Sentinel van opdrachtgever betreft?		Opdrachtnemer kan niet verantwoordelijk worden gehouden voor het beveiligen van gegevens (opslaan en transport) conform eis 5.1, voor zover dit in de Sentinel-omgeving van aanbestedende dienst wordt uitgevoerd.

99	Bijlage 5 Programma van Eisen	5	eis 5.2	Kan de gemeente deze eis laten vervallen?	Deze eis is niet uitvoerbaar met de dienstverlening die de gemeente uitvraagt. De gemeente beschikt zelf over Microsoft E5 (Cloud) licenties, dus alle data die via de sentinel tenant wordt gedeeld met de leverancier, zijn reeds opgeslagen bij Microsoft, een partij met een vestiging in de Verenigde Staten. Het voldoen aan deze eis is uitsluitend mogelijk als de gemeente zelf geen systemen, netwerken, en applicaties heeft draaien via een SaaS van een Amerikaanse partij, en daarbij in het geval dat de leverancier geen gebruik maakt van een SaaS van een partij met vestiging in de Verenigde Staten. Er zijn momenteel geen deugdelijke alternatieven binnen de EU voorhanden die een soortgelijke kwaliteit van dienstverlening kunnen leveren. Deze garantie kan bovendien uitsluitend door deze partij zelf worden afgegeven en niet door leverancier. Als de gemeente dit wenst, zal zij dus rechtstreeks met haar eigen leverancier van haar netwerkomgeving moeten afstemmen. Wel kan leverancier bevestigen dat zij alle data opslaat op een omgeving gevestigd binnen EER.	De gemeente maakt gebruik van de 'Microsoft EU Data Boundary'. Microsoft garandeert hierbinnen contractueel dat de opslag en verwerking van klantgegevens voor Europese klanten uitsluitend binnen de EU/EER plaatsvindt. Hiermee wordt voldaan aan de gestelde eisen omtrent data-residentie en de geldende privacywetgeving.
100	Bijlage 5	5	5.2	Aangezien Sentinel in Azure draait op een tenant van de gemeente. Wat is de exacte scope van deze eis? Kunt u dat nader toelichten?	We kunnen niet verantwoordelijk voor zijn voor iets waar we zelf de regie niet over hebben.	Gemeente Steenwijkerland blijft eigenaar van de Azure-tenant. Er zal een mandaat opgesteld moeten worden dat bepaalt wat de regie zal zijn voor de opdrachtnemer.
101	Bijlage 5 - Programma van Eisen		5.2	Kan aangegeven worden dat opdrachtnemer niet verantwoordelijk kan worden gehouden voor deze eisen voor zover dit de Sentinel van opdrachtgever betreft (https://www.convotis.com/en/news/microsoft-access-eu-data/)?		De aanbestedende dienst verduidelijkt dat de opdrachtnemer niet verantwoordelijk wordt gehouden voor de juridische kaders en de onderliggende infrastructuur-compliance van Microsoft als cloudprovider (zoals de 'Microsoft EU Data Boundary'). Deze vallen binnen de directe contractuele relatie tussen de gemeente en Microsoft. De verantwoordelijkheid van de opdrachtnemer onder eis 5.2 richt zich op de configuratie, het beheer en de operationele veiligheid van de Microsoft Sentinel-omgeving. Dit omvat onder meer het toepassen van de juiste toegangsbeveiliging (RBAC), het voorkomen van ongeautoriseerde toegang door medewerkers van de opdrachtnemer en het juist inrichten van de monitoring conform de overeengekomen standaarden. Verder is eis 5.2 van toepassing op het moment dat inschrijver extra tooling inzet.
102	Bijlage 5 - Programma van Eisen		5.2	Inschrijver begrijpt dat deze eis is bedoeld om risico's rondom toegang tot gegevens door buitenlandse overheidsinstanties, zoals op grond van de VS Freedom Act, te mitigeren. Inschrijver merkt daarbij op dat in de huidige markt de meeste cloud-providers echter wel een vestiging in de VS hebben. De inschrijver merkt daarbij op dat: -Alle applicatiecomponenten en gegevens in principe uitsluitend binnen de EER worden gehost en verwerkt, tenzij er is voldaan aan art. 45 of 46 van de AVG; -Verzoeken tot toegang tot gegevens door (buitenlandse) overheidsinstanties in de praktijk zeer ongebruikelijk zijn en zich bij de inschrijver nog nooit hebben voorgedaan; -Dergelijke verzoeken, indien zij zich toch zouden voordoen, zeer kritisch worden beoordeeld in het licht van de wet- en regelgeving op het gebied van gegevensbescherming; -De inschrijver gegevens uitsluitend verstrekt indien daartoe een juridisch bindende verplichting bestaat en daarbij alle redelijke inspanningen verricht om verstrekking te voorkomen, waaronder het toetsen van de rechtmatigheid van het verzoek en het benutten van beschikbare rechtsmiddelen, voor zover wettelijk toegestaan; - Indien verstrekking desalniettemin wettelijk verplicht is, zal de inschrijver de verstrekking beperken tot uitsluitend die gegevens die strikt noodzakelijk zijn om aan de wettelijke verplichting te voldoen; -De verwerkingsverantwoordelijke altijd wordt geïnformeerd over een dergelijk verzoek, voorafgaand aan enige verstrekking of – indien voorafgaande kennisgeving wettelijk niet is toegestaan – onverwijld daarna. Kan de aanbestedende dienst bevestigen dat, bovenstaande omstandigheden en waarborgen, voldoende garantie bieden als bedoeld in deze eis?		De aanbestedende dienst erkent dat veel cloudproviders een vestiging in de VS hebben. De door u genoemde waarborgen, zoals hosting binnen de EER, het juridisch toetsen van verzoeken en het informeren van de gemeente, zijn essentieel om de risico's rondom buitenlandse wetgeving (zoals de US Cloud Act) te beperken. Deze werkwijze biedt voldoende garantie, mits de uitvoering voldoet aan de AVG-wetgeving en de richtlijnen van de Autoriteit Persoonsgegevens.
103	Bijlage 5 - Programma van Eisen		5.2	Op basis van art. 4.3 van de Verwerkersovereenkomst mag Verwerker Persoonsgegevens buiten de EER (laten) verwerken wanneer is voldaan aan de voorwaarden van artikel 45 of 46 AVG. Kunt u bevestigen dat dit evenwel geldt in relatie tot deze eis?		De aanbestedende dienst gaat hier niet mee akkoord.
104	Programma van Eisen (Bijlage 5)	5	5.2 5.3	Welke concrete criteria en bewijslast hanteert opdrachtgever om aan te tonen dat data binnen Microsoft Sentinel niet opvraagbaar is onder Amerikaanse wetgeving, gezien Microsoft als cloudleverancier?	ter verduidelijking van juridische en compliance eisen in relatie tot Sentinel	Licenties zijn onder VNG-contract gesloten. In dit contract is opgenomen dat alle data wordt gehost op Europese servers.
105	Programma van Eisen (Bijlage 5)	5	5.2 - 5.3 en 4.12	Opdrachtgever beschikt al over een bestaande Microsoft Sentinel omgeving in de eigen Azure tenant en schrijft in4.12 het gebruik hiervan voor. Tegelijk worden in 5.2 en 5.3 eisen gesteld aan datalocatie en het nie -opvraagbaar zijn van data onder Amerikaanse wetgeving. Kan opdrachtgever toelichten hoe is vastgesteld dat de huidige Sentinel inrichting hieraan voldoet, en welke onderbouwing of aantoonbaarheid hierover van inschrijvers wordt verwacht?	Om beter te begrijpen hoe opdrachtgever de verplichte inzet van Microsoft Sentinel combineert met de juridische en compliance-eisen rondom dataopslag en toegang, en hoe inschrijvers hier concreet op moeten aansluiten in hun aanbieding.	Microsoft Sentinel valt binnen de huidige Microsoft-licenties die zijn afgesloten conform het VNG-framework GT Microsoft. Dit framework helpt bij het borgen van wet- en regelgeving omtrent security en privacy. Bij het sluiten van de overeenkomst heeft Microsoft bevestigd hieraan te voldoen. Aanbestedende dienst is van mening dat de omgeving van Sentinel eveneens voldoet aan hetgeen dat is beschreven in eis 5.2 en 5.3.
106	Programma van Eisen (Bijlage 5)	5	5.2 5.4	In welke Azure regio's moet de Log Analytics Sentinel omgeving worden ingericht om te voldoen aan de EU/EER eisen, en hoe wordt dit gecontroleerd?	Regiokeuze is bepalend voor data residency en compliance.	De Microsoft Sentinel / Log Analytics-omgeving dient te worden ingericht in de Azure-regio West Europe (gevestigd in Nederland). Alle opgeslagen data (Data at Rest) dient binnen de Europese Economische Ruimte (EER) te blijven. De controle hierop vindt op de volgende wijze plaats: Inrichting: De opdrachtnemer dient bij de configuratie aan te tonen dat de Log Analytics Workspace fysiek is gekoppeld aan de regio West Europe. Rapportage: De opdrachtnemer dient periodiek (of op verzoek) te bevestigen dat de data-opslaglocatie ongewijzigd is gebleven conform de vigerende privacywetgeving en gemeentelijke richtlijnen.
107	Programma van Eisen		6.1 Verklaring Omtrent het Gedrag (VOG)	In 6.1 wordt een VOG-eis gesteld. Kunt u toelichten voor welke functies of rollen binnen de dienstverlening deze VOG-eis geldt en welke screeningsprofielen hierbij van toepassing zijn?		Het geldt voor alle rollen en functies die toegang hebben tot verzamelde gegevens. Het gaat om een standaard VOG zonder screeningsprofielen.

108	Bijlage 5 Programma van Eisen	Algemeen	6.1	Is er binnen deze eis een expliciete eis opgenomen ten aanzien van het minimale aantal medewerkers dat beschikbaar moet zijn voor de SOC- en/of Incident Response (IR)-dienstverlening, in het kader van continuïteit en beschikbaarheid?	Het hanteren van een minimaal aantal beschikbare medewerkers draagt bij aan de continuïteit en beschikbaarheid van de dienstverlening, mede gezien het momenteel hoge personeelsverloop binnen de Nederlandse securitymarkt.	De aanbestedende dienst stelt geen expliciet minimum aan het aantal medewerkers. De opdrachtnemer is zelf verantwoordelijk voor een personele bezetting die de continuïteit en kwaliteit van de 24/7 dienstverlening waarborgt, conform de gestelde SLA-eisen. Wel dient de opdrachtnemer in het kader van eis 6.1 (en de kwalitatieve toelichting in het plan van aanpak) continuïteit te geborgen bij ziekte, vakantie en personeelsverloop. Hierbij wordt specifiek gekeken naar de beschikbaarheid van de verschillende expertiseniveaus (1e, 2e en 3e lijns analisten en Incident Responders).
109	Bijlage 5 Programma van Eisen	6	eis 6.5	ISO 27001 en ISO 9001 overlappen elkaar in dit opzicht. Kan de gemeente bevestigen dat het voldoen aan ISO 27001 voldoende is? Zo nee, kan de gemeente bevestigen dat leverancier ook voldoet aan deze eis als ze voldoende aantoont dat zij maatregelen heeft genomen om aan soortgelijke normen te voldoen?		ISO 27001 en ISO 9001 zijn beide internationale normen en zullen beperkt overlap hebben, maar ze richten zich op heel verschillende onderwerpen. ISO 9001 richt zich op kwaliteitsmanagement, terwijl ISO 27001 zich primair richt op informatiebeveiliging. Aanbestedende dienst gaat niet akkoord met het enkel voldoen aan ISO 27001 of vergelijkbaar. Als u niet over de certificaten beschikt, maar over een gelijkwaardig certificaat of kwaliteitsborgingssysteem, dan dient u bij uw inschrijving aan te geven en te omschrijven waarom het certificaat of systeem gelijkwaardig is. Wij moeten uit deze omschrijving kunnen opmaken dat er sprake is van gelijkwaardigheid.
110	Programma van Eisen		7 Notificatie	In 7 wordt notificatie beschreven, waarbij Incident Response niet expliciet wordt genoemd. Kunt u verduidelijken wie verantwoordelijk is voor het initiëren van Incident Response en wie besluit over opschaling naar een IR-organisatie bij een (grootschalig) incident?		De opdrachtnemer levert een Incident Response (IR)-retainer waarmee de opdrachtgever 24/7 directe toegang heeft (via een dedicated noodnummer, telefonisch) tot een team van cyberbeveiligingsexperts, met vooraf vastgestelde reactietijden en tarieven, teneinde schade te beperken en herstel te versnellen. De retainer biedt gegarandeerde beschikbaarheid bij incidenten, inclusief directe telefonische ondersteuning en een overeengekomen starttijd voor het onderzoek. De opdrachtnemer stelt gespecialiseerde expertise beschikbaar voor onder meer digitaal forensisch onderzoek, juridische ondersteuning en begeleiding bij communicatie met toezichthouders en verzekeraars. Daarnaast omvat de retainer proactieve voorbereidende diensten, zoals het helpen van de opdrachtnemer bij het opstellen of actualiseren van een Incident Response-plan, afgestemd op de organisatie van de opdrachtgever, en het verzorgen van trainingen (minimaal één IR-oefening of -training per jaar voor relevante medewerkers), met als doel het beperken van financiële, reputatie- en juridische schade. De opdrachtnemer stelt gespecialiseerde expertise beschikbaar voor: 1.digitaal forensisch onderzoek (inclusief loganalyse, malware-onderzoek en vaststelling van de oorzaak en impact); 2.mitigatie- en herstelmaatregelen; 3.rapportage: De opdrachtgever ontvangt na afronding van een incident een schriftelijk incidentrapport, inclusief tijdlijn, bevindingen, genomen maatregelen en aanbevelingen.
111	Programma van Eisen		8 Rapportage	Kunt u bevestigen of post-incident rapportage na afronding van Incident Response-activiteiten onderdeel is van de scope, en zo ja, welk format en detailniveau hiervoor wordt verwacht?		De aanbestedende dienst bevestigt dat post-incidentrapportage integraal onderdeel is van de scope van de dienstverlening. Wat betreft het format en detailniveau wordt het volgende verwacht: Standaardincidenten: Een beknopte rapportage in het ticketsysteem (oorzaak, getroffen systemen, genomen acties). Significante incidenten (bijv. P1/P2): Een formeel Post-Incident Report (PIR) dat minimaal de volgende elementen bevat: Timeline van detectie tot herstel. Root Cause Analysis (RCA). Impactanalyse op data en systemen. Geleverde adviezen ter voorkoming van herhaling (verbetermaatregelen). De opdrachtnemer mag hiervoor eigen standaarden hanteren, mits deze voldoen aan bovenstaande minimale vereisten.
112	Bijlage 5 Programma van Eisen	Algemeen	9.1	Onbeperkte bewaartermijnen (retentie) zijn doorgaans niet mogelijk zonder aanvullende kosten. Kan opdrachtgever aangeven of de vereiste bewaartermijnen mogen worden gelimiteerd, of dat het volstaat wanneer data na afloop van de retentieperiode beschikbaar wordt gesteld via een export?	Kosten mbt bewaartermijn	De aanbestedende dienst vereist geen onbeperkte bewaartermijn. Voor de prijsvorming dient de opdrachtnemer uit te gaan van de volgende retentie-eisen: Hot storage (Sentinel): Een standaardretentieperiode van 90 dagen voor directe analyse en correlatie. Long-term storage: Loggegevens dienen in totaal 12 maanden beschikbaar en doorzoekbaar te blijven voor forensische doeleinden. De opdrachtnemer mag voor de periode na de eerste 90 dagen gebruikmaken van kostenefficiënte oplossingen zoals Sentinel Archive of een koppeling met een Azure Storage Account. Het volstaat niet om enkel een export aan te bieden; de data moet binnen de afgesproken termijn van 12 maanden door de opdrachtnemer bevraagd kunnen worden bij incidentonderzoek.
113	Programma van Eisen		9.1 Logretentie	Ten aanzien van logdata binnen de Microsoft Sentinel-tenant van opdrachtgever: kunt u bevestigen hoe de verantwoordelijkheden voor logretentie zijn verdeeld tussen opdrachtgever en opdrachtnemer?		De verantwoordelijkheden met betrekking tot logretentie zijn als volgt verdeeld: Opdrachtgever (gemeente): Blijft eindverantwoordelijk voor het vaststellen van het retentiebeleid op basis van wettelijke kaders (zoals AVG en BIO) en de bijbehorende kosten voor de Azure-consumptie. Opdrachtnemer (leverancier): Is verantwoordelijk voor de correcte configuratie en het beheer van de retentie-instellingen binnen Microsoft Sentinel conform de afgesproken termijnen (bijv. 90 dagen hot / 12 maanden totaal). Daarnaast heeft de opdrachtnemer een proactieve adviesrol: indien wijzigingen in het Microsoft-platform (bijv. nieuwe storage-tiers) of wetgeving invloed hebben op de retentiestrategie of kosten, dient de opdrachtnemer de gemeente hierover te adviseren.
114	Bijlage 5 - Programma van Eisen		9.1-5	Er dient gebruik gemaakt te worden van Sentinel en de retentieperiode daarin. Kan opdrachtnemer ervan uitgaan de deze retentieperiodes door de gemeente in overleg met Microsoft zijn vastgesteld?		Ja, deze retentieperiodes zijn vastgelegd vanuit de BIO.
115	Bijlage 5	7	9.3	Gaat het hier ook om Meta data?	helder beeld van de scope	Nee, de metadata valt hier niet onder.
116	Bijlage 5 Programma van Eisen	7	eis 9.4	Kan de gemeente bevestigen dat hiermee aan deze eis wordt voldaan?	Aangezien de data die niet tot een alert hebben geleid vanuit het oogpunt van privacy- en security by design binnen de tenant van de gemeente blijft en niet door leverancier wordt opgeslagen, kan de gemeente binnen haar softwarelicentie kiezen om deze data voor tenminste zes maanden op te slaan.	Binnen Sentinel kun je maximaal zes maanden terug. Deze data hebben we dan zelf ook inzichtelijk.

117	Bijlage 5 Programma van Eisen		eis 9,5	U geeft aan dat de auditlogs minimaal 3 jaar moeten worden bewaaard. Bent u zich ervan bewust dat dit extra kosten in Azure met zich meebrengt? Kunt u tevens aangeven wat nu ongeveer de hoeveelheid data-ingestie is?		De aanbestedende dienst is zich bewust van de Azure-opslagkosten voor de 3-jarige bewaartermijn van auditlogs (beheerhandelingen). Deze eis is specifiek bedoeld voor compliance-doeleinden en betreft een beperkt datavolume. Met betrekking tot de huidige data-ingestie: de huidige inrichting is minimaal en niet representatief voor de toekomstige situatie. De opdrachtgever kan op dit moment geen betrouwbare indicatie geven van het aantal GB's per dag voor de volledige scope. Inschrijvers worden daarom gevraagd om in hun voorstel op basis van de verstrekte omgevingsfactoren (aantal werkplekken, servers en licentievormen zoals opgenomen in de bijlage) een deskundige inschatting te maken van de te verwachten data-ingestie en de bijbehorende Azure-consumptiekosten.
118	Programma van Eisen (Bijlage 5)	8	10.1 en 10.2	Moet de exitstrategie alleen betrekking hebben op de SOC-dienstverlening, of ook op Sentinel-configuraties, analytics rules, use cases en data?	Ter verduidelijking van de scope en diepgang van de exitverplichtingen.	De exitstrategie heeft betrekking op de volledige scope van de dienstverlening om de continuïteit van de informatiebeveiliging te borgen. Dit betekent dat de exitstrategie niet alleen de overdracht van de SOC-operatie (procedures, lopende incidenten) omvat, maar ook: Sentinel-configuraties: Alle instellingen binnen de tenant van de gemeente. Analytics rules & use cases: Alle actieve detectielogica die binnen de Microsoft Sentinel-omgeving van de opdrachtgever is ingericht. Deze dienen volledig gedocumenteerd, inzichtelijk en functioneel achter te blijven. Data: Alle logdata en historische incidentinformatie blijven in de tenant van de opdrachtgever en vallen daarmee onder de directe regie van de gemeente. Het doel is dat de gemeente bij beëindiging van de overeenkomst de dienstverlening zonder 'blind spots' kan overdragen aan een volgende partij of intern kan voortzetten.
119	Bijlage 5 Programma van Eisen	8	eis 10.2 en 10.3	Kan de gemeente akkoord gaan met de toelichting van Leverancier en de eis hierop aanpassen?	De standaard use cases en configuraties die Leverancier inzet voor de dienstverlening aan de gemeente, zijn en blijven in eigendom van Leverancier en worden niet overgedragen als onderdeel van de overeenkomst. De gemeente verkrijgt slechts een niet exclusief gebruiksrecht hierop voor de duur van de overeenkomst. Dat betekent dat deze bij een exit ook niet aan een derde partij worden overgedragen. Dit is immers onderdeel van het bedrijfsdebiet van Leverancier. Dit is anders voor specifieke use cases die exclusief voor de gemeente worden ontwikkeld. Hiervoor geldt echter dat deze na separate betaling daarvoor aan de gemeente worden overgedragen. Deze vallen in principe namelijk buiten de scope van de managed dienstverlening. Uiteraard wordt alle klantdata van de gemeente voor zover Leverancier daarover beschikt, als ook alle rapportages kostenloos ter beschikking gesteld, zodat de gemeente die kan delen met een nieuwe leverancier. Daarnaast geldt dat Leverancier eventuele werkzaamheden in het kader van een exit in redelijkheid vergoed moet kunnen krijgen. Het betreffen immers extra (project)werkzaamheden. Wel acht Leverancier het redelijk als zij die kosten moet dragen in het geval dat het einde van de overeenkomst het gevolg is van ontbinding vanwege een toerekenbare tekortkoming in de nakoming van de overeenkomst door leverancier. Leverancier verwijst in dat kader ook naar artikel 26.4 van GIBIT 2023.	Akkoord.
120	Bijlage 5 - Programma van Eisen		10.2	Kan deze eisen worden beperkt tot use cases welke specifiek voor de gemeente zijn aangemaakt? De door opdrachtnemer gebruikte use cases die gebruikt worden voor alle klanten vallen onder Intellectual Property en kunnen na afloop van de dienstverlening tegen betaling gebruikt worden door klanten, maar niet door onze concurrenten.		Aanbestedende dienst gaat niet akkoord.
121	Bijlage 5 Programma van Eisen	8	Eis 10.4	Kan de gemeente bevestigen dat hiermee aan deze eis wordt voldaan?	Leverancier kan aan deze eis voldoen, mits en voor zover de gemeente aan haar betalingsverplichtingen die betrekking hebben op de voortzetting van de dienstverlening voldoet voor de duur van de retransitie.	Akkoord.
122	Bijlage 5 Programma van Eisen	8	Eis 11.1 en 4.10	Op basis van welke frequentie wil de gemeente de dienstverlening bespreken / evalueren?	Eis 11.1 gaat uit van 4x per jaar, terwijl eis 4.10 uitgaat van minimaal 1x per maand. Dit is tegenstrijdig.	Per abuis in in eis 4.10 1 keer per maand aangeven. Dit moet zijn 4 keer per jaar.
123	Bijlage 5 Programma van Eisen	8	eis 11.3	U heeft het hier over de eis bij 9.3, maar die gaat over de bewaartermijn. Wordt hier 8.2 bedoeld?		Ja, dat klopt. De verwijzing naar eis 9.3 is onjuist; dit moet inderdaad eis 8.2 zijn.
124	Bijlage 5 Programma van Eisen	8	Eis 11.4	Graag de bevestiging van de gemeente dat deze eis alleen betrekking heeft op de systemen die leverancier levert / beschikbaar stelt om haar dienstverlening te kunnen leveren.		Dat klopt. De aanbestedende dienst bevestigt dat eis 11.4 uitsluitend betrekking heeft op de systemen, tooling en infrastructuur die de leverancier inzet of beschikbaar stelt voor het leveren van de dienstverlening. De verantwoordelijkheid voor de beveiliging en het beheer van de bronsystemen van de gemeente zelf blijft bij de gemeente.
125	Bijlage 5 Programma van Eisen	Algemeen	11.4	Kunt u bevestigen dat de eis met betrekking tot patchmanagement niet ziet op het patchmanagement van de volledige klantomgeving, maar uitsluitend betrekking heeft op de binnen scope vallende componenten van de dienstverlening	Patch management in niet in scope alleen voor de toegevoegde dienst onderdelen?	Patchmanagement is inderdaad van toepassing op de binnen de scope vallende componenten. De componenten die in gebruik zijn, moeten worden voorzien van de laatste beveiligingspatches, mits deze beschikbaar en bekend zijn.
126	Bijlage 5 Programma van Eisen	Algemeen	11.5	Wij bieden zowel een Nederlandstalige als een Engelstalige helpdesk aan. Kunt u bevestigen dat dit akkoord is binnen de gestelde eisen?	Akkoord voor tweetaligheid.	Akkoord, mits de keuze voor Nederlands altijd beschikbaar is.
127	Bijlage 5 Programma van Eisen	9	11.10, 8.2	Welke SLA-afspraken gelden voor incidentrespons en -herstel? Heeft u daarnaast nog meer SLA afspraken op het oog of wordt dit nader afgesproken naast eis 8.2? Bijvoorbeeld NTTD en MTTR?		De aanbestedende dienst hanteert voor incidentrespons de volgende minimale SLA-reactietijden, gebaseerd op de prioriteit van de melding: Prioriteit 1 (Kritiek): Respons binnen 30 minuten, 24/7. Prioriteit 2 (Hoog): Respons binnen 1 uur, 24/7. Prioriteit 3 & 4 (Medium/Laag): Respons binnen kantoortijden (NBD). Naast deze responstijden (TTO – Time to Own) verwacht de opdrachtgever dat inschrijvers in hun aanbieding voorstellen doen voor: MTTD (Mean Time to Detect): De streeftijd tussen het optreden van een event en de detectie in het SOC. MTTR (Mean Time to Respond/Remediate): De gemiddelde tijd tot actie is ondernomen om de dreiging te isoleren. De definitieve KPI's worden in overleg met de geselecteerde opdrachtnemer vastgesteld, waarbij de ingediende voorstellen uit de inschrijving als minimum dienen.

128	Bijlage 5 Programma van Eisen	9	11.10	Wat is de escalatieprocedure bij kritieke incidenten? Heeft de gemeente zelf over 24/7 piket of stand-by bij kritieke incidenten?		We maken met elkaar afspraken over mandaat bij kritieke incidenten. De gemeente heeft geen 24/7-piket, maar moet wel op de hoogte worden gebracht wanneer een gemandateerde opdracht is uitgevoerd.
129	Bijlage 5 Programma van Eisen	Algemeen	12.1	Kunt u een Microsoft Visio-diagram van de huidige omgeving beschikbaar stellen?	Voorkomen dat er een klant netwerk gemaakt moet worden	Vanuit veiligheidsoverwegingen (bedrijfsgevoelige informatie) deelt aanbestedende dienst deze informatie niet op TenderNed.
130	Bijlage 5 Programma van eisen	9	Pve 12.2	In paragraaf 12.2 van bijlage 5 (Programma van Eisen) wordt aangegeven dat de opdrachtnemer bij inschrijving moet aangeven welke minimale vereisten de opdrachtgever moet voldoen om de SIEM-oplossing te realiseren. Kunt u toelichten hoe deze informatie wordt gebruikt in het beoordelingskader en bij de gunningscriteria, bijvoorbeeld of deze informatie een rol speelt bij de beoordeling van de kwaliteit van de aanbieding of bij de toetsing van de geschiktheid van de opdrachtnemer?	Deze vraag zorgt voor helderheid over het gebruik van de informatie in het beoordelingsproces en voorkomt dat je onterecht wordt uitgesloten door een onduidelijke interpretatie van de documenten.	Per abuis is aangegeven dat deze informatie aangeleverd moet worden bij inschrijving. Dit moet zijn bij voorlopige gunning, door de voorlopig gegunde partij.
131	Programma van Eisen		11.10 Afhandelingstijden	In 11.10 wordt gesproken over afhandelingstijden. Kunt u bevestigen dat deze afhandelingstijden uitsluitend betrekking hebben op SOC-dienstverlening (detectie, analyse en escalatie van security events) en niet op het volledig oplossen van security breaches of grootschalige incidenten?		De aanbestedende dienst bevestigt dat de afhandelingstijden onder eis 11.10 primair betrekking hebben op de kernactiviteiten van het SOC: de tijdige detectie, triage, analyse en de initiële respons (zoals het isoleren van een besmet endpoint). Voor het volledig herstellen van de bedrijfsvoering na een grootschalige security breach (remediation en recovery) gelden geen vaste afhandelingstijden binnen deze eis, aangezien de duur hiervan afhankelijk is van de aard en omvang van het incident. Wel wordt van de opdrachtnemer verwacht dat zij gedurende het gehele incidentonderzoek de regie voert over de technische analyse en de opdrachtgever proactief adviseert over de te nemen herstelstappen.
132	Programma van Eisen		11.5 Nederlandstalige helpdesk	In 11.5 wordt een Nederlandstalige helpdesk benoemd. Kunt u bevestigen dat deze helpdesk betrekking heeft op meldingen en vragen over door het SOC gedetecteerde security events, en dat deze helpdesk uitsluitend tijdens kantooruren beschikbaar is en geen		De aanbestedende dienst maakt voor de bereikbaarheid van de helpdesk het volgende onderscheid: Functionele en technische vragen: Voor algemene vragen over de dienstverlening, rapportages of de werking van de portal is bereikbaarheid tijdens kantooruren (08:30 – 17:00 uur) akkoord. Security-incidenten (P1/P2): Voor de afhandeling van en communicatie over gedetecteerde security-events met een hoge prioriteit dient de opdrachtnemer 24/7 bereikbaar en beschikbaar te zijn voor de opdrachtgever, conform de afgesproken respons-SLA. De helpdesk dient dus voor kritieke meldingen ook buiten kantooruren als aanspreekpunt te fungeren.
133	Bijlage 5 Programma van eisen	9	Pve 11.7	In het Programma van Eisen, eis 11.7, wordt aangegeven dat het concept SLA moet worden ingediend bij inschrijving. Kunt u toelichten hoe het concept SLA wordt beoordeeld in het kader van het beoordelingskader en de gunningscriteria, bijvoorbeeld of er specifieke eisen of criteria zijn waaraan het concept SLA moet voldoen en hoe deze beoordeling invloed heeft op de totale beoordeling van de inschrijving? Is het indienen van het concept SLA puur ter kennisgeving, of heeft dit een invloed op de beoordeling en gunning van de inschrijving?	Deze vraag zorgt voor helderheid over het gebruik en de beoordeling van het concept SLA en voorkomt dat je onterecht wordt uitgesloten door een onduidelijke interpretatie van de documenten.	Per abuis is aangegeven dat de concept-SLA bij inschrijving moet worden aangeleverd. Dit moet zijn: bij voorlopige gunning, door de voorlopig gegunde partij. Verder is aangegeven dat bij definitieve gunning een definitieve versie van de SLA wordt vastgesteld. Dit moet zijn: de definitieve versie wordt, in samenspraak, na definitieve gunning vastgesteld.
134	Bijlage 5 Programma van eisen	9	Pve 11.7	In het Programma van Eisen, eis 11.7, wordt aangegeven dat het concept SLA moet worden ingediend bij inschrijving. Kunt u toelichten op welk niveau het concept SLA moet worden ingediend, bijvoorbeeld of dit een voorlopig concept is of een zo goed als definitief SLA dat direct kan worden toegepast na gunning?	Deze vraag zorgt voor helderheid over het niveau en de beoordeling van het SLA in het kader van de voorlopige gunning en voorkomt dat je onterecht wordt uitgesloten door een onduidelijke interpretatie van de documenten.	Het bij inschrijving in te dienen SLA betreft een concept-SLA. Dit document heeft een indicatief en voorlopig karakter. Het doel van het concept-SLA is om inzicht te geven in de wijze waarop de inschrijver doorgaans invulling geeft aan SLA-afspraken binnen vergelijkbare dienstverlening. Hoe completer en concreter het concept is, des te efficiënter kan worden toegewerkt naar een definitieve SLA. Zie ook antwoord op vraag 133.
135	Bijlage 5 Programma van eisen	9	Pve 11.7	In het Programma van Eisen, eis 11.7, wordt aangegeven dat het concept SLA moet worden ingediend bij inschrijving. Verzoeken wij u vriendelijk om het SLA op de vragen bij voorlopige gunning aan de partij die de opdracht voorlopig gegund heeft gekregen te toetsen, in het kader van lastenverlichting. Graag uw akkoord.	Wij stellen deze vraag om te voorkomen dat we onterecht worden belast met het uitwerken van een SLA op een niveau dat pas na gunning relevant is, en om te waarborgen dat het SLA pas daadwerkelijk wordt beoordeeld als de opdracht daadwerkelijk wordt gegund, conform het principe van lastenverlichting en proportioneelheid.	Zie antwoord op vraag 133.
136	Bijlage 5 Programma van eisen	9	Pve 11.7	In het Programma van Eisen, eis 11.7, wordt aangegeven dat het concept SLA moet worden ingediend bij inschrijving. Kunt u bevestigen dat het SLA vertrouwelijk wordt behandeld en dat er geen gebruik wordt gemaakt van de SLA's van alle inschrijvers om een “beste mix” samen te stellen?	Deze vraag zorgt voor helderheid over de vertrouwelijke behandeling van het SLA en voorkomt dat je onterecht wordt uitgesloten door een onduidelijke interpretatie van de documenten.	Zie antwoord op vraag 133.
137	Bijlage 5 Programma van Eisen	Algemeen	13.3	Is het mogelijk om de dienstverlening jaarlijks vooraf te factureren? Dit kan een gunstige invloed hebben op de prijs, aangezien de dienstverlening in dat geval niet tussentijds wordt afgeschaald en voor een vaste periode (bijvoorbeeld vier jaar) doorloopt.	Ten gunste van publieke gelden	Niet akkoord.
138	Bijlage 6 Concept Overeenkomst	2	Artikel 4.2	Inschrijver stelt voor om aan de bepaling toe te voegen dat de andere partij gerechtigd is om tot ontbinding over te gaan in het geval dat de tekortschietende partij, ondanks schriftelijke ingebrekestelling inhoudende een of meerdere concrete redenen waarin zij tekortschiet, nalaat om het gebrek binnen de in redelijke termijn te herstellen. Kan de gemeente daarmee akkoord gaan?	De bepaling is nu zo opgesteld dat in het geval van toerekenbaar tekortschieten geen ingebrekestelling zou zijn vereist voordat tot ontbinding mag worden overgegaan. Leverancier verwijst in dat kader ook naar artikel 24.10 GIBIT 2023.	Niet akkoord. Graag wijzen we u op artikel 4.1 van de conceptovereenkomst. In het geval één van de partijen tekortschiet in de nakoming van de overeenkomst, zal de andere partij hem om die reden in gebreke stellen, tenzij nakoming van de betreffende verplichtingen reeds blijvend onmogelijk is. Daarbij dient de ingebrekestelling de nalatige partij een redelijke termijn te bieden om alsnog zijn verplichtingen na te komen. De nalatige partij is in verzuim indien nakoming reeds blijvend onmogelijk is, of de redelijke termijn is verstreken. Wanneer sprake is van verzuim, kan de andere partij de overeenkomst ontbinden conform artikel 4.2 van de conceptovereenkomst.
139	Bijlage 6 Concept Overeenkomst	3	Artikel 4.3	Leverancier verzoekt deze bepaling buiten toepassing te verklaren en uit de overeenkomst te verwijderen.	Leverancier acht een dergelijke generieke ontbindingsgrond zonder enige vorm van ingebrekestelling niet redelijk, nu deze bepaling verder gaat dan op grond van de GIBIT 2023 proportioneel wordt geacht. Leverancier levert haar dienstverlening aan veel grote en middelgrote overheden en een dergelijke bepaling maakt eigenlijk nooit onderdeel uit van soortgelijke contracten.	Akkoord.

140	Conceptovereenkomst		Artikel 5	Geheel vervangen door: 5.1 Een partij bij deze overeenkomst is aansprakelijk: a. Voor aanspraken op schadevergoeding ten gevolge van dood of lichamelijk letsel; en/of b. Indien de andere partij schade lijdt als gevolg van opzet of grove schuld; en/of c. In geval deze in de uitvoering van de overeenkomst een intellectuele eigendomsrecht schendt; en/of d. Voor zaakschade. 5.2 De aansprakelijkheid van een Partij bij deze overeenkomst is voor zaakschade beperkt tot 500.000 EUR per gebeurtenis met een absoluut maximum van 1.000.000 EUR per jaar. Een reeks van opeenvolgende gebeurtenissen wordt aangemerkt als één gebeurtenis. 5.3 Geen der Partijen is aansprakelijk voor gevolgschade, waaronder wordt verstaan dat aansprakelijkheid voor andere schade dan genoemd in lid 1 van dit artikel uitdrukkelijk uitgesloten is.	Het door u gedane voorstel is disproportioneel en niet marktconform. Het bevat een te ruim schadebegrip. Bent u bereid om het door Opdrachtnemer hiernaast gedane tekstvoorstel over te nemen dan wel een alternatief voorstel te formuleren waarmee tegemoet wordt gekomen aan de wensen van Opdrachtnemer?	Niet akkoord.
141	Bijlage 6 Concept Overeenkomst	3	Artikel 5.1	Is de gemeente derhalve bereid om indirecte schade uit te sluiten en de bepaling als volgt te wijzigen? "De partij die toerekenbaar tekortschiet in de nakoming van zijn verplichtingen of jegens de ander onrechtmatig handelt, is tegenover de andere partij enkel en alleen aansprakelijk voor de door deze aldus geleden en/of te lijden directe schade. Onder directe schade wordt uitsluitend verstaan: (i) de kosten die Opdrachtgever redelijkerwijs heeft moeten maken om de tekortkoming van Leverancier te herstellen of op te heffen, zodat de prestatie van Leverancier wel aan de Overeenkomst beantwoordt; (ii) redelijke kosten voor het langer operationeel houden van de oude producten of systemen van Opdrachtgever, verminderd met de besparingen; (iii) schade aan zaken van de gemeente en personen, die rechtstreeks het gevolg is van het toerekenbaar tekortschieten; en (iv) redelijke kosten ter voorkoming of beperking van zulke schade en redelijke kosten ter vaststelling van de oorzaak en omvang daarvan. Elke aansprakelijkheid voor alle andere vormen of categoriën van schade is uitgesloten."	In de IT-branche is het gebruikelijk dat er onderscheid wordt gemaakt tussen directe en indirecte schade (zoals gederfde winst, vertragingsschade, omzetverlies, gemiste besparingen of reputatieschade), waarbij Inschrijver uitsluitend aansprakelijkheid wenst te accepteren voor directe schade.	Niet akkoord. De aanbestedende dienst sluit aan bij de aansprakelijkheidsbepalingen uit het Burgerlijk Wetboek. In het Burgerlijk Wetboek wordt ook geen onderscheid gemaakt tussen directe en indirecte schade.
142	Bijlage 6 Concept Overeenkomst	3	Artikel 5.3	Leverancier verzoekt deze bepaling buiten toepassing te verklaren en uit de overeenkomst te verwijderen.	Leverancier acht een dergelijke generieke vrijwaring zonder specifiek aantoonbaar zwaarwegend belang niet redelijk, nu deze bepaling verder gaat dan op grond van de GIBIT 2023 proportioneel wordt geacht. Leverancier levert haar dienstverlening aan veel grote en middelgrote overheden en een dergelijke bepaling maakt eigenlijk nooit onderdeel uit van soortgelijke contracten.	Niet akkoord. Het is niet redelijk dat een partij de schade van derden dient te vergoeden die voortvloeit uit een toerekenbare tekortkoming van de wederpartij.
143	Conceptovereenkomst	3	5.3	Wij verzoeken u het artikel te wijzigen in: "De partij die in zijn verplichtingen tekortschiet vrijwaart de andere partij voor eventuele aanspraken van derden op vergoeding van de schade: a. in geval deze voortvloeien uit toerekenbaar toegebracht letsel of de dood en/of; b. in geval van schending van intellectuele eigendomsrechten van die derden en/of; c. in geval deze voortvloeien uit een toerekenbare schending van wet- en regelgeving op het terrein van de bescherming van persoonsgegevens."	Het is gebruikelijk dat in geval van een tekortkoming de schade van de wederpartij/opdrachtgever wordt vergoed en niet tevens de schade van derden, tenzij in de hiernaast genoemde gevallen. De opdrachtnemer is, anders dan de opdrachtgever, immers niet in de positie aansprakelijkheid voor schade van die derden uit te sluiten of te beperken en kan daarvoor dan ook geen vrijaring verlenen.	Zie antwoord op vraag 142.
144	Conceptovereenkomst		Artikel 6.c	Artikel schrappen	Het wettelijke systeem voor verrekening is afdoende.	Niet akkoord.
145	Bijlage 6 Concept Overeenkomst	3	Artikel 6.1	Kan de gemeente op grond van de toelichting van de Leverancier toelichten wat het belang en de reikwijdte is van deze bepaling en de bepaling op grond daarvan verduidelijken of aanpassen?	Leverancier kan deze bepaling niet goed plaatsen. Afspraken die contactpersonen maken over de uitvoering van de overeenkomst, zijn in de praktijk bijna altijd een aanvulling op de overeenkomst, althans zien op de feitelijke invulling en uitvoering van de overeenkomst. Dergelijke afspraken zijn wat Leverancier betreft ook in zekere vorm juridisch bindend.	Artikel 6.1 van de conceptovereenkomst ziet niet op de feitelijke invulling en uitvoering van de overeenkomst. Het artikel heeft betrekking op aanvullingen of wijzigingen van de overeenkomst inclusief alle bijlagen. Derhalve ziet de aanbestedende dienst geen reden om dit artikel aan te passen.
146	Bijlage 6 Concept Overeenkomst	3	Artikel 6.3	Leverancier stelt voor om toe te voegen dat het gaat om wezenlijke wijzigingen "in de zin van de Aanbestedingswet".		Akkoord.
147	Conceptovereenkomst		Artikel 12.a	Toevoegen aan bestaand artikel de tekst: "Alle (intellectuele) eigendomsrechten, auteursrechten, gebruiksrechten en andere rechten ten aanzien van programmatuur of ontwerpen die rustten bij Partijen of derden vooraf gaand aan het sluiten van deze overeenkomst, behoren bij uitsluiting toe aan die rechthebbende, alsmede alle aanpassingen, bewerkingen of uitbereidingen daarvan."	Hierdoor wordt een duidelijke scheiding aangelegd tussen bestaande Intellectuele Eigendomsrechten voor het sluiten van de overeenkomst en Intellectuele Eigendomsrechten die daarna ontstaan tijdens de loop van de overeenkomst.	Het is onduidelijk op welk artikel uw vraag betrekking heeft. De conceptovereenkomst bevat namelijk geen artikel 12a. Wij verzoeken u de vraag te verduidelijken en in te dienen t.b.v. Nvl 2.
148	Conceptovereenkomst		Artikel 12.b en c	Artikel 12.b en c schrappen	Deze overeenkomst tussen partijen heeft niet tot doen de overdracht van enige IE rechten. Deze leden zijn in alle gevallen onacceptabel voor aanbieder, zulks met uitzondering van die gevallen waarbij op grond van de Auteurswet de IE rechten toe zouden komen aan de Gemeente. Indien er sprake is van 'nieuwe' IE en deze onder leiding en toezicht van de Gemeente tot stand zou komen ('echte maatwerk software'), zouden de IE rechten toe kunnen komen aan Gemeente Lisse. Aanbieder vraagt zich in goede gemoede af waarom de Gemeente streeft naar het verkrijgen van IE rechten terwijl dit niet behoort tot diens kerndoelen; dit is wel het geval bij aanbieder (en diens concurrenten). Alle regelingen betreffende standaardsoftware zijn afhankelijk van de door de rechthebbende van deze software gebruikelijk gehanteerde licentievoorwaarden. Aanbieder kan 'niet meer weggeven dan zij zelf heeft'. Op het gebruik van de software zijn de standaardlicentievoorwaarden van de rechthebbende van toepassing. Tussen de rechthebbende en de Gemeente zal een directe overeenkomst tot stand komen.	De conceptovereenkomst heeft geen artikel 12. Het is niet duidelijk waar u naar verwijst.

149	Bijlage 8 - SROI			Opdrachtgever geeft aan dat de SROI-invulling 'Direct toe te rekenen moet zijn aan de opdracht'. In verband met hooggeschoold en specialistisch werk, zowel binnen als in relatie tot de gegunde opdracht, is het niet altijd mogelijk om aan Social Return invulling te geven binnen de opdracht. Is het toegestaan om de Social Return verplichting binnen de bredere bedrijfsvoering van Opdrachtnemer in te vullen?		Het is toegestaan om de verplichting binnen de bredere bedrijfsvoering van opdrachtnemer te laten plaatsvinden.
150	Bijlage 8 - SROI			Inschrijver begrijpt dat Opdrachtgever werkt met het systeem WIZZR ter controle van afspraken over Social Return. Inschrijver is van mening dat zij in strijd met de AVG handelt als zij gegevens van medewerkers op persoonsniveau aanlevert (al dan niet via WIZZR), omdat de Social Return afspraken ook op een andere manier kunnen worden gecontroleerd, zonder (bijzondere) persoonsgegevens te delen. Het is m.a.w. niet noodzakelijk om (gezondheids)gegevens op persoonsniveau te delen via WIZZR ter controle van Social Return afspraken en als Inschrijver dit wel zou doen handelt zij in strijd met de AVG (toestemming is geen grond bij bijzondere personeelsgegevens). Staat de Gemeente open voor alternatieve oplossingen waarbij de Social Return afspraken gecontroleerd worden, zoals bijvoorbeeld het aanleveren van een verklaring van een onafhankelijke auditor, al dan niet via het systeem WIZZR? Verwijzen naar een privacy-protocol is daarbij voor ons geen passend, inhoudelijk antwoord, omdat we anders aankijken tegen de wijze waarop wij gegevens van onze medewerkers (niet) kunnen delen en wij daarom willen kijken met elkaar naar een andere werkwijze waarbij dit niet nodig is.		Het delen van persoonsgegevens is onder de AVG toegestaan; daarover verschillen we dan van mening. Wanneer u de SROI-opgave wilt verantwoorden via kandidateninzet, dan willen we daar een onderbouwing van kunnen zien. Denk bijvoorbeeld aan de overeenkomst die hoort bij een stage, een leerwerktraject, een proefplaatsing o.i.d. Wanneer het gaat om mensen die vanuit een uitkeringssituatie bij u aan het werk zijn/gaan, dan kan – naast de arbeidsovereenkomst – ook volstaan worden met bijvoorbeeld correspondentie met de uitkeringsinstantie. Daaruit blijkt in welke SROI-doelgroep (bouwblok) de betreffende persoon valt, zodat er een juiste SROI-waarde aan de invoer gekoppeld kan worden. Er worden niet meer persoonsgegevens gevraagd dan nodig. Privacygevoelige informatie kunt u desnoods zwartlakken. Die onderbouwing kunt u in Wizzr doen. Buiten Wizzr om de onderbouwing verzorgen is zeker bespreekbaar. NB: Behalve kandidateninzet heeft u ook andere mogelijkheden om uw SROI in te vullen. Sociale inkoop en/of maatschappelijke activiteiten behoren evengoed tot de mogelijkheden.
151	Bijlage 9 verwerkersovereenkomst	1 en 2	3.1	Artikel 3.1 stelt dat Verwerker uitsluitend handelt op basis van schriftelijke instructies van Verwerkingsverantwoordelijke. Kan worden verduidelijkt hoe dit zich verhoudt tot de rol van opdrachtnemer als SOC-dienstverlener die proactief detecteert, analyseert en adviseert, zonder dat hiervoor telkens expliciete instructies nodig zijn?	Om te voorkomen dat de verwerkersovereenkomst de uitvoering van de SOC-dienstverlening onnodig beperkt of vertraagt.	In de verwerkersovereenkomst is duidelijk aangegeven met welk(e) doel(en) gegevens worden verwerkt (en waarom). Hierdoor zou de uitvoering van de dienstverlening niet onnodig beperkt of vertraagd moeten worden. Het verwerken binnen de scope van de verwerkersovereenkomst heeft als doel dat uitsluitend de nodige gegevens worden verwerkt (met zo min mogelijk benodigde persoonsgegevens en op basis van subsidiariteit en proportionaliteit).
152	Bijlage 9 - Verwerkersovereenkomst		art. 4.2.	Is opdrachtgever bereid aan dit artikel toe te voegen dat: -Een controle niet wordt verricht door een concurrent van Opdrachtnemer; -Dat de partij die de controle uitvoert gehouden is aan geheimhoudingverplichtingen welke tenminste vergelijkbaar zijn met die welke zijn opgenomen in deze voorwaarden; -Een controle altijd wordt uitgevoerd op basis van een vooraf tussen partijen overeengekomen auditplan -De resultaten en de vaststelling van de controle en de eventueel op basis daarvan uit te voeren acties tussen partijen worden besproken en overeengekomen tussen partijen; -Opdrachtnemer minimaal 10 werkdagen van tevoren schriftelijk op de hoogte wordt gesteld van de controle.		Niet akkoord.
153	Bijlage 9 verwerkersovereenkomst	2	4.2	Kan worden verduidelijkt wat wordt verstaan onder "tekortkomingen van niet ondergeschikte aard" en op welke wijze objectief wordt vastgesteld wanneer auditkosten voor rekening van Verwerker komen?	Om interpretatieverschillen en onvoorziene financiële risico's voor Verwerker te voorkomen.	Dit is wanneer er sprake is van een serieuze , wezenlijke schending van de overeenkomst. Het gaat niet om kleine foutjes of onbeduidende afwijkingen, maar om tekortkomingen die voldoende ontbinding van de overeenkomst rechtvaardigen.
154	Bijlage 9 verwerkersovereenkomst	2	4.2	Kan worden bevestigd dat het gebruik van cloudleveranciers die data binnen de EU/EER opslaan, maar onderdeel zijn van een internationale groep, niet automatisch wordt aangemerkt als verwerking buiten de EER?	Om helderheid te krijgen over de praktische interpretatie van verwerking buiten de EER bij gangbare cloud- en securitydiensten.	Het enkele feit dat een cloudleverancier onderdeel is van een internationale groep leidt niet automatisch tot een "doorgifte naar een derde land" onder de AVG, zolang de data binnen de EU/EER blijft en niet toegankelijk wordt gemaakt voor een partij buiten de EER.
155	Bijlage 9 verwerkersovereenkomst	2	4.5	Kan worden bevestigd dat de algemene toestemming voor subverwerkers betekent dat wijzigingen in subverwerkers niet vooraf gaand hoeven te worden goedgekeurd, maar enkel tijdig worden gemeld?	Om flexibiliteit in de dienstverlening te behouden en onnodige vertragingen te voorkomen.	Bij toekomstige wijzigingen dient dit voortijdig te worden gemeld en waar nodig opnieuw te worden afgewogen.
156	Bijlage 9 verwerkersovereenkomst	2	4.7	Kan worden verduidelijkt of medewerking aan DPIA's beperkt blijft tot redelijke inspanningen binnen de scope van de opdracht en geen open-einde verplichting vormt?	Om de inzet en verantwoordelijkheid van Verwerker af te bakenen.	Het verlenen van medewerking aan DPIA's is een open einde verplichting. Als inspanningsverplichting geldt dat er redelijke inspanning mag worden geeist om te komen afronding van de DPIA.
157	Bijlage 9 verwerkersovereenkomst	3	5.1	Kan worden bevestigd dat de meldtermijn van 24 uur geldt vanaf het moment dat een inbreuk met redelijke zekerheid is vastgesteld, en niet bij een eerste vermoeden zonder feitelijke onderbouwing?	Om overrapportage en onnodige escalaties te voorkomen.	De aanbestedende dienst bevestigt dat de meldtermijn van 24 uur ingaat op het moment dat een beveiligingsincident of datalek door de opdrachtnemer is geconstateerd. Onder constatering wordt verstaan: het moment waarop de opdrachtnemer op basis van een eerste triage of analyse heeft vastgesteld dat er sprake is van een daadwerkelijke onregelmatigheid die de integriteit, vertrouwelijkheid of beschikbaarheid van gegevens (mogelijk) heeft aangetast. Hoewel een gedetailleerde feitelijke onderbouwing op dat moment nog niet volledig hoeft te zijn, mag de melding niet worden opgehouden in afwachting van een definitief onderzoeksrapport. Een eerste melding van een 'vermoedelijk' ernstig incident is essentieel om de wettelijke 72-uurs termijn richting de Autoriteit Persoonsgegevens niet in gevaar te brengen.
158	Bijlage 9 - Verwerkersovereenkomst		art 5.1	In de AVG wordt geen specifieke termijn vermeld waarbinnen de Verwerker de Verwerkingsverantwoordelijke moet waarschuwen, behalve dat hij dit "zonder onredelijke vertraging" doet en dient de Verwerkingsverantwoordelijke pas een melding te doen binnen 72 uur nadat deze daarvan in kennis is gesteld. De termijn van 24 uur is niet altijd realistisch en niet in alle gevallen proportioneel vanwege het feitenonderzoek, contact met eventuele sub-Verwerkers en een impactanalyse. Bent u bereid om aan te sluiten bij de tekst van de AVG (dus de tekst "onmiddellijk, maar in ieder geval binnen 24 uur" te vervangen door "zonder onredelijke vertraging, maar in ieder geval binnen 72 uur")?		De aanbestedende dienst gaat niet akkoord met het verlengen van de meldtermijn naar 72 uur. De wettelijke termijn van 72 uur uit de AVG geldt voor de melding van de verwerkingsverantwoordelijke (de gemeente) aan de Autoriteit Persoonsgegevens. Om deze termijn te kunnen halen, is het essentieel dat de opdrachtnemer de gemeente onverwijld, maar uiterlijk binnen 24 uur na constatering, informeert. Deze 24-uurs termijn biedt de gemeente de noodzakelijke ruimte voor eigen afwegingen, bestuurlijke afstemming en de uiteindelijke melding aan de toezichthouder. De opdrachtnemer wordt niet geacht binnen deze 24 uur het volledige feitenonderzoek af te ronden, maar dient de beschikbare informatie te delen zodat de gemeente aan haar wettelijke zorgplicht kan voldoen.
159	Bijlage 9 - Verwerkersovereenkomst		art. 5.3	Een dergelijk overzicht omvat mogelijk ook intern vertrouwelijke informatie. Inschrijver gaat er vanuit dat Verwerkingsverantwoordelijke uitsluitend inzage verlangt in die incidenten die rechtstreeks betrekking hebben op Verwerkingsverantwoordelijke, kunt u dat bevestigen?		De aanbestedende dienst bevestigt dit.
160	Bijlage 9 verwerkersovereenkomst	3	5.3	Kan worden verduidelijkt in welke mate Verwerkingsverantwoordelijke inzage krijgt in het dataleklogboek, en of dit beperkt blijft tot incidenten die betrekking hebben op deze opdracht?	Ter bescherming van vertrouwelijkheid en scheiding tussen klanten.	Een datalek bij verwerkingsverantwoordelijken wordt behandeld bij de verantwoordelijken zelf. Een datalek waarbij Verwerker is betrokken maar wordt gemeld en behandeld bij verwerkingsverantwoordelijke levert waar nodig vragen aan Verwerker op (telefonisch overleg), maar blijft uitsluitend beperkt tot incidenten die betrekking hebben op de opdracht.

161	Bijlage 9 verwerkersovereenkomst	3	6.1	Kan worden bevestigd dat eventuele aansprakelijkheidsbeperkingen uit de Hoofdovereenkomst onverkort van toepassing zijn en niet worden uitgebreid via de verwerkersovereenkomst?	Om te voorkomen dat via de verwerkersovereenkomst aanvullende aansprakelijkheid ontstaat	De aanbestedende dienst bevestigt dit.
162	Bijlage 9 verwerkersovereenkomst	3	7.3	Kan worden verduidelijkt binnen welke termijn en op welke wijze teruggave en/of wissing van persoonsgegevens plaatsvindt, en of hierbij rekening wordt gehouden met wettelijke bewaarplichten en back-upcycli?	Om uitvoerbaarheid en compliance met andere wettelijke verplichtingen te borgen.	Artikel 7.3 bestaat niet in bijlage 9.
163	Bijlage 9 - Verwerkersovereenkomst		bijlagen (en artikelen die daaraan refereren)	De inhoud van de bijlagen (waaronder de inschakeling van sub-verwerkers en eventuele verwerkingen buiten de EER en) is afhankelijk van hoe de diensten voor Opdrachtgever, naar aanleiding van deze aanbesteding, uiteindelijk ingevuld gaan worden. Het is daarom op voorhand niet mogelijk hier een definitieve invulling aan te geven. Is Opdrachtgever bereid om na gunning nader in overleg te treden over de inhoud van deze bijlagen?		Ja, daar gaat aanbestedende dienst mee akkoord.
164	Bijlage 10 - Controlelijst volledigheid inschrijving + Bijlage 5 Programma van eisen	9	Pve 12.2	In paragraaf 12.2 van bijlage 5 (Programma van Eisen) wordt aangegeven dat de opdrachtnemer bij inschrijving moet aangeven welke minimale vereisten de opdrachtgever moet voldoen om de SIEM-oplossing te realiseren. a) Kunt u bevestigen of deze uitwerking wel of niet moet worden opgenomen bij onze inschrijving, aangezien deze uitwerking niet in de controlelijst van de inschrijving is opgenomen? b) Indien deze uitwerking wel moet worden ingediend, verzoeken wij u vriendelijk om een nieuwe controlelijst	Deze vraag zorgt voor helderheid over de verplichtingen bij de inschrijving en voorkomt dat je onterecht wordt uitgesloten door een onduidelijke interpretatie van de documenten.	Zie antwoord op vraag 130.
165	Bijlage 11	Algemeen	Algemeen	Bevestigt u dat het vooraf niet onvoorwaardelijk akkoord gaan met de gehele GIBIT 2023 een directe uitsluiting inhoudt?	Dit ter verduidelijking van het aanbestedingsproces, daar dit mist in Bijlage 10.	Inschrijvers dienen onvoorwaardelijk akkoord te gaan met hetgeen is opgenomen in de aanbestedingsdocumenten en antwoorden op de Nota van Inlichtingen. Het niet akkoord gaan leidt tot uitsluiting.
166	Bijlage 11 inkoopvoorwaarden GIBIT	4-6	GIBIT 2023, Art 1.30 Begrippen	Bent u akkoord met het volgende beperkende formulering van dit artikel: "Overeengekomen gebruik: het beoogde gebruik van de ICT Prestatie door de Opdrachtgever, zoals kenbaar gemaakt aan de Inschrijver op het moment van het sluiten van de Overeenkomst"?	Verduidelijking of aanpassing op artikel	Niet akkoord. Artikel 3.5 bepaalt reeds dat de verplichting beperkt is tot de door opdrachtgever verstrekte gegevens.
167	Inkoopvoorwaarden GIBIT-2023		Artikel 2.5 en art 1.2. Concept Overeenkomst.	Leverancier stelt voor om de rangorde van de GIBIT 2023 aan te houden omdat die ook veel meer recht doet aan relevante bijlagen zoals EULA, SLA, exit plan en implementatieplan. Is de gemeente bereid om de rangorde in de overeenkomst daarop aan te passen, dan wel deze te verwijderen?	Dit artikel bevat een regeling tussen de Overeenkomst, bijlagen bij de overeenkomst (zoals SLA, implementatieplan, exit-plan), en ook de EULA, waarbij deze bijlagen juist prevaleren boven de Overeenkomst. Deze bepaling sluit naar overtuiging van Leverancier beter aan bij de deze uitvraag en de te sluiten overeenkomst dan de rangorde als vastgelegd in art. 1.2 van de conceptovereenkomst.	Niet akkoord. De onderstaande rangorde is van toepassing: I.Overeenkomst; II. SLA en implementatieplan; III. Verwerkersovereenkomst; IV. Inhoud nota van inlichtingen 2 d.d. datum; V. Inhoud nota van inlichtingen 1 d.d. datum; VI. Inhoud uitnodiging tot inschrijving ten behoeve van de openbare procedure d.d. datum; VII. Algemene inkoopvoorwaarden GIBIT 2023; VIII. Inhoud inschrijving opdrachtnemer d.d. datum. Artikel 1.2 van de overeenkomst wordt hierop aangepast.
168	Bijlage 11 inkoopvoorwaarden GIBIT	6	GIBIT 2023, Art 2.5 Toepasselijkheid	Het belang van de overeenkomsten tussen partijen zou prioriteit moeten krijgen boven algemene voorwaarden die van toepassing zijn op alle partijen. Bent u bereid om de specifieke overeenkomst (sub iii) en eventuele aanvullende overeenkomsten (sub ii) te laten prevaleren boven de inkoop- en licentievoorwaarden, gezien het feit dat deze laatste algemeen van toepassing zijn? Wat is uw standpunt ten aanzien van deze hiërarchie in uw specificatie?	Verduidelijking of aanpassing op artikel	Niet akkoord. Zie antwoord op vraag 167.
169	GIBIT 2023		Artikel 3 lid 2 i)	Onder (i) In plaats van "Doelstellingen" beter om te spreken over bijvoorbeeld "Het door Opdrachtgever beoogde gebruik van de Prestatie, zoals dat door de Opdrachtgever kenbaar is gemaakt."	Doelstellingen kunnen tegenstrijdig zijn. Hier ligt een taak voor de Opdrachtgever om de leverancier daarover te informeren. Kunt u hiermee instemmen?	Artikel 3 lid 2 onder i wordt vervangen door de volgende bepaling: "Het door opdrachtgever beoogde gebruik van de ICT-prestatie, zoals dat door de opdrachtgever kenbaar is gemaakt of voor leverancier bekend hoorde te zijn."
170	GIBIT 2023		Artikel 3 lid 3	Graag de volgende woorden toevoegen aan artikel 3 lid 3: "en Opdrachtgever zal ook (proactief) de Leverancier tijdig van adequate informatie voorzien."	Goede informatieverschaffing door Opdrachtgever is essentieel voor goede overeenstemming tussen partijen over de ICT-Prestatie. Kunt u hiermee instemmen?	Akkoord.
171	Bijlage 11 inkoopvoorwaarden GIBIT	7	GIBIT 2023, Art 3.4 Totstandkoming overeenkomst	Voor het kunnen uitvoeren van een risicoanalyse volgens artikel 3.4 (ii) van de GIBIT is opdrachtnemer afhankelijk van de door opdrachtgever verstrekte informatie over de IT-infrastructuur, processen en gebruikte software. Dit artikel benadrukt dat de vorm en inhoud van de risicoanalyse en beheersmaatregelen niet specifiek zijn bepaald. (i) Kan opdrachtgever akkoord gaan met het verwijderen van de vermeldingen over de risicoanalyse? (ii) Indien niet, kan gedetailleerd worden beschreven welke aspecten moeten worden geanalyseerd/beheerst, zodat het aanbod beter op maat kan worden gemaakt? (iii) Heeft opdrachtgever recentelijk zelf een risicoanalyse uitgevoerd? Indien ja, kunnen de bevindingen gedeeld worden met opdrachtnemer om een beter inzicht te verschaffen en opdrachtnemer in staat te stellen potentiële risico's te identificeren die relevant zijn voor de aangeboden dienst?	Verduidelijking of aanpassing op artikel	Niet akkoord. De risicoanalyse zoals verplicht conform art. 3.4 omvat onder meer het beoordelen in welke mate een risico wordt voorzien met het invoeren van de ICT-prestatie binnen het applicatielandschap van opdrachtgever. Conform art. 3.5 is deze verplichting beperkt tot de informatie die opdrachtgever bij de aanbesteding heeft gegeven. Uit deze informatie blijkt op/waar de geleverde ICT-prestatie staat/aangeboden moet worden en op welke wijze hier gebruik van moet kunnen worden gemaakt. Juist de aanbieder weet welke (systeem)eisen er zijn om haar eigen ICT-prestatie goed te kunnen gebruiken. Indien uit de geleverde informatie reeds inzichtelijk was dat het applicatielandschap van opdrachtgever onvoldoende aan deze (systeem)eisen voldoet, dan had dit door de aanbieder aangegeven moeten worden om te voorkomen dat opdrachtgever achteraf met financieel nadelige consequenties geconfronteerd wordt (en wellicht daarmee ook niet met de juiste partij een overeenkomst heeft gesloten n.a.v. de aanbesteding en de daarvoor ontvangen aanbiedingen).
172	Gibit2023		3.4 (ii)	Voor het kunnen maken van een risicoanalyse (GIBIT art. 3.4 (ii)) is opdrachtnemer afhankelijk van de door opdrachtgever verstrekte informatie en hoe het een en ander op het gebied van IT en samenhangende processen is ingericht en welke software al wordt gebruikt. Bovendien wordt in dit artikel de vorm en inhoud van de risicoanalyse en beheersmaatregelen onbepaald. (i) Kan opdrachtgever instemmen met het verwijderen van het bepaalde over de risicoanalyse? (ii) Zo nee, kunt u beschrijven wat precies moet worden geanalyseerd/beheerst, zodat het aanbod meer op maat gemaakt kunnen worden? (iii) Heeft opdrachtgever recent nog zelf nog een risicoanalyse uitgevoerd? Zo, ja zit hier informatie bij die opdrachtgever met Opdrachtnemer kan delen? Dit om Opdrachtnemer een beter inzicht te geven en in staat te stellen risico's te detecteren die onderdeel van de aangeboden dienst kunnen vormen?		Zie het antwoord op vraag 171.

173	Gibit2024		4.1 & 4.2	Leverancier is van mening dat zij in redelijkheid niet aan welke termijn dan ook – dus ook niet aan een fatale termijn – kan worden gehouden indien het overschrijden ervan verband houdt met de omstandigheid dat: i. de aanbestedende dienst zelf niet of niet tijdig de noodzakelijke medewerking verleent aan de uitvoering van de overeenkomst, of ii. de aanbestedende dienst zelf niet of niet alle door voor de uitvoering van de overeenkomst benodigde informatie verstrekt, of iii. de aanbestedende dienst zelf de voor de voortgang van de werkzaamheden van Leverancier benodigde besluiten niet of niet tijdig neemt; of iv. Betrokken derden – waaronder een of meer van de leveranciers en/of dienstverleners van ICT – hun medewerking en/of benodigde informatie niet, niet tijdig of anderszins gebrekkig verlenen; of v. Sprake is van meerwerk of sprake is van wijziging van de opdracht door of op verzoek van de aanbestedende dienst zelf; Bent u bereid deze redelijke nuancering van de in art. 4.2 GIBIT genoemde regel te aanvaarden?		i. Akkoord. ii. Akkoord. iii. Akkoord. iv. Akkoord, tenzij deze derde(n) door Leverancier worden ingezet ten uitvoering van de opdracht. v. Deels akkoord. Alleen indien sprake is van wijziging van de opdracht door of op verzoek van Opdrachtgever of wanneer er sprake is van meerwerk, met uitzondering van meerwerk dat door omstandigheden toe te rekenen is aan het handelen of juist het niet handelen van Leverancier.
174	Bijlage 11 - Inkoopvoorwaarden GIBIT 2023		4.1	Tekstvoorstel: Leverancier zou graag volgende toevoegen:" In alle gevallen, derhalve ook indien partijen schriftelijk en uitdrukkelijk een uiterste termijn zijn overeengekomen, komt Leverancier wegens tijdsoverschrijding eerst in verzuim nadat Opdrachtgever hem schriftelijk in gebreke heeft gesteld. " Bent u hiertoe bereid? Zo nee, waarom niet?	Leverancier acht het redelijk dat hij eerst in gebreke wordt gesteld voordat verzuim intreedt. Dit komt de rechtszekerheid ten goede.	Niet akkoord. Aanbestedende dienst hecht aan het tijdig beschikbaar hebben van de ICT-prestatie. Vandaar dat gehecht wordt aan het fatale karakter van termijnen.
175	Inkoopvoorwaarden GIBIT-2023		Artikel 4.2	Is de gemeente derhalve bereid om het artikel als volgt te wijzigen? "De volgende termijnen zijn – in afwijking van het vorige lid – in alle gevallen fataal: i. een in de Overeenkomst of het Implementatieplan opgenomen specifieke einddatum voor de Implementatie (waarbij daarmee verband houdende tussentijdse opleverdata niet fataal zijn); ii. indien het Overeengekomen gebruik omvat dat de Implementatie of de levering van Updates en/of Upgrades tijdig voor de inwerkingtreding van (een wijziging in) Wet- en regelgeving is afgerond: de ingangsdatum van die (gewijzigde) Wet- en regelgeving. In alle gevallen geldt bij niet-nakoming van een termijn, dat Opdrachtgever Leverancier eerst door middel van een schriftelijke ingebrekestelling de gelegenheid geeft om de het gebrek alsnog binnen een redelijke termijn te herstellen."	Inschrijver accepteert op zichzelf fatale termijnen, maar wenst bij het niet behalen van een termijn tenminste altijd eerst ingebreke gesteld te worden om zodoende een gebrek in de implementatie of levering van de diensten te kunnen herstellen. Daarnaast geldt dat vertraging die niet aan Inschrijver kan worden toegerekend ook niet voor haar risico moet komen.	Niet akkoord. Aanbestedende dienst hecht aan het tijdig beschikbaar hebben van de ICT Prestatie. Vandaar dat gehecht wordt aan het fatale karakter van termijnen.
176	Bijlage 11 inkoopvoorwaarden GIBIT	8	GIBIT 2023, Art 4.3 Uitvoering overeenkomst	Het voorgestelde artikel biedt de Opdrachtgever aanzienlijke vrijheid bij het ontbinden van de Overeenkomst. Het beoordelingsproces lijkt voornamelijk gebaseerd te zijn op subjectieve criteria, wat het moeilijk maakt voor de Inschrijver om de aanvaardbaarheid van het voorstel te objectiveren en te verwerkenen in de kosten en prijs. Daarom verzoekt de Inschrijver om artikel 4.3 te laten vervallen. Bent u bereid om hiermee in te stemmen?	Verduidelijking of aanpassing op artikel	Niet akkoord. De risicoanalyse zoals verplicht conform art. 3.4 omvat onder meer het beoordelen in welke mate een risico wordt voorzien met het invoeren van de ICT-prestatie binnen het applicatielandschap van opdrachtgever. Conform art. 3.5 is deze verplichting beperkt tot de informatie die opdrachtgever bij de aanbesteding heeft gegeven. Uit deze informatie blijkt op/waar de geleverde ICT-prestatie staat/aangeboden moet worden en op welke wijze hier gebruik van moet kunnen worden gemaakt. Juist de aanbieder weet welke (systeem)eisen er zijn om haar eigen ICT-prestatie goed te kunnen gebruiken. Indien uit de geleverde informatie reeds inzichtelijk was dat het applicatielandschap van opdrachtgever onvoldoende aan deze (systeem)eisen voldoet, dan had dit door de aanbieder aangegeven moeten worden om te voorkomen dat opdrachtgever achteraf met financieel nadelige consequenties geconfronteerd wordt (en wellicht daarmee ook niet met de juiste partij een overeenkomst heeft gesloten n.a.v. de aanbesteding en de daarvoor ontvangen aanbiedingen).
177	Bijlage 11 - Inkoopvoorwaarden GIBIT 2023		4.3	Leverancier ziet aan deze bepaling graag toegevoegd dat indien u de ontbinding van de overeenkomst inroept de reeds door leverancier uitgevoerde werkzaamheden, verrichte leveringen en diensten worden afgerekend naar de stand van het werk op het moment van ontbinding. Bent u hiertoe bereid? Zo nee, waarom niet?	Dit biedt leverancier zekerheid met betrekking tot het kunnen terugverdienen van (tenminste) de gemaakte investeringen.	Niet akkoord. Het voorstel houdt geen rekening met de situatie waarin nog niet verrekende werkzaamheden/leveringen verband houden met de door de derde beweerde schending.
178	Gibit2025		6.3	Het daadwerkelijke implementatieplan/plan van aanpak kan op punten afwijken van de verantwoordelijkheden en verplichtingen van Leverancier genoemd in dit artikel. Bent u bereid te accepteren dat het door Leverancier aan te leveren plan van aanpak/implementatieplan prevaleert?		Dit bevestigt de aanbestedende dienst.
179	Bijlage 11 inkoopvoorwaarden GIBIT	9	GIBIT 2023, Art 6.5 Implementatie ICT Prestatie	De Inschrijver kan geen inzicht krijgen in de risico's die verbonden zijn aan dit artikel buiten de aanbestedingsstukken om. Daarom acht de Inschrijver het niet redelijk dat eventuele kosten voor aanpassingen voor rekening van de opdrachtnemer komen. De opdrachtnemer stelt daarom voor om deze bepaling te schrappen. Gaat u hiermee akkoord?	Verduidelijking of aanpassing op artikel	Niet akkoord. De risicoanalyse zoals verplicht conform art. 3.4 omvat onder meer het beoordelen in welke mate een risico wordt voorzien met het invoeren van de ICT-prestatie binnen het applicatielandschap van opdrachtgever. Conform art. 3.5 is deze verplichting beperkt tot de informatie die opdrachtgever bij de aanbesteding heeft gegeven. Uit deze informatie blijkt op/waar de geleverde ICT-prestatie staat/aangeboden moet worden en op welke wijze hier gebruik van moet kunnen worden gemaakt. Juist de aanbieder weet welke (systeem)eisen er zijn om haar eigen ICT-prestatie goed te kunnen gebruiken. Indien uit de geleverde informatie reeds inzichtelijk was dat het applicatielandschap van opdrachtgever onvoldoende aan deze (systeem)eisen voldoet, dan had dit door de aanbieder aangegeven moeten worden om te voorkomen dat opdrachtgever achteraf met financieel nadelige consequenties geconfronteerd wordt (en wellicht daarmee ook niet met de juiste partij een overeenkomst heeft gesloten n.a.v. de aanbesteding en de daarvoor ontvangen aanbiedingen).
180	Bijlage 11 inkoopvoorwaarden GIBIT	9	GIBIT 2023, Art 6.5 Implementatie ICT Prestatie	Inschrijver acht het niet redelijk dat de kosten voor eventuele aanpassingen in het applicatielandschap van de Aanbestedende Dienst voor zijn rekening komen, gezien het gebrek aan beschikbare informatie over het applicatielandschap van Aanbestedende Dienst. Is Aanbestedende Dienst het ermee eens dat dergelijke kosten voor zijn rekening zijn?	Verduidelijking of aanpassing op artikel	Zie het antwoord op vraag 179.
181	Gibit2026		6.5	Leverancier kan zich buiten de aanbestedingsstukken om geen beeld vormen van de aan dit artikel verbonden risico's en acht het daarom voorts niet redelijk dat kosten voor eventuele aanpassingen voor rekening van opdrachtnemer komen. Opdrachtnemer stelt daarom voor om deze bepaling te schrappen. Bent u daarmee akkoord?		Zie het antwoord op vraag 179.
182	Bijlage 11 inkoopvoorwaarden GIBIT	9-10	GIBIT 2023, Art 7 Afhankelijkheid van en afstemming met derde partijen	Inschrijver is volgens artikel verantwoordelijk voor de operationele coördinatie van werkzaamheden met andere leveranciers. Inschrijver heeft momenteel echter geen contractuele relatie met deze partijen en dus geen invloed op of inspraak in additionele kosten of meerwerk door een derdeleverancier, functionele onmogelijkheden en leveringsdata van deze derden. Hoe loopt het escalatiepad als implementatie vertraagd raakt door derden en wat betekent dit voor de overeengekomen termijnen?	Verduidelijking of aanpassing op artikel	Dit artikel ziet op derden die de leverancier zelf inzet voor de uitvoering van de opdracht. Opdrachtnemer blijft verantwoordelijk voor deze inzet.

183	Inkoopvoorwaarden GIBIT-2023		Artikel 7.6	Leverancier neemt aan dat in het geval dat een Acceptatieprocedure niet slaagt, maar dit aantoonbaar niet te wijten is aan Leverancier, Aanbestedende Dienst Inschrijver gewoon de opdrachtsom voor zover die betrekking heeft op de implementatie van de ICT Prestatie zal betalen? Zo niet, dan verzoekt inschrijver dit te motiveren.		Indien het niet slagen van de acceptatieprocedure aantoonbaar niet aan leverancier is toe te rekenen, zullen partijen in overleg treden om de oorzaak weg te nemen, de acceptatieprocedure te hervatten en/of termijnen redelijkerwijs aan te passen. Voor zover de overeenkomst voorziet in (deel)betalingen op basis van bereikte mijlpalen of (deel)acceptatie, zal opdrachtgever die overeenkomstig betalen.
184	Bijlage 11 inkoopvoorwaarden GIBIT	10	GIBIT 2023, Art 8.1 Gemeentelijke ICT-kwaliteitsnormen, Interoperabiliteitseisen, normen en standaarden	Welke van de Gemeentelijke ICT-Kwaliteitsnormen zijn specifiek van toepassing op de opdracht?	Verduidelijking of aanpassing op artikel	Op de opdracht zijn de Gemeentelijke ICT-kwaliteitsnormen behorend bij de GIBTI van toepassing. Deze zijn te vinden op de website van de VNG: https://vng.nl/sites/default/files/2024-07/gemeentelijke_ict_kwaliteitsnormen_2024.pdf.
185	Gibit2027		8.1	Deze bepaling verlangt dat Leverancier voldoet aan de in de overeenkomst (nader) gespecificeerde interoperabiliteitseisen. Eventuele eisen op dit punt in de overeenkomst – en dus de daarin genoemde interoperabiliteitseisen – kent Leverancier nu niet. Kan daarover thans meer duidelijkheid worden verschaft?		De interoperabiliteitseisen hebben primair betrekking op de naadloze integratie binnen de bestaande Microsoft-architectuur van de gemeente (waaronder Azure, Microsoft 365 en Defender). Daarnaast dient de oplossing te beschikken over standaardkoppelvlakken (zoals REST API's en ondersteuning voor gangbare logformaten als Syslog/CEF) om gegevensuitwisseling met andere beveiligingscomponenten of een eventueel ticketsysteem mogelijk te maken. Van de opdrachtnemer wordt niet verwacht dat zij maatwerkkoppelingen ontwikkelt voor systemen die niet in de huidige scope zijn opgenomen, mits de geboden oplossing voldoet aan de marktstandaarden voor open interoperabiliteit zoals beschreven in de BIO.
186	Bijlage 11 inkoopvoorwaarden GIBIT	10-11	GIBIT 2023, Art 9 Acceptatie	In de GIBIT staat geen termijn voor de Acceptatieprocedure door de Aanbestedende Dienst. Wij stellen voor om de volgende artikelen toe te voegen om deze afspraken SMART vast te leggen: a. Opdrachtgever deelt binnen 14 dagen na oplevering aan Inschrijver mee of hij de ICT Prestatie accepteert. Dit kan worden gedaan door een expliciete mededeling of door toezending van het testverslag. b. Als de Opdrachtgever niet in staat is om binnen de in artikel a genoemde termijn aan Inschrijver mee te delen of hij de ICT Prestatie accepteert, moet hij dit voor het verstrijken van die termijn aan Leverancier melden, met opgave van redenen en van de termijn waarbinnen hij alsnog aan Leveranicer zal meedelen of hij de ICT Prestatie accepteert. Deze termijn is maximaal wederom 14 dagen. Deze verlenging kan eenmalig toegepast worden. c. Indien er geen mededeling wordt gedaan zoals beschreven in artikelen a en b, en als de aanvullende termijn voor Acceptatie zoals beschreven in artikel b verstrijkt zonder nader bericht van de Opdrachtgever, wordt de ICT Prestatie geacht door de Opdrachtgever te zijn geaccepteerd.	Verduidelijking of aanpassing op artikel	De aanbestedende dienst gaat gedeeltelijk akkoord. De voorgestelde termijn van 14 dagen voor de eerste beoordeling (artikel a) en de eenmalige verlenging van 14 dagen (artikel b) worden overgenomen om de voortgang te borgen. De opdrachtgever gaat niet akkoord met artikel c. Vanwege de kritieke aard van de security-dienstverlening is 'fictieve' of 'stilzwijgende' acceptatie niet wenselijk. Acceptatie vindt uitsluitend plaats door een expliciete schriftelijke mededeling van de opdrachtgever (decharge). Indien de opdrachtgever de termijnen overschrijdt zonder bericht, is er sprake van vertraging aan de zijde van de opdrachtgever, maar dit leidt niet tot automatische goedkeuring van de ICT-prestatie.
187	Bijlage 11 inkoopvoorwaarden GIBIT	10-11	GIBIT 2023, Art 9 Acceptatie	Is de Aanbestedende Dienst van mening dat de acceptatie van de gevraagde diensten plaatsvindt op basis van een implementatieplan dat in overleg tussen beide partijen wordt opgesteld? En dat dit implementatieplan de acceptatieprocedure en -criteria moet bevatten, waardoor het bepaalde in dit artikel in dit geval niet van toepassing is?	Verduidelijking of aanpassing op artikel	Niet akkoord. De voorwaarden in de GIBIT gelden als minimumvoorwaarden voor implementatie, tenzij hiervan in het implementatieplan is afgeweken.
188	Gibit2028		9	Bent u met opdrachtnemer van mening dat de acceptatie door opdrachtgever van de uitgevraagde diensten plaatsvindt op basis van het in overleg tussen partijen op te stellen implementatieplan en dat in dit implementatieplan de acceptatieprocedure en acceptatiecriteria dienen te worden opgenomen en dat het daaromtrent in dit artikel bepaalde in dit geval niet van toepassing is?		Zie het antwoord op vraag 187.
189	Inkoopvoorwaarden GIBIT-2023		Artikel 9.10	Is de gemeente derhalve bereid de bepaling alsvolgt te wijzigen? "Acceptatie wordt geacht te hebben plaatsgevonden indien a) Opdrachtgever de ICT Prestatie voor productieve doeleinden in gebruik heeft genomen binnen zijn organisatie, tenzij de vroegtijdige ingebruikname van de ICT Prestatie voor productieve doeleinden verband houdt met vertragingen of tekortschieten aan de zijde van Leverancier; of, b) te allen tijde indien binnen 10 werkdagen na implementatie van de ICTgeen gebreken met betrekking tot de ICT Prestatie aan Opdrachtnemer worden gemeld."	Om discussie over het ontstaan van gebreken te voorkomen acht Inschrijver het van belang dat eventuele bezwaren naar aanleiding van een Acceptatieprocedure ten alle uiterlijk binnen 10 werkdagen na implementatie van de ICT-prestatie worden gemeld bij Opdrachtnemer.	Niet akkoord.
190	Inkoopvoorwaarden GIBIT-2023		Artikel 9.2 i)	Is de gemeente bereid de beapaling als volgt aan te passen? "i) Na iedere levering van (delen van) de ICT Prestatie, wordt de betreffende levering door Opdrachtgever binnen 14 dagen getest op Gebreken. Door partijen wordt daarbij een testverslag opgemaakt en ondertekend. In dit testverslag zal worden vastgelegd of de ICT Prestatie Gebreken vertoont en voorts of de ICT Prestatie (deels) is goedgekeurd, dan wel afgekeurd; "	Het artikel bevat geen termijn waarbinnen de Acceptatieprocedure door Opdrachtgever moet worden doorlopen. Wij zouden graag de afspraken hierover SMART vast willen leggen en stellen daarom voor om de bepaling daarop aan te passen.	Niet akkoord.
191	Gibit2029		9.3	Zie hierover onze eerdere vraag bij artikel 4.2 GIBIT. Hetgeen daar is opgemerkt geldt overeenkomstig voor art. 9.3 GIBIT. Bent u daarmee akkoord?		Zie het antwoord op vraag 173.
192	Bijlage 11 inkoopvoorwaarden GIBIT	12	GIBIT 2023, Art 9.5, 10.10, 24.10, 24.11 en 24.13 Ontbinding	De term 'ontbinden' heeft juridisch gezien het gevolg dat Leverancier de geleverde diensten moet terugnemen en dat Leverancier de door de Opdrachtgever betaalde facturen moet terugbetalen. Gelet op de aard van de opdracht is dit slecht uitvoerbaar. Kunt u er derhalve mee akkoord gaan dat ontbinding alleen kan gelden voor toekomstige verplichtingen en geen ongedaanmakingsverplichtingen met zich meebrengt?	Verduidelijking of aanpassing op artikel	Niet akkoord. Aanbestedende dienst erkent dat een ontbinding als gevolg heeft dat de prestaties over en weer ongedaan moeten worden gemaakt. Bij een ICT-prestatie die alleen een dienst omvat, is het over en weer ongedaan maken van geleverde prestaties in een aantal omstandigheden niet mogelijk. In aanvulling op het gestelde in de GIBIT geldt dat na ontbinding op grond van 9.5, 10.10, 24.10, 24.11 en 24.13 de prestaties die over en weer zijn geleverd, niet ongedaan hoeven te worden gemaakt.

193	Inkoopvoorwaarden GIBIT-2023		Artikel 9.5	Bent u hiertoe bereid? Zo nee, waarom niet?	De sanctie van ontbinding, zoals beschreven in art. 9.5 is zeer zwaar, onder andere omdat daardoor de verplichting ontstaat tot ongedaanmaking. Die mogelijkheid zou alleen moeten bestaan bij materiele tekortkomingen. Inschrijver verzoekt u daarom de bevoegdheid tot ontbinding te beperken tot gevallen waarin na het voor de tweede maal doorlopen van de acceptatieprocedure nog altijd sprake is van gebreken, welke toegerekend kunnen worden aan Opdrachtnemer, die productie belemmerend zijn, c.q. operationeel gebruik verhinderen. Inschrijver verzoekt u tevens om, indien gebruik wordt gemaakt van deze bevoegdheid tot ontbinding, het recht op schadevergoeding uit te sluiten. Anders zou leverancier immers zowel ongedaanmaking als schadevergoeding verschuldigd (kunnen) raken wat in deze fase van de Opdracht een dubbele en niet proportionele sanctie zou zijn met betrekking tot een geconstateerde tekortkoming.	Niet akkoord. Aanbestedende dienst wil een stevige stok achter de deur hebben om een goed werkend product af te kunnen dwingen. Ontbinding is geenszins in het belang van opdrachtgever en opdrachtgever zal hier niet lichtvaardig toe overgaan. De bepaling heeft reeds in zich dat na een eerste acceptatieprocedure een tweede doorlopen wordt. Daarboven wordt de mogelijkheid geboden om afspraken te maken over het alsnog verhelpen van de gebreken (zie art. 9.5 sub ii) dan wel onder overeen te komen voorwaarden te accepteren (zie art. 9.5 sub iii). Mochten die bepalingen onder sub ii en iii voor opdrachtgever niet tot de voorziene oplossing leiden, dan moet een mogelijkheid bestaan tot ontbinding, welke met art. 9.5 sub i geboden wordt.
194	Bijlage 11 inkoopvoorwaarden GIBIT	11	GIBIT 2023, Art 9.8 Acceptatie	Kunt u bevestigen dat wanneer u de ICT Prestatie al voor productieve doeleinden in gebruik heeft, betaling verschuldigd bent aan Leverancier voor het gedeelte van de ICT Prestatie dat u voor productieve doeleinden in gebruik heeft?	Verduidelijking of aanpassing op artikel	De aanbestedende dienst bevestigt dit. Indien opdrachtgever (een onderdeel van) de ICT-prestatie voor productieve doeleinden in gebruik heeft, wordt dat onderdeel derhalve geacht niet door dergelijke gebreken te worden belemmerd en kan acceptatie daarvan niet worden onthouden. De bijbehorende betaling voor dat (geaccepteerde) gedeelte is dan verschuldigd conform de overeengekomen betalings-/mijlpaalafspraken, onverminderd de verplichting van leverancier om de bedoelde gebreken op korte termijn te herstellen.
195	Gibit2030		10	Het bepaalde in dit artikel in relatie tot de gevraagde dienstverlening is weinig duidelijk. Bunt u bereid te aanvaarden dat enkel die verplichtingen op het punt van onderhoud gelden welke door partijen eventueel later in een onderhoudsovereenkomst c.q. Service Level Agreement zijn overeengekomen?		Niet akkoord. De voorwaarden in de GIBIT gelden als minimumvoorwaarden voor onderhoud, tenzij hiervan in de overeenkomst/SLA is afgeweken.
196	Bijlage 11 inkoopvoorwaarden GIBIT	12-13	GIBIT 2023, Art 10 Onderhoud en ondersteuning	Het artikel in kwestie met betrekking tot de gevraagde dienstverlening is onvoldoende duidelijk. Bent u bereid te aanvaarden dat alleen de verplichtingen met betrekking tot onderhoud van kracht zijn die mogelijk later door de partijen zijn overeengekomen in een onderhoudsovereenkomst of Service Level Agreement?	Verduidelijking of aanpassing op artikel	Zie het antwoord op vraag 195.
197	Bijlage 11 inkoopvoorwaarden GIBIT	12	GIBIT 2023, Art 10.1 Onderhoud en ondersteuning	In dit artikel is opgenomen dat de onderhoudsdienstverlening start na acceptatie van de producten. Om een goede implementatie te waarborgen, is het noodzakelijk dat er vanaf het moment van levering al onderhoud is afgesloten voor de aangeboden producten. Kunt u dit artikel dienovereenkomstig aanpassen?	Verduidelijking of aanpassing op artikel	Niet akkoord.
198	Bijlage 11 inkoopvoorwaarden GIBIT	13	GIBIT 2023, Art 10.12 Onderhoud en ondersteuning	Het is redelijk om aan te nemen dat het achterlopen in versies niet aan de Leverancier kan worden toegeschreven als deze vertraging het gevolg is van de keuze van de Opdrachtgever. Kunt u bevestigen dat dit niet aan de Leverancier kan worden toegeschreven?	Verduidelijking of aanpassing op artikel	Akkoord.
199	Inkoopvoorwaarden GIBIT-2023		Artikel 10.14	Wij verzoeken u art. 10.14 buiten toepassing te verklaren.	De diensten die onderdeel zijn van de opdracht zijn kwalitatief afhankelijk van de meest recente updates. Als Opdrachtgever weigert updates van sensoren uit te rollen, komt direct de kwaliteit van de bewaking in gevaar. Het is voor Leverancier ondenkbaar dat Opdrachtgever 18 maanden mag achterlopen bij het in gebruik nemen van Updates van sensoren bij het leveren van een SOC-dienst. Dit artikel is niet bedoeld voor bewakingsdiensten: er ontstaan niet zozeer kosten voor Leverancier als u achterblijft bij Updates, maar wel risico's voor uw veiligheid.	Niet akkoord. Opdrachtgever heeft tijd nodig om de implementatie van een update/upgrade in te plannen. Tevens kan een update/upgrade mogelijk gevolgen hebben voor andere applicaties van opdrachtgever, waardoor er een bepaalde termijn nodig kan zijn voordat een update/upgrade in gebruik kan worden genomen. Juist artikel 10.14 ii dient de belangen van leverancier, aangezien hier een verplichting voor opdrachtgever is opgenomen om binnen een bepaalde termijn de ingebruikname te doen. Tevens geeft artikel 10.14 i reeds aan dat er geen sprake is van een tekortkoming door leverancier in onderhoud indien een gebrek reeds in een update/upgrade is verholpen.
200	Gibit2031		11.2	Mag opdrachtnemer ervan uitgaan dat voor dit artikel geldt dat het definitieve betalingsschema dat partijen op basis van de inschrijving van Opdrachtnemer overeenkomen onderdeel wordt van de overeenkomst(en)?		Niet akkoord. Artikel 11.2 wordt gehandhaafd.
201	Bijlage 11 - Inkoopvoorwaarden GIBIT 2023		11.2	Wij stellen daarom het volgende voor: - 35% bij opdrachtverlening (ondertekening van de overeenkomsten) - 35% na installatie - 30% na acceptatie of in gebruik name. Kunt u hiermee akkoord gaan? Zo nee, waarom niet?	Deze bepaling omschrijft dat 30% van de kosten voor de implementatie pas na integrale Acceptatie in rekening gebracht kan worden. Wij achten het voor alle partijen wenselijk van te voren al te weten wat het hele facturatieschema wordt.	Niet akkoord. Artikel 11.2 wordt gehandhaafd.
202	Inkoopvoorwaarden GIBIT-2023		Artikel 11.5	Kan de gemeente dat bevestigen? zo niet, kan de gemeente de noodzaak dan toelichten?	Het is voor Inschrijver mede in verband met vakanties haast ondoendelijk om ervoor zorg te dragen dat werkzaamheden die tegen het einde van het jaar zijn verricht uiterlijk voor zes januari te factureren. Deze vervaltermijn is niet realistisch en daarmee ook niet redelijk. Uit de toelichting bij de GIBIT - 2023 volgt dat de gemeente moet toelichten waarom toepassing van deze strikte vervaltermijn noodzakelijk is. Nu die toelichting in de aanbestedingsstukken ontbreekt, gaat Inschrijver er vooralsnog van uit dat deze deadline buiten toepassing is en dat de gangbare vervaltermijn van drie maanden geldt.	Zie antwoord op vraag 204.
203	Bijlage 11 - Inkoopvoorwaarden GIBIT 2023		11.5	Bent u derhalve bereid om artikel 11.5 als volgt te vervangen: Een factuur dient te voldoen aan de wettelijke eisen alsmede de eisen die in de Overeenkomst worden gesteld. Leverancier spant zich maximaal in om facturen uiterlijk binnen drie maanden nadat de betreffende werkzaamheden opeisbaar zijn geworden te versturen. Leverancier spant zich eveneens maximaal in om alle werkzaamheden die voor een jaarwisseling zijn verricht voor 6 januari te versturen. Dit betreffen geen verval termijnen. Zo nee, waarom niet?	Op grond van de wet vervalt het opeisen van een vordering door schuldeiser pas na jaren. Met de toegevoegde zinssnede dient Leverancier een factuur te sturen 3 maanden na het opeisbaar worden van de werkzaamheden op straffe van in zijn geheel vervallen van de factuur. Dit zal niet altijd mogelijk zijn, denk hierbij bijvoorbeeld aan een vakantieperiode of inwerken van nieuwe (externe) medewerkers. Voor Leveranciers is dit een zeer grote beperking op de standaard bepalingen uit de wet waarbij gevolgen van het niet inacht nemen van deze termijn niet in verhouding staat tot de mogelijke gevolgen. Daarnaast is het niet reëel om alle werkzaamheden die voor een jaarwisseling zijn verricht uiterlijk op 6 januari te moeten factureren i.v.m. vakantieperiode in deze tijd van het jaar	Zie antwoord op vraag 204.

204	Inkoopvoorwaarden GIBIT	14	Artikel 11.5	Wij stellen voor de laatste zin te verwijderen.	Wij achten het niet realistisch om ervan uit te gaan dat binnen een periode van 6 dagen na een kalenderjaar alle facturen zijn ingediend.	Aanbestedende dienst is akkoord met het laten vervallen van de zin "Alle werkzaamheden die voor een jaarwisseling zijn verricht dienen uiterlijk op 6 januari te zijn gefactureerd, tenzij anders overeengekomen" in artikel 11.5. De vervaltermijn van 3 maanden geldt voor alle facturen.
205	Bijlage 11 inkoopvoorwaarden GIBIT	14	GIBIT 2023, Art 11.6	Kan de Aanbestedende Dienst bevestigen dat zij akkoord gaan om de 30-daagse termijn te laten ingaan vanaf de datum vermeld op de factuur?	Verduidelijking of aanpassing op artikel	Niet akkoord. De betalingstermijn van 30 dagen gaat in na ontvangst van de factuur door aanbestedende dienst.
206	Bijlage 11 inkoopvoorwaarden GIBIT	14	GIBIT 2023, Art 11.8 & 11.9 Vergoeding, facturatie en betaling	Er staat dat aantoonbare prijsstijgingen van Derdenprogrammatuur altijd per 1 januari kunnen worden doorbelast, op voorwaarde dat deze prijsstijgingen niet voorzienbaar waren bij het sluiten van de Overeenkomst. Voor bepaalde Derdenprogrammatuur, waaronder Microsoft, is het voorgekomen dat ergens gedurende het lopende jaar ineens een prijsstijging van ruim 10% heeft plaatsgevonden. Het doorvoeren van prijswijzigingen pas per 01 januari heeft echter een aanzienlijke impact op inschrijvers en het is onredelijk om dit volledig voor rekening van de inschrijver te laten komen. Een dergelijke prijsstijging kan een professionele dienstverlener niet van tevoren inschatten of voorzien. Daarom stelt de inschrijver voor om dergelijke prijswijzigingen de eerstvolgende maand door te voeren. Gaat u hiermee akkoord?	Verduidelijking of aanpassing op artikel	Artikel 11.8 ziet op de jaarlijkse indexering die plaatsvindt op basis van het in het artikel genoemde indexcijfer. Artikel 11.9 ziet op het doorbelasten van aantoonbare prijsstijgingen van derden-programmatuur, mits deze prijsstijging ten tijde van het sluiten van de overeenkomst nog niet voorzienbaar was. Aanbestedende dienst gaat hierbij akkoord om prijsstijgingen op grond van art. 11.9 de eerstvolgende maand door te voeren.
207	Bijlage 11 inkoopvoorwaarden GIBIT	15	GIBIT 2023, Art 12 Garanties	Het lijkt erop dat er een innerlijke tegenstrijdigheid ontstaat in de voorwaarden vanwege het vereisen van garanties in combinatie met de verplichting tot verzekering, aangezien veel verzekeringen geen dekking bieden voor aansprakelijkheid die voortvloeit uit schending van garantieverplichtingen. Om deze inconsistentie aan te pakken, wordt voorgesteld om het kopje 'Garanties' te vervangen door 'Verplichtingen' en de eerste zin als volgt aan te passen: "Leverancier zal zich er tot het uiterste voor inspannen dat…	Verduidelijking of aanpassing op artikel	Niet akkoord.
208	Gibit2032		12	Veel verzekeringen plegen in beginsel geen dekking te bieden voor aansprakelijkheid die ontstaat bij schending van een garantieverplichting. Door in de GIBIT zowel garanties op te leggen en ook een verzekering te verlangen wordt een innerlijke tegenstrijdigheid in de voorwaarden gecreëerd. Bent u om die reden bereid om het kopje 'Garanties' te vervangen door 'Verplichtingen' en de 1e volzin als volgt aan te passen: 'Leverancier zal zich er tot het uiterste voor inspannen dat…"?		Niet akkoord.
209	Inkoopvoorwaarden GIBIT-2023		Artikel 12.2	Gelet op het bovenstaande is het verzoek om aan te sluiten bij de wettelijke regeling en de laatste zin uit artikel 10.2 GIBIT 2020 te schrappen. Gaat de gemeente hiermee akkoord?	Met de tweede volzin van artikel 12.2 wordt de bewijslast om met betrekking tot de reikwijdte van de garantie, de toerekenbaarheid van gebreken en door Leverancier wel of niet geleverde diensten omgedraaid. Dit leidt ertoe dat, indien de gemeente een garantie inroept, het aan Leverancier is te bewijzen dat dit beroep onterecht is, bijvoorbeeld wanneer een gebrek niet onder de garantie valt. Dit artikel bevat aldus een bewijslastverdeling die ervoor zorgt dat Leverancier negatief bewijs moeten leveren en dat is erg lastig. Een dergelijke omkering van de bewijslast is hoogst ongebruikelijk en achten wij onredelijk. Een bewijslast kan in uitzonderlijke gevallen worden omgedraaid, maar daar moeten goede redenen voor zijn. Bovendien is het zeer ongebruikelijk een bewijslast op voorhand, contractueel om te draaien. Leverancier stelt voor om aan te sluiten bij de wettelijke bepaling uit artikel 150 van het Wetboek van Burgerlijke Rechtsvordering. Daaruit volgt dat de partij die zich beroept op een rechtsgevolg dit dient te bewijzen. Dit betreft wat betreft Leverancier een redelijke benadering.	Niet akkoord.
210	Bijlage 11 - Inkoopvoorwaarden GIBIT 2023		13.1	Kan Opdrachtgever ermee akkoord gaan dat de volgende zinsnede aan dit artikel wordt toegevoegd: "….voor zover dit binnen de invloedssfeer van Leverancier ligt"? Zo nee, waarom niet?	Leverancier is van mening dat de garanties over bias, nauwkeurigheid en rechtmatigheid begrijpelijk zijn vanuit ethisch oogpunt, maar strikte en potentieel onbeheersbare eisen opleggen aan de Leverancier. Bovendien is "nauwkeurigheid" moeilijk objectief te kwantificeren bij complexe AI- of data-analyses. Ook "rechtmatige verwerking" kan buiten de controle van de Leverancier vallen als data door Opdrachtgever wordt aangeleverd.	Akkoord.
211	Bijlage 11 - Inkoopvoorwaarden GIBIT 2023		13.3-13.5	Leverancier stelt voor om een extra lid 6 aan dit artikel toe te voegen waarin het volgende wordt opgenomen: "Informatieverstrekking zoals genoemd in bovenstaande leden 1 tot en met 5 vindt uitsluitend plaats voor zover dit commercieel en technisch verantwoord is en zonder dat daarmee intellectueel eigendom van Leverancier in gevaar wordt gebracht. Derden die toegang krijgen tot deze algoritmische informatie via Opdrachtgever zullen een geheimhoudingsplicht inachtenemen die tenminste even ver strekt als die van Opdrachtgever." Kan Opdrachtgever hiermee akkoord gaan? Zo nee, waarom niet?	De informatieverplichting in deze artikelen is zeer verstrekkend, met name het verplicht en kosteloos leveren van detailuitleg over (statistische) modellen en besluitvorming. Dit kan commerciële belangen en intellectueel eigendom van Leverancier schaden, zeker indien concurrenten of derden toegang krijgen via Opdrachtgever. Het opnemen van het controlerecht (artikel 25) tot het algoritmisch model zelf en de achterliggende data is vergaand en potentieel bedrijfskritisch.	Akkoord.
212	Inkoopvoorwaarden GIBIT-2023		Artikel 14.2	Kan de gemeente bevestigen dat aanlevering van documentatie in het Engels in afwijking van dit artikel uit de GIBIT-2023 akkoord is?	De dienst die Leverancier levert is technisch van aard en in de IT-sector is technische documentatie veelal uitsluitend beschikbaar in het Engels. Inschrijver kan niet garanderen dat alle documentatie in het Nederlands beschikbaar is (en zal blijven)	Akkoord.
213	Bijlage 11 inkoopvoorwaarden GIBIT	16	GIBIT 2023, Art 14.4 Documentatie en informatie	Deze bepaling vereist dat de Inschrijver de documentatie steeds up-to-date houdt. Bij oplevering wordt een volledige set documentatie verstrekt die de stand van zaken weergeeft op dat moment. Echter, de Inschrijver is niet op de hoogte van alle wijzigingen die de beheerders van de Aanbestedende Dienst aanbrengen na de ingebruikname van de omgeving. Hierdoor is het niet haalbaar om de documentatie voortdurend bij te werken. Vraag: Is het mogelijk om deze bepaling te laten vervallen?	Verduidelijking of aanpassing op artikel	Niet akkoord. Documentatie is nodig voor het gebruik van de ICT-prestatie dan wel voor de inpasbaarheid van de ICT-prestatie in het applicatielandschap; de bepaling mag niet vervallen. De leverancier zal opdrachtgever alleen voorzien van documentatie bij de applicatie zoals die door leverancier wordt geleverd. Het verzorgen van documentatie bij de aanpassingen die opdrachtgever zelf aanbrengt, is de verantwoordelijkheid van opdrachtgever zelf.
214	Bijlage 11 inkoopvoorwaarden GIBIT	16	GIBIT 2023, Art 15.1 Productmanagement	Is het toegestaan om Roadmap-informatie alleen op verzoek te verstrekken?	Verduidelijking of aanpassing op artikel	Nee, de opdrachtgever gaat niet akkoord met het uitsluitend op verzoek verstrekken van roadmap-informatie. Gezien de snelle ontwikkelingen binnen het cybersecurity-domein en de Microsoft-cloudomgeving is proactieve informatievoorziening essentieel voor de strategische regie van de gemeente. De opdrachtgever staat er wel voor open om dit procesmatig te borgen door de roadmap-updates als vast agendapunt op te nemen in het periodieke tactische overleg (bijv. kwartaaloverleg). Op deze wijze wordt de administratieve last beperkt, terwijl de proactieve informatieplicht van de opdrachtnemer behouden blijft.

215	GIBIT 2023		Artikel 16	Geheel vervangen door: 16.1 Partijen aanvaarden over en weer slechts wettelijke verplichtingen tot schadevergoeding voor zover dat uit dit artikel en de navolgende artikelen blijkt. 16. 2 Partijen zijn aansprakelijk voor de door de andere partij geleden directe schade indien de aanspraken zijn ontstaan: • ten gevolge van een toerekenbaar tekortschieten in de nakoming van een of meerdere verplichtingen in haar verplichtingen jegens de andere partij; • ten gevolge van een buitencontractueel toerekenbaar handelen of nalaten bij de werkzaamheden die de andere partij haar medewerkers en/of haar onderaannemers verricht ter uitvoering van deze Overeenkomst. 16.3 Aansprakelijkheid van Partijen voor indirecte schade, daaronder begrepen gevolgschade, gederfde winst, gemiste besparingen, verlies van gegevens, gegevensbestanden en schade door bedrijfsstagnatie, is nadrukkelijk uitgesloten. 16.4 Dit artikel is van overeenkomstige toepassing op vrijwaring. 16.5 De Partij die toerekenbaar tekortschiet in de nakoming van zijn verplichtingen is tegenover de andere Partij uitsluitend aansprakelijk voor de door de andere Partij geleden of te lijden directe schade. 16.6 De hierboven bedoelde aansprakelijkheid voor directe schade is, per gebeurtenis, beperkt tot een bedrag van € 1.000.000,- per gebeurtenis, waarbij een reeks van samenhangende gebeurtenissen aangemerkt zal worden als één gebeurtenis, zulks met een maximum van € 2.000.000,- per kalenderjaar. Onder directe schade wordt uitsluitend verstaan:	a. schade aan producten en functies, waaronder in elk geval verstaan wordt: materiële beschadiging, gebrekkig of niet functioneren, verminderde betrouwbaarheid en verhoogde storingsgevoeligheid; b. schade aan andere eigendommen van de andere partij en/of derden; c. schade ten gevolge van dood of lichamelijk letsel; d. kosten van noodzakelijke wijzigingen c.q. veranderingen in producten, specificaties, materialen of documentatie, aangebracht ter beperking danwel herstel van schade; e. redelijke kosten van noodvoorzieningen, zoals het uitwijken naar andere systemen of het inhuren van derden; f. redelijke kosten gemaakt ter voorkoming of beperking van directe schade, die als gevolg van de gebeurtenis waarop de aansprakelijkheid berust, mocht worden verwacht; g. redelijke kosten gemaakt ter vaststelling van de schadeoorzaak, de aansprakelijkheid, de directe schade en wijze van herstel. 16.7 De hierboven opgenomen beperkingen komen te vervallen indien sprake is van opzet of grove schuld aan de zijde van een der partijen danwel diens leidinggevend personeel. 16.8 Op eerste verzoek zullen certificaten van verzekering door Partijen overgelegd worden. Aanbieder meent dat dit alternatief meer in lijn ligt met de bij deze overeenkomst betrokken relatieve wederzijdse risico's en een meer marktconforme regeling is. Kunt u daarmee instemmen?	Niet akkoord.
216	Bijlage 11 - Inkoopvoorwaarden GIBIT 2023		16.1	Bent u bereid de aansprakelijkheid van Leverancier voor indirecte schade uit te sluiten en directe schade als volgt, limitatief te definiëren: a) schade aan programmatuur, apparatuur en gegevensbestanden; b) schade aan andere eigendommen; c) kosten van noodzakelijke wijzigingen en/of veranderingen in apparatuur, programmatuur, specificaties, materialen of documentatie, aangebracht ter beperking c.q. herstel van schade; d) de kosten van noodvoorzieningen, zoals het uitwijken naar andere computersystemen, of het inhuren van derden; e) kosten van het noodgedwongen langer operationeel houden van (het) oude syste(e)m(en) en daarmee samenhangende voorzieningen; f) redelijke kosten gemaakt ter voorkoming of beperking van directe schade, die als gevolg van de gebeurtenis waarop de aansprakelijkheid berust, mocht worden verwacht; g) redelijke kosten gemaakt ter vaststelling van de schadeoorzaak, de aansprakelijkheid, de directe schade en de wijze van herstel. Kunt u hiermee akkoord gaan? Zo nee, waarom niet?	Het is redelijk en gebruikelijk om aansprakelijkheid t.a.v. indirecte schade zoals gevolgschade en winstderving uit te sluiten. Aansprakelijkheid t.a.v. indirecte schade vormt een niet te overzien risico voor Leverancier.	Niet akkoord. De aanbestedende dienst sluit aan bij de aansprakelijkheidsbepalingen uit het Burgerlijk Wetboek. In het Burgerlijk Wetboek wordt ook geen onderscheid gemaakt tussen directe en indirecte schade.
217	Bijlage 11 - Inkoopvoorwaarden GIBIT 2023		16.3	Kunt u akkoord gaan met de aanpassing van dit artikel als volgt: "De in lid 1 bedoelde aansprakelijkheid voor persoons- en zaakschade is beperkt tot een bedrag van € 750.000,– per gebeurtenis met een maximum van € 1.250.000,-. Samenhangende gebeurtenissen worden daarbij aangemerkt als één gebeurtenis. De aansprakelijkheid van partijen voor gevolgschade en/of indirecte schade is uitgesloten. Onder gevolgschade en/of indirecte schade wordt onder andere verstaan gederfde winst, gemiste besparingen, geleden verlies, verminderde goodwill en schade door bedrijfsstagnatie." Bent u daartoe bereid? Zo nee, waarom niet?	Gezien de potentiele omvang van de contractwaarde stelt Leverancier voor deze bepaling naar redelijkheid aan te passen	Niet akkoord. De aanbestedende dienst sluit aan bij de aansprakelijkheidsbepalingen uit het Burgerlijk Wetboek. In het Burgerlijk Wetboek wordt ook geen onderscheid gemaakt tussen directe en indirecte schade.
218	Bijlage 11 inkoopvoorwaarden GIBIT	17	GIBIT 2023, Art 16.3 Aansprakelijkheid	Aansprakelijkheid voor indirecte en gevolgschade is doorgaans ongebruikelijk en voor inschrijvers niet verzekerbaar. De inschrijver verzoekt de aanbestedende dienst om indirecte en gevolgschade uit te sluiten. Gaat u hiermee akkoord? Zo niet, kunt u uw antwoord motiveren?	Verduidelijking of aanpassing op artikel	Zie het antwoord op vraag 216.
219	Inkoopvoorwaarden GIBIT-2023		Artikel 16.3	Is de gemeente derhalve bereid om de bepaling als volgt te wijzigen? "De in lid 1 bedoelde aansprakelijkheid en daaruit voortvloeiende directe schade, is voor ieder contractjaar te allen tijde beperkt tot maximaal tweemaal de Vergoeding per contractjaar. Voor vergoeding van Samenhangende gebeurtenissen worden daarbij aangemerkt als één gebeurtenis, welke vallen in het contractsjaar waarin de eerste gebeurtenis heeft plaatsgevonden."	In de IT-branche is het gebruikelijk dat de aansprakelijkheid van schade te alle tijde wordt beperkt tot een realistisch en redelijkerwijs te verzekeren bedrag, Leverancier acht het redelijk haar aansprakelijkheid in beginsel te beperkten tot maximaal tweemaal de Vergoeding per contractsjaar. In dat kader wijst Inschrijver er ook op dat uit de toelichting op de GIBIT - 2023 volgt dat de GIBIT een vangnet is en onverlet laat dat er altijd proportionele afspraken moeten worden gemaakt.	Zie het antwoord op vraag 217.
220	Bijlage 11 inkoopvoorwaarden GIBIT	17	GIBIT 2023, Art 16.4 Aansprakelijkheid	Inschrijver is van mening dat de mogelijke aansprakelijkheid per jaar, gezien de omvang en complexiteit van de opdracht, disproportioneel hoog is. Het wordt redelijk geacht dat de overeenkomst en voorwaarden een zekere mate van risicodeling tussen partijen bevatten, wat de vraag doet rijzen of (potentiële) inschrijvers in staat zijn de beste mogelijke aanbieding te doen. Om deze reden stelt de inschrijver voor om de aansprakelijkheid te beperken en verzoekt om artikel 16.4 te vervangen door het volgende artikel: "De aansprakelijkheid voor overige schade is beperkt tot een maximaal bedrag per jaar van 1 maal de hoogte van de vergoeding per jaar. Samenhangende gebeurtenissen worden daarbij aangemerkt als één gebeurtenis."	Verduidelijking of aanpassing op artikel	Niet akkoord.
221	Bijlage 11 inkoopvoorwaarden GIBIT	17	GIBIT 2023, Art 16.4 Aansprakelijkheid	Dit artikel houdt de opdrachtnemer ook aansprakelijk voor indirecte schade van de opdrachtgever. Dit is buiten redelijke proporties voor deze dienstverlening. Bent u bereid om, zoals gebruikelijk is, de aansprakelijkheid van de Leverancier voor indirecte schade uit te sluiten of te beperken?	Verduidelijking of aanpassing op artikel	Zie het antwoord op vraag 216.
222	Bijlage 11 inkoopvoorwaarden GIBIT	17	GIBIT 2023, Art 16.4 Aansprakelijkheid	Bent u bereid de totale aansprakelijkheid van Inschrijver te beperken tot maximaal eenmaal de bedongen jaarvergoeding wegens een toerekenbare tekortkoming in de nakoming van de overeenkomst of uit enige andere hoofde gedurende de gehele looptijd van de overeenkomst? Indien niet, staat u open voor een alternatief plafondbedrag dat niet gebonden is aan de jaarlijkse beperking?	Verduidelijking of aanpassing op artikel	Niet akkoord.

223	Gibit2033		16.4	Bent u bereid de totale aansprakelijkheid van Leverancier wegens een toerekenbare tekortkoming in de nakoming van de overeenkomst of uit enige andere hoofde – over de gehele looptijd van de overeenkomst - te beperken tot maximaal eenmaal de bedongen jaarvergoeding? Zo neen, bent u dan bereid akkoord te gaan met een ander plafondbedrag (anders dan de beperking per jaar)?		Niet akkoord.
224	Gibit2034		16.4	Dit artikel houdt opdrachtnemer ook aansprakelijk voor indirecte schade van opdrachtgever. Dat is voor deze dienstverlening buiten redelijke proporties. Bent u bereid om, zoals te doen gebruikelijk is, de aansprakelijkheid van opdrachtnemer voor indirecte schade uit te sluiten of te beperken?		Zie het antwoord op vraag 216.
225	Bijlage 11 inkoopvoorwaarden GIBIT	17	GIBIT 2023, Art 16.5 Aansprakelijkheid	We beschouwen deze uitsluiting als gerechtvaardigd als er sprake is van verwijtbaar gedrag van de Leverancier. Zou u willen bevestigen of dit ook uw interpretatie is en/of u bereid bent om het aspect van verwijtbaarheid toe te voegen aan dit specifieke artikel?	Verduidelijking of aanpassing op artikel	Niet akkoord.
226	Bijlage 11 inkoopvoorwaarden GIBIT	17	GIBIT 2023, Art 16.5 Aansprakelijkheid	Het is belangrijk op te merken dat onbeperkte aansprakelijkheid voor leveranciers niet verzekerbaar is, wat een aanzienlijk risico vormt voor leveranciers. Voorschrift 3.9 D van de Gids Proportionaliteit vereist ook dat aansprakelijkheid moet worden beperkt. Overweegt u daarom om deze bepaling te laten vervallen?	Verduidelijking of aanpassing op artikel	Niet akkoord. Er is geen sprake van onbeperkte aansprakelijkheid. De aansprakelijkheid wordt immers beperkt in artikel 16.3 en 16.4.
227	Gibit2035		16.5 iv	Opdrachtnemer acht het in dit artikel bepaalde over het doorleggen naar de verwerker van een door de toezichthouder opgelegde boete niet redelijk, immers de hoogte van een opgelegde boete wordt mede bepaald door omstandigheden (o.m. de door verwerkingsverantwoordelijke gegeven medewerking, in het verleden door de verwerkingsverantwoordelijke begane overtredingen) waarop de verwerker geen invloed heeft. Opdrachtnemer verzoekt de aanbestedende dienst daarom dit artikel te verwijderen. Bent u daartoe bereid?		Niet akkoord.
228	Inkoopvoorwaarden GIBIT-2023		Artikel 16.5	Kan de gemeente daarmee akkoord gaan? Indien u niet akkoord bent verzoeken wij u dit te motiveren.	Artikel 16.5 sub IV GIBIT 2023 luidt als volgt: "De in dit artikel opgenomen beperkingen van aansprakelijkheid zijn niet van toepassing:ten aanzien van de door toezichthoudende autoriteit opgelegde boetes: (1. voor zover die boetes ook rechtstreeks aan Leverancier hadden kunnen worden opgelegd, maar niet zijn opgelegd; en 2. onder de voorwaarde dat Opdrachtgever Leverancier: a. onverwijld schriftelijk informeert over een door een toezichthoudende autoriteit gestart onderzoek dat kan leiden tot een boete alsmede over en het bestaan en de inhoud van de opgelegde boete; en b. Leverancier volledig betrekt bij het voeren van verweer tegen die boete althans het aan Leverancier toe te rekenen deel van die boete." In het aanbestedingsrecht geldt dat de overheid geen disproportionele eisen mag stellen aan leveranciers. Het eisen van onbeperkte aansprakelijkheid wordt als disproportioneel gezien. In de door de overheid vastgestelde 'gids proportionaliteit' staat hierover: ´De aanbestedende dienst verlangt geen aansprakelijkheid die op geen enkele manier gelimiteerd is'. Daarnaast is recent in een vonnis gezegd: "... dat ieder computersysteem uiteindelijk kan worden gehackt, zodat [de overheid] ook geen volledig hackfree systeem mocht verwachten" (ECLI:NL:GHARL:2018:7967). Zowel de rechtspraak als de wetgever zijn het er over eens dat 100% beveiliging niet bestaat en een aanbestedende dienst de Leverancier daarvoor dus niet volledig onbeperkt aansprakelijk mag houden. Leverancier verzoekt u derhalve om artikel 16.5 sub IV GIBIT buiten toepassing te laten.	Niet akkoord. Er is geen sprake van onbeperkte aansprakelijkheid. De aansprakelijkheid wordt immers beperkt in artikel 16.3 en 16.4. Bovendien heeft de rechter de mogelijkheid de verplichting tot schadevergoeding te matigen wanneer toekenning van de volledige schadevergoeding, gezien de omstandigheden, onaanvaardbaar zou zijn (artikel 6:109 BW).
229	Bijlage 11 - Inkoopvoorwaarden GIBIT 2023		16.5	Leverancier ziet graag dat de bepalingen onder i), iii) en iv) ook onder de aansprakelijkheidsbeperking van artikel 13.3 en 13.4 vallen. Tekstvoorstel: "De in dit artikel bedoelde beperking van aansprakelijkheid komt te vervallen indien sprake is van opzet of grove schuld aan de zijde van de andere partij of diens Personeel." Kunt u hiermee akkoord gaan?	Het is Leverancier niet toegestaan onbeperkte aansprakelijkheid voor schade te aanvaarden. Een onbeperkte aansprakelijkheid van Leverancier is gelet op de bedrijfsbelangen van Leverancier een te groot risico, staat niet in verhouding tot de opdracht en is onverzekerbaar. Wij verwijzen u hierbij tevens naar de Gids Proportionaliteit, voorschrift 3.9 D waarin aangegeven is dat een onbeperkte aansprakelijkheid niet toegestaan is.	Zie het antwoord op vraag 226.
230	Inkoopvoorwaarden GIBIT	18 en 23	Artikel 18.5 en 24.14	Wij verzoeken u de volgende aanvulling op te nemen in 18.5 en 24.14: "Dit artikel laat onverlet dat Leverancier informatie mag bewaren teneinde te voldoen aan wettelijke verplichtingen tot bewaring van gegevens."	Wij zijn uiteraard bereid om aan het eind van de contracttermijn informatie van opdrachtgever te retourneren, echter dient een uitzondering te worden opgenomen voor de gevallen waarin civiele of fiscale wetgeving opdrachtnemer tot bewaring verplicht.	Akkoord.
231	Bijlage 11 - Inkoopvoorwaarden GIBIT 2023		18.4	Leverancier geeft er de voorkeur aan om vooraf om toestemming te worden gevraagd voor het delen van de inhoud van de Overeenkomst met de in dit artikel genoemde partijen. Kan Opdrachtgever ermee akkoord gaan dat dit artikel dienovereenkomstig wordt aangepast? Zo nee, waarom niet?	Leverancier geeft er de voorkeur aan om vooraf om toestemming te worden gevraagd voor het delen van de inhoud van de Overeenkomst met de in dit artikel genoemde partijen.	Aanbestedende dienst gaat niet akkoord. Wij vinden kennisdeling en markttransparantie tussen gemeenten en voor samenwerking belangrijk voor verdere digitalisering.
232	Bijlage 11 inkoopvoorwaarden GIBIT	18	GIBIT 2023, Art 18.6 Geheimhouding	Het schenden van een geheimhoudingsverplichting kan leiden tot schade, die mogelijk moet worden vergoed volgens artikel 6:74 BW. Als er desondanks een boete wordt opgelegd, moet deze worden verrekend met eventuele schadevergoedingen om te voorkomen dat de Opdrachtgever zich ongerechtvaardigd verrijkt, zoals bepaald in artikel 6:92 lid 2 BW. Het laten vervallen van artikel 18 lid 6 wordt gevraagd. Als het antwoord negatief is, wordt verzocht om een toelichting.	Verduidelijking of aanpassing op artikel	Niet akkoord. Juist bij geheimhouding is een boete opgenomen omdat de schade die ontstaat door schending van de geheimhoudingsplicht veelal niet eenvoudig is aan te tonen. Aansprakelijk stellen (artikel 16) is in deze gevallen dus lastig. Om die reden is deze boeteclausule opgenomen.

233	Bijlage 11 inkoopvoorwaarden GIBIT	18	GIBIT 2023, Art 18.6 Geheimhouding	Het niet opleggen van een maximale boete zoals beschreven in dit artikel wordt als disproportioneel beschouwd. Bovendien vallen contractuele boetes doorgaans buiten de dekking van de beroepsaansprakelijkheidsverzekering. Overweegt u daarom alstublieft het opnemen van een boetebepaling te herzien? Indien niet, bent u dan bereid om in te stemmen met een maximaal bedrag dat Leverancier aan boetes verschuldigd kan zijn onder deze overeenkomst? Bijvoorbeeld, dat het totaal aan boetes gemaximeerd is op EUR 10.000,-, ongeacht het aantal gebeurtenissen.	Verduidelijking of aanpassing op artikel	Niet akkoord. Juist bij geheimhouding is een boete opgenomen omdat de schade die ontstaat door schending van de geheimhoudingsplicht veelal niet eenvoudig is aan te tonen. Aansprakelijk stellen (artikel 13) is in deze gevallen dus lastig. Om die reden is deze boeteclausule opgenomen. Aanbestedende dienst gaat wel akkoord met het beperken van de boeteclausule. Hierbij stemt aanbestedende dienst in met een maximaal bedrag van € 30.000,- per contractjaar (ongeacht het aantal gebeurtenissen).
234	Gibit2036		18.6	Een niet gemaximeerde boete zoals opgenomen in dit artikel is niet proportioneel. Bovendien vallen contractuele boetes doorgaans niet onder de dekking van de beroepsaansprakelijkheidsverzekering. Bent u derhalve bereid het opnemen van een boetebepaling te heroverwegen? Zo neen, bent u bereid in te stemmen met een maximaal bedrag dat Leverancier aan boetes verschuldigd kan zijn onder deze overeenkomst, bijv. dat het totaal aan boetes gemaximeerd is op [X] EURO (ongeacht het aantal gebeurtenissen)?		Zie antwoord op vraag 233.
235	Inkoopvoorwaarden GIBIT-2023		Artikel 18.6	Leverancier acht het niet redelijk en disproportioneel dat de boete niet beperkt is tot een maximaal bedrag. Is de gemeente bereid om de boete maximaliseren op € 25.000,- per contractjaar?		Zie antwoord op vraag 233.
236			Artikel 19.2	Is de gemeente bereid om op basis van de toelichting hosting in het artikel toe te voegen als overmachtssituatie?	In de IT/security branche is het gebruikelijk om ook een aantoonbare storing in hosting als overmacht aan te merken, tenzij door Leverancier zelf is veroorzaakt.	Nee, de opdrachtgever gaat niet akkoord met het expliciet toevoegen van 'hosting' als standaard overmachtssituatie in artikel 19.2. Er is geen sprake van hosting.
237	Bijlage 11 - Inkoopvoorwaarden GIBIT 2023		19.2	Leverancier stelt voor deze bepaling aan te passen en alleen stakingen van Personeel niet onder de overmachtsgrond te laten vallen en verlate aanlevering uit het artikel te schrappen. Kan Opdrachtgever daarmee akkoord gaan? Zo nee, waarom niet?	In deze bepaling worden vrijwel alle operationele risico's bij Leverancier gelegd, ook wanneer die oorzaken buiten de invloedsfeer van Leverancier liggen (bijvoorbeeld toeleveringsproblemen door geopolitieke omstandigheden of stakingen bij een derde partij).	Akkoord.
238	Bijlage 11 - Inkoopvoorwaarden GIBIT 2023		20.4	Leverancier stelt voor om de volgende zin aan dit artikel toe te voegen: "Leverancier is gerechtigd generieke bouwstenen, componenten, algoritmes en methodieken die in het kader van de ontwikkeling zijn toegepast of ontstaan, te hergebruiken en te exploiteren ten behoeve van andere opdrachten en klanten." Kan Opdrachtgever daarmee akkood gaan? Zo nee, waarom niet?	Gevolg van dit artikel is dat Leverancier elke mogelijkheid verliest om onderdelen van het maatwerk (her) te gebruiken bij andere klanten.	De opdrachtgever gaat akkoord met de voorgestelde toevoeging, onder de uitdrukkelijke voorwaarde dat dit hergebruik uitsluitend betrekking heeft op generieke methodieken, algoritmes en bouwstenen. Het is de opdrachtnemer nimmer toegestaan om klantspecifieke data, specifieke configuratiedetails van de gemeentelijke infrastructuur of informatie die herleidbaar is naar de bedrijfsvoering van de opdrachtgever te hergebruiken of te exploiteren voor derden. Het eigendom van de binnen de tenant van de gemeente geconfigureerde instellingen en de daaruit voortvloeiende data blijft onverkort bij de opdrachtgever.
239	Bijlage 11 inkoopvoorwaarden GIBIT	19	GIBIT 2023, Art 20.5 Intellectuele eigendom	Op basis van dit artikel zijn wij verplicht u volledig te vrijwaren tegen eventuele schadeclaims van derden als gevolg van inbreuk op intellectuele eigendomsrechten. Een onbeperkte vrijwaringsplicht is voor ons echter niet aanvaardbaar. We streven ernaar de vrijwaringsplicht te beperken door middel van de overeengekomen aansprakelijkheidsbeperking tussen beide partijen. Kan de Aanbestedende Dienst op basis van het bovenstaande instemmen met het toevoegen van de volgende tekst aan artikel 20.5 van GIBIT 2023: "Leverancier garandeert dat de aan Opdrachtgever geleverde ICT Prestatie geen inbreuk maakt op enig intellectueel eigendomsrecht of ander recht, inclusief persoonlijkheidsrechten, van derden. Leverancier vrijwaart Opdrachtgever en vergoedt Opdrachtgever voor alle claims van derden die gebaseerd zijn op de bewering dat de door Leverancier aan Opdrachtgever geleverde ICT Prestatie inbreuk maakt op de genoemde rechten van die derden, onder voorwaarde dat Opdrachtgever Leverancier onmiddellijk schriftelijk informeert over het bestaan en de inhoud van de claim en de afhandeling van de zaak, inclusief het treffen van eventuele schikkingen, volledig overlaat aan Leverancier. Opdrachtgever zal hiervoor de nodige volmachten, informatie en medewerking verlenen, zodat Leverancier effectief verweer kan voeren tegen dergelijke claims. De overeengekomen aansprakelijkheidsbeperking tussen partijen is eveneens van toepassing op deze vrijwaring."	Verduidelijking of aanpassing op artikel	Aanbestedende dienst kan bevestigen dat de aansprakelijkheid ten aanzien van artikel 20.5 valt onder de aansprakelijkheidsclasules zoals opgenomen in artikel 16.
240	Inkoopvoorwaarden GIBIT-2023		Artikel 20.5	Leverancier begrijpt het belang van de gemeente bij een vrijwaring tegen aanspraken van derden met betrekking tot IP. Echter, Leverancier acht het wel van belang dat die vrijwaring wordt uitgesloten voor handelingen welke kunnen worden toegerekend aan de gemeente, en als gevolg waarvan derden hun aanspraken doen laten gelden. Is de gemeente bereid de bepaling derhalve als volgt te wijzigen? "Leverancier garandeert dat de door hem aan Opdrachtgever verstrekte ICT Prestatie geen inbreuk maken op enige intellectuele eigendomsrechten of andere rechten, waaronder persoonlijkheidsrechten, van derden. Leverancier vrijwaart Opdrachtgever tegen alle aanspraken van derden gebaseerd op de stelling dat door Leverancier aan Opdrachtgever ter beschikking gestelde ICT Prestatie, inbreuk maken op bedoelde intellectuele eigendoms rechten van die derden, onder voorwaarde dat Opdrachtgever Leverancier onverwijld schriftelijk informeert over het bestaan en de inhoud van de aanspraak en de afhandeling van de zaak, waaronder het treffen van eventuele schikkingen, geheel overlaat aan Leverancier. Opdrachtgever zal daartoe de nodige volmachten, informatie en medewerking verlenen, zodat Leverancier zich effectief tegen deze aanspraken kan verweren.De verplichting tot vrijwaring vervalt indien de verweten inbreuk verband houdt (i) met gebruik van de intellectuele eigendomsrechten in strijd met wet- en regelgeving of de overeenkomst, dan wel (ii) met gebruik van de intellectuele eigendomsrechten in combinatie met publiek beschikbare AI. Leverancier is te allen tijde slechts gehouden tot betaling van de daadwerkelijk schadevergoeding waartoe hij in een eventuele gerechtelijke procedure wordt veroordeeld, dan wel de vergoeding waarover hij in een eventuele schikking overeenstemming over bereikt."		Niet akkoord.
241	Inkoopvoorwaarden GIBIT-2023		Artikel 20.8	Leverancier acht het redelijk en ook marktconform dat de vrijwaring zoals opgenomen in artikel 20.5 de enige remedie is die de gemeente ter beschikking staat. Is de gemeente derhalve bereid deze bepaling buiten toepassing te verklaren? Zo nee waarom niet?		Niet akkoord. IE-claims kunnen tot hoge kosten leiden. De derde partij die eigenlijk rechthebbende is, kan namelijk gederfde licentievergoedingen en geleden schade claimen als de gemeente software (of andere beschermde goederen) gebruikt. In de praktijk zien we dat leveranciers in zo'n geval tot wel 200% van de catalogusprijs gaan claimen. Bovendien kan de eigenlijk rechthebbende middels auteursrechtelijk beslag zelfs de computers in beslag nemen waarop de software staat geïnstalleerd. Met andere woorden: er is een continuïteitsrisico en dat dient beperkt te worden door zo snel mogelijk de overeenkomst te kunnen ontbinden. Hoe sneller ontbonden wordt, hoe lager de claim voor het (voortgezet) gebruik zal zijn en hoe kleiner de kans dat de (beweerdelijk) rechthebbende zijn claim doorzet. Deze mogelijkheid bestaat naast de vrijwaring voor de schadeclaims (artikel 17.7), in de gedachte dat de leverancier wellicht een "kale kip" blijkt te zijn (en dan valt er weinig te vrijwaren).

242	Bijlage 11 - Inkoopvoorwaarden GIBIT 2023		21.1	Leverancier stelt voor de volgende zin aan dit artikel toe te voegen: "Deze verplichting ziet uitsluitend op de eigen gegevens van Opdrachtgever en niet op de onderliggende programmatuur, datamodellen, configuraties, algoritmes of overige knowhow van Leverancier." Kan Opdrachtgever daarmee akkoord gaan? Zo nee, waarom niet?	Dit sluit aan bij wat hieromtrent gebruikelijk is in de markt.	Niet akkoord. Volgens de aanbestedende dienst ziet de verplichting waarnaar wordt verwezen uitsluitend op eigen gegevens van opdrachtgever en eigen configuratie van de opdrachtnemer.
243	Bijlage 11 - Inkoopvoorwaarden GIBIT 2023		21.2	Leverancier stelt voor de volgende zin aan dit artikel toe te voegen: "Het ontwikkelen van nieuwe koppelingen, het converteren naar specifieke bestandsformaten of het opstellen van aanvullende documentatie valt buiten de scope van de Overeenkomst en geschiedt uitsluitend op basis van afzonderlijke afspraken en tegen vergoeding van de daaruit voortvloeiende kosten." Kan Opdrachtgever daarmee akkoord gaan? Zo nee, waarom niet?	Dit sluit aan bij wat hieromtrent gebruikelijk is in de markt.	Aanbestedende dienst gaat niet akkoord. Indien zich een dergelijke situatie zich voordoet, dan worden tarieven in het prijzenblad zoals opgegeven voor categorie C toegepast.
244	Bijlage 11 inkoopvoorwaarden GIBIT	20-21	GIBIT 2023, Art 22 Derdenprogrammatuur	In het geval van de aanschaf van standaard software van derden als onderdeel van de uitvraag, is het voor de Aanbestedende Dienst onvermijdelijk om de desbetreffende licentievoorwaarden te accepteren. Deze licentievoorwaarden vormen een integraal onderdeel van de aankoop van de software en definiëren de rechten en verplichtingen met betrekking tot het gebruik ervan. Ze worden opgesteld door de softwarefabrikant en zijn specifiek gericht op de (eind)gebruiker van de software. Voor het gebruik van de software is het noodzakelijk dat de licentievoorwaarden voorafgaand aan het gebruik worden geaccepteerd; zonder acceptatie kan de software eenvoudigweg niet worden gebruikt. Bij de aanbieding zal de opdrachtnemer de toepasselijke licentievoorwaarden van de leverancier meesturen. Kan de Aanbestedende Dienst bevestigen dat zij akkoord gaan met de licentie- en contractvoorwaarden van de leverancier, waaronder de EULA (End User License Agreement)?	Verduidelijking of aanpassing op artikel	De aanbestedende dienst bevestigt dit.
245	Gibit2037		22	In het geval van de aanschaf van standaard software van derden (toch) onderdeel is van de uitvraag, ontkomt Opdrachtgever niet aan de desbetreffende licentievoorwaarden. De licentievoorwaarden maken integraal onderdeel van de aankoop van de software. Door middel van licentievoorwaarden worden de rechten en plichten van het gebruik van de software benoemd. Licentievoorwaarden zijn opgesteld door de softwarefabrikant en specifiek geschreven voor de (eind)gebruiker van de software. Om gebruik te mogen maken van de software dienen voorafgaand aan het gebruik de licentievoorwaarden geaccepteerd te worden, zonder acceptatie mag de software simpelweg niet gebruikt worden. Uiteraard zal opdrachtnemer bij de aanbieding de toepasselijke licentievoorwaarden van de vendor meesturen. Kunt u bevestigen dat opdrachtgever akkoord gaat met de licentie- en contractvoorwaarden vanuit de vendor, waaronder de EULA (End User License Agreement)?		De aanbestedende dienst bevestigt dit.
246	Bijlage 11 - Inkoopvoorwaarden GIBIT 2023		23.1	Bent u bereid aan dit artikel toe te voegen: "mits opdrachtgever daarbij schriftelijk gemotiveerd onderbouwt en kenbaar maakt aan Leverancier waarom deze persoon niet voldoet aan de overeengekomen kwalificaties?" En kan Opdrachtgever toelichten wat zij bedoelt met de zinsnede 'om redenen in de persoon gelegen'?	Het is onduidelijk wat hiermee bedoeld wordt.	Akkoord. De zinsnede "om redenen in de persoon gelegen" ziet op omstandigheden die specifiek te maken hebben met de betrokken medewerker zelf, en niet op externe factoren of algemene omstandigheden binnen de opdracht. Het gaat dus om persoonlijke gedragingen of het functioneren van het ingezette personeel, waardoor de opdrachtgever de inzet niet langer wenselijk vindt.
247	Bijlage 11 - Inkoopvoorwaarden GIBIT 2023		23.2	Bent u bereid aan dit artikel toe te voegen: "indien Leverancier geen geschikt vervangend Personeel heeft binnen de onderneming van Leverancier en de kosten voor de inhuur van de vervanger wezenlijk hoger zijn, treden partijen in overleg?"	Het is in onderhavig geval onredelijk om Leverancier volledig voor deze hogere kosten te laten opdraaien.	Niet akkoord.
248	Inkoopvoorwaarden GIBIT-2023		artikel 24.1	Leverancier stelt voor om dit artikel wederkerig te maken en stelt de volgende tekst voor: "Een Partij is niet gerechtigd hun verplichtingen op te schorten dan na het sturen van een ingebrekestelling, waarin aan de andere partij een redelijke termijn van minimaal 30 dagen wordt geboden om alsnog aan de verplichtingen te voldoen." Vraag: Is de gemeente bereid om deze bepaling overeenkomstig aan te passen?		Niet akkoord.
249	Bijlage 11 inkoopvoorwaarden GIBIT	22	GIBIT 2023, Art 24.10/24.11 Ontbinding	Inschrijver verzoekt Aanbestedende Dienst te bevestigen dat in het geval van ontbinding van de overeenkomst op basis van deze artikelen, er geen verplichting tot ongedaan making van verbintenissen ontstaat.	Verduidelijking of aanpassing op artikel	Zie het antwoord op vraag 192.
250	Bijlage 11 inkoopvoorwaarden GIBIT	22	GIBIT 2023, Art 24.11 Opschorting, opzegging en ontbinding	De in sub i t/m v genoemde omstandigheden kunnen ook de Aanbestedende Dienst treffen. De Inschrijver wil in die situaties ook het recht hebben om de overeenkomst te ontbinden. Het is bijvoorbeeld niet redelijk om van de Inschrijver te verwachten dat deze blijft leveren als duidelijk is dat de Aanbestedende Dienst niet van plan is om te betalen of niet in staat is om te betalen. Kan een dergelijke verkorte bepaling in de overeenkomst worden opgenomen?	Verduidelijking of aanpassing op artikel	Niet akkoord. Deze situaties zijn immers niet van toepassing op opdrachtgever.
251	Inkoopvoorwaarden GIBIT-2023		artikel 24.11	Is de gemeente ermee akkoord om de volgende bepaling op te nemen in de overeenkomst? "In afwijking van artikel 24.11 GIBIT komen partijen overeen dat Opdrachtgever de Overeenkomst niet kan ontbinden wegens het enkele feit dat sprake is van een fusie, splitsing of overname van Leverancier, tenzij deze wijziging in zeggenschap een aantoonbare wezenlijke achteruitgang van de dienstverlening onder de Overeenkomst met zich meebrengt dan wel mee zal brengen."		Niet akkoord. In artikel 24.11 wordt bepaald dat de Overeenkomst kan worden ontbonden naar aanleiding van een ingrijpende wijziging in de zeggenschap over de activiteiten van de onderneming van Leverancier die maakt dat het in alle redelijkheid niet van de opdrachtgever kan worden verwacht dat zij de Overeenkomst in stand houdt. Dit artikel is opgenomen omdat zo'n wijziging in zeggenschap bijvoorbeeld gevolgen kan hebben voor de bescherming van (gevoelige) (persoons)gegevens. Gezien de ook voor Opdrachtgever verstrekkende consequenties van ontbinding is het niet waarschijnlijk dat hij van deze mogelijkheid gebruik zal maken als dat niet strikt noodzakelijk is.
252	Gibit2038		24.10/24.11	Opdrachtnemer verzoekt opdrachtgever te bevestigen dat indien ontbinding van de overeenkomst plaatsvindt op basis van deze artikelen er geen ongedaan making verbintenissen ontstaan.		Zie het antwoord op vraag 192.
253	Bijlage 11 inkoopvoorwaarden GIBIT	21	GIBIT 2023, Art 24.1 Opschorting, opzegging en ontbinding	De inschrijver stelt voor om het artikel wederkerig te maken en suggereert de volgende tekst: "Partijen zijn over en weer niet gerechtigd hun verplichtingen op te schorten dan na het sturen van een ingebrekestelling, waarin aan de andere partij een redelijke termijn van minimaal 30 dagen wordt geboden om alsnog aan de verplichtingen te voldoen." Graag vernemen wij of u bereid bent deze bepaling overeenkomstig aan te passen	Verduidelijking of aanpassing op artikel	Zie het antwoord op vraag 248.

254	Bijlage 11 inkoopvoorwaarden GIBIT	21	GIBIT 2023, Art 24.1 Opschorting, opzegging en ontbinding	Bent u het eens met het opnemen van de volgende bepaling in de overeenkomst? "In afwijking van artikel 20.11 van de GIBIT geldt dat de Opdrachtgever de Overeenkomst niet kan ontbinden louter vanwege een fusie, splitsing of overname van de Leverancier, tenzij dit aanzienlijke aanpassingen in de uitvoering van de overeenkomst met zich meebrengt.	Verduidelijking of aanpassing op artikel	Zie het antwoord op vraag 251.
255	Bijlage 11 inkoopvoorwaarden GIBIT	21	GIBIT 2023, Art 24.1 Opschorting, opzegging en ontbinding	Inschrijver stelt voor om dit artikel wederkerig te maken en stelt de volgende tekst voor: "Partijen zijn over en weer niet gerechtigd hun verplichtingen op te schorten dan na het sturen van een ingebrekestelling, waarin aan de andere partij een redelijke termijn van minimaal 30 dagen wordt geboden om alsnog aan de verplichtingen te voldoen." Vraag: Bent u bereid om deze bepaling overeenkomstig aan te passen?	Verduidelijking of aanpassing op artikel	Zie het antwoord op vraag 248.
256	Bijlage 11 inkoopvoorwaarden GIBIT	21	GIBIT 2023, Art 24.2 Opschorting, opzegging en ontbinding	Inschrijver is van mening dat de opzegtermijn van de Aanbestedende Dienst (3 maanden) niet in verhouding staat tot die van de Inschrijver (18 maanden). Aangezien artikel 26 van de GIBIT de Aanbestedende Dienst de garantie biedt dat zij nooit zonder leverancier zal zitten, verzoekt Inschrijver om de opzegtermijn voor beide partijen op 3 of 6 maanden te zetten. Inschrijver verneemt graag of de Aanbestedende Dienst akkoord gaat met het gelijktrekken van de opzegtermijnen in de overeenkomst.	Verduidelijking of aanpassing op artikel	Niet akkoord. Het verschil in opzegtermijn tussen Opdrachtgever en Leverancier is bewust gekozen. Indien Leverancier de Overeenkomst opzegt, dient Opdrachtgever veelal een nieuw aanbestedingstraject te doorlopen om een vervanging van de ICT-prestatie te vinden. Hier dient Opdrachtgever de tijd voor te krijgen. Indien Opdrachtgever de Overeenkomst opzegt, is er daarmee geen nadere afhankelijkheid aan de kant van de Leverancier die een langere periode vereist.
257	Bijlage 11 - Inkoopvoorwaarden GIBIT 2023		24.2	Kan Opdrachtgever ermee instemmen om de opzegtermijn van 3 maanden ook voor Leverancier te laten gelden? Zo nee, waarom niet?	De opzegtermijn voor Leverancier is erg lang.	Zie het antwoord op vraag 257.
258	Bijlage 11 - Inkoopvoorwaarden GIBIT 2023		24 lid 11 sub v	Kan Opdrachtgever ermee akkoord gaan om dit artikel uit te sluiten aangezien een verandering van zeggenschap geen invloed hoeft te hebben op het leveren van de afgesproken diensten? Zo nee, waarom niet?	Dit hoeft geen reden voor ontbinding te zijn aangezien dit geen invloed hoeft te hebben op de werkzaamheden die Leverancier levert.	Zie het antwoord op vraag 251.
259	Bijlage 11 - Inkoopvoorwaarden GIBIT 2023		24.15	Tekstvoorstel (toe te voegen aan artikel): "Indien Opdrachtgever op het moment van de ontbinding reeds prestaties ter uitvoering van de Overeenkomst heeft ontvangen, zullen deze prestaties en de daarmee samenhangende betalingsverplichtingen geen voorwerp van ongedaanmaking zijn. Bedragen die Leverancier vóór de ontbinding heeft gefactureerd in verband met hetgeen hij ter uitvoering van de overeenkomst reeds heeft verricht of geleverd, blijven onverminderd verschuldigd en worden op het moment van de ontbinding direct opeisbaar." Kunt u hiermee akkoord gaan? Zo nee, waarom niet?	Het is wel zo redelijk als Leverancier in onderhavig geval gecompenseerd wordt.	Niet akkoord. Het tekstvoorstel regelt dat de ontbinding geen gevolgen heeft voor reeds verrichte prestaties en betalingen. Bij diensten is dat zeker een mogelijkheid, omdat de reeds verrichte prestatie lastig terug te geven is. Bij ICT-diensten is het niet ongebruikelijk dat bij ontbinding de prestatie zodanig wordt opgeleverd dat een derde deze verder kan afmaken. Wij stellen voor om het tekstvoorstel als volgt op te nemen, 'nieuw artikel 24.15': 'In afwijking van artikel 24.14 kan Opdrachtgever ervoor kiezen om na ontbinding van de Overeenkomst de ICT-prestatie over te nemen. Leverancier is verplicht de ICT-prestatie zodanig op te leveren dat de ICT-prestatie door Opdrachtgever of een derde kan worden voltooid. Opdrachtgever behoudt in dat geval alle door Leverancier aangeleverde documenten, boeken en bescheiden, waaronder gegevens en gegevensdragers, dan wel ontvangt van Leverancier de op de ICT-prestatie betrekking hebbende documenten, boeken en bescheiden, waaronder gegevens en gegevensdragers. In dit geval betaalt Opdrachtgever de met de ICT-prestatie tot het moment van ontbinding gemoeide facturen die betrekking hebben op de opgeleverde ICT-prestatie tot het moment van ontbinding en waarvan de facturen zijn ingediend maar nog niet betaald'.
260	Bijlage 11 inkoopvoorwaarden GIBIT	21	GIBIT 2023, Art 24.3 Opschorting, opzegging en ontbinding	Bij een SaaS-oplossing is het niet mogelijk om de licentie- en onderhoudsovereenkomst los van elkaar te zien. Wij stellen daarom voor om dit artikel niet van toepassing te laten. Kunt u hiermee akkoord gaan?	Verduidelijking of aanpassing op artikel	Niet akkoord. Een SaaS-dienst, waarvan uitgegaan wordt in de vraag, houdt in dat de opdrachtgever functionaliteit inkoopt die een bepaalde beschikbaarheid heeft. In dat geval is geen sprake van een set samenhangende overeenkomsten, maar van één overeenkomst. Verder blijkt uit artikel 34 lid 3 GIBIT dat de leverancier verantwoordelijk is bij hosting, waar een SaaS-dienst onder valt, voor de updates en upgrades. Hieruit volgt dat artikel 24 lid 3 GIBIT geen toepassing heeft voor wat betreft updates en upgrades en het onderhoud van de SaaS-dienst niet kan worden ontbonden zonder de licentieovereenkomst ook te ontbinden.
261	Bijlage 11 inkoopvoorwaarden GIBIT	21	GIBIT 2023, Art 24.3 Opschorting, opzegging en ontbinding	Bent u bereid overeen te komen dat dit artikel als volgt wordt geformuleerd: "Wanneer de Opdrachtgever een deel van de Overeenkomsten opzegt, zoals bijvoorbeeld een licentieovereenkomst met een derdeleverancier die naar het oordeel van de Leverancier essentieel is voor de te leveren diensten, is het redelijk dat de Leverancier gelijktijdig de hoofdovereenkomst kan opzeggen. Zonder deze mogelijkheid kan de Leverancier gedwongen worden gedurende 15 maanden ontoereikend te presteren, met alle gevolgen van dien. Wij verzoeken u artikel 24.3 van de GIBIT buiten toepassing te verklaren of gezamenlijk te herformuleren."	Verduidelijking of aanpassing op artikel	Niet akkoord. Zie het antwoord op vraag 260.
262	Gibit2039		25	Is opdrachtgever bereid aan dit artikel toe te voegen dat: -Een controle niet wordt verricht door een concurrent van Opdrachtnemer; -Dat de partij die de controle uitvoert gehouden is aan geheimhoudingverplichtingen welke tenminste vergelijkbaar zijn met die welke zijn opgenomen in deze voorwaarden; -Een controle altijd wordt uitgevoerd op basis van een vooraf tussen partijen overeengekomen auditplan; -De resultaten en de vaststelling van de controle en de eventueel op basis daarvan uit te voeren acties tussen partijen worden besproken en overeengekomen tussen partijen.		- Niet akkoord. - Akkoord. - Niet akkoord. - De aanbestedende dienst gaat akkoord, mits de resultaten worden besproken en overeengekomen tussen opdrachtgever en opdrachtnemer.
263	Inkoopvoorwaarden GIBIT	23	Artikel 25	Wij verzoeken u de volgende condities aan een audit te verbinden en in artikel 25 vast te leggen: i) een audit zal in beginsel niet vaker dan eenmaal per jaar plaatsvinden, tenzij sprake is van een gegronde en spoedeisende reden; ii) een controle of audit dient ten minste 30 dagen van tevoren te worden aangekondigd, tenzij dit vanwege een gegronde en spoedeisende reden redelijkerwijs niet kan worden gevergd, in welk geval de aankondiging zo vroegtijdig als mogelijk zal worden gedaan; iii) partijen zullen de scope en criteria van de audit vooraf bespreken; iv) een audit zal niet worden uitgevoerd door een directe concurrent van Leverancier; v) een audit zal plaatsvinden tijdens normale werktijden zonder de dagelijkse bedrijfsvoering van Leverancier te verstoren en met inachtneming van de huisregels van Leverancier; v) in het kader van een controle of audit zal geen toegang worden verleend tot informatie, documenten of gegevens van andere klanten dan Opdrachtgever.	Een onbeperkt auditrecht zou de bedrijfsvoering en daarmee de dienstverlening aan andere klanten kunnen verstoren, tot schending van vertrouwelijkheid kunnen leiden, tot het openbaren van commercieel vertrouwelijke gegevens kunnen leiden, tot een onevenwichtige vergelijking kunnen leiden, etc. Daarom wensen wij een aantal condities aan een audit te verbinden.	i) Niet akkoord. ii) Akkoord. iii) Akkoord. iv) Niet akkoord. v) De aanbestedende dienst gaat akkoord met het verzoek om de audit te laten plaatsvinden tijdens normale werktijden. Daarnaast gaat de aanbestedendde dienst niet akkoord met de huisregels van Leverancier. vi) Akkoord.

264	Bijlage 11 inkoopvoorwaarden GIBIT	23	GIBIT 2023, Art 25 Controlerecht en medewerking audits bij Opdrachtgever	Is de Aanbestedende Dienst bereid om aan dit artikel toe te voegen dat: Een controle niet wordt uitgevoerd door een concurrent van de Opdrachtnemer; De partij die de controle uitvoert gebonden is aan geheimhoudingsverplichtingen die ten minste vergelijkbaar zijn met die welke zijn opgenomen in deze voorwaarden; Een controle altijd wordt uitgevoerd op basis van een vooraf overeengekomen auditplan tussen de partijen; De resultaten en de bevindingen van de controle, evenals eventuele daaropvolgende acties, worden besproken en overeengekomen tussen de partijen.	Verduidelijking of aanpassing op artikel	Zie de antwoorden op vragen 262 en 263.
265	Bijlage 11 inkoopvoorwaarden GIBIT	23	GIBIT 2023, Art 25.1 Controlerecht en medewerking audits bij Opdrachtgever	Bent u bereid om de volgende waarborgen toe te voegen met betrekking tot de audit: (i) Een maximum van één audit per jaar, (ii) Een voorafgaande kennisgeving van minstens drie weken, (iii) De mogelijkheid voor Inschrijver om een auditor af te wijzen indien deze een concurrent is, en (iv) Dat de auditwerkzaamheden de werkzaamheden/bedrijfsactiviteiten van Inschrijver niet hinderen of anderszins verstoren? Gelieve te bevestigen of aan te passen. Indien u niet wenst te bevestigen en/of aan te passen, wilt u dat dan motiveren?	Verduidelijking of aanpassing op artikel	Zie de antwoorden op vragen 262 en 263.
266	Inkoopvoorwaarden GIBIT-2023		Artikel 25.1	Leverancier begrijpt het belang van de gemeente bij een controlerecht via een audit. Leverancier wil zich daar ook aan conformeren, maar acht het in haar belang dat een dergelijke audit de bedrijfsvoering van Leverancier niet, althans zo min mogelijk zal frusteren. Is de gemeente daarom bereid om deze bepaling als volgt te wijzigen? "Opdrachtgever is gerechtigd de naleving door Leverancier van de wezenlijke verplichtingen uit hoofde van de Overeenkomst, de Inkoopvoorwaarden en de daarmee samenhangende overeenkomsten (SLA,verwerkersovereenkomst, etc.), binnen een redelijke termijn (van tenminste 60 dagen na aankondiging) maximaal eenmaal per jaar door een onafhankelijke ter zake deskundige aan geheimhouding gebonden derde te laten controleren. Een dergelijke controle of audit zal te allen tijde uitsluitend onder kantoortijden plaatsvinden en maximaal drie dagen in beslag nemen."		Niet akkoord. Zie het antwoord op vraag 380.
267	Bijlage 11 inkoopvoorwaarden GIBIT	23	GIBIT 2023, Art 25.4 Controlerecht en medewerking audits bij Opdrachtgever	Het is niet altijd mogelijk voor de Inschrijver om toegang te verkrijgen tot de locatie waar de diensten worden verleend, zoals wanneer de diensten worden uitgevoerd op een locatie van een derde partij. We stellen voor om de laatste zin van deze bepaling als volgt aan te passen: "Ook zal de Leverancier, indien redelijkerwijs mogelijk, toegang verlenen tot de locatie waar de diensten worden verleend." Bent u bereid deze aanpassing over te nemen?	Verduidelijking of aanpassing op artikel	Niet akkoord. De huidige bepaling voorziet voldoende in de door u genoemde situatie.
268	Bijlage 11 - Inkoopvoorwaarden GIBIT 2023		26.4	Leverancier acht het reëel dat tijdens het simuleren of daadwerkelijk verrichten van (delen) van het exit plan 1) de overeengekomen service levels niet van toepassing verklaard worden (louter op het simuleren van het exit-plan of daadwerkelijk verrichten van de in het plan beschreven werkzaamheden en dus niet op de primaire dienstverlening) 2) de verplichtingen van leverancier aangemerkt worden als inspanningsverplichtingen. Bent u bereid deze uitzonderingen op te nemen? Zo nee, waarom niet?	Leverancier is mede afhankelijk van de inspanningen van de opvolgend leverancier.	1) Akkoord. 2) Niet akkoord.
269	Bijlage 11 inkoopvoorwaarden GIBIT	24	GIBIT 2023, Art 26.7 Exit-plan, overstap, beperkte voortzetting, overdracht en vertengd gebruik	Volgens Inschrijver moeten de kosten van een mogelijke exit in verhouding staan tot de tekortkoming van de Leverancier. Bent u daarmee akkoord?	Verduidelijking of aanpassing op artikel	Niet akkoord. De kosten dienen in redelijke verhouding te staan tot de oorspronkelijke kosten voor de gehele ICT-prestatie (naar rato van de verminderde functionaliteit).
270	Bijlage 11 inkoopvoorwaarden GIBIT	26	GIBIT 2023, Art 29.4 Informatiebeveiliging Back-up	Gezien de aard van de dienst die Aanbestedende Dienst afneemt bij Inschrijver, lijkt het zinvol om dit artikel niet van toepassing te verklaren. Accepteert de Aanbestedende Dienst dit voorstel?	Verduidelijking of aanpassing op artikel	De aanbestedende dienst gaat gedeeltelijk akkoord. Voor zover de back-upverplichting ziet op de ruwe logdata en de hosting van de Microsoft Sentinel-omgeving zelf, erkent de aanbestedende dienst dat de primaire verantwoordelijkheid bij de platformleverancier (Microsoft) ligt en de gemeente hiervoor de retentie-instellingen beheert. Echter, artikel 29.4 blijft onverkort van toepassing op alle door opdrachtnemer ontwikkelde en beheerde configuraties, scripts, detectieregels, playbooks en documentatie. De opdrachtnemer dient zorg te dragen voor een deugdelijk versiebeheer en back-up van deze 'infrastructure-as-code'-elementen, zodat de dienstverlening na een calamiteit of foutieve aanpassing onverwijld kan worden hersteld.
271	Bijlage 11 - Inkoopvoorwaarden GIBIT 2023		29.5	Bent u bereid deze verplichting te beperken voor zover het de ICT prestatie betreft? Gaat u hiermee akkoord? Zo niet, kunt u dit nader toelichten hoe u dit ziet?	Het is voor grote ondernemingen met diverse portfolio's ondoenlijk om te rapporteren over alle incidenten in verband met informatiebeveiliging.	De opdrachtgever gaat akkoord met het beperken van de rapportageverplichting tot incidenten die betrekking hebben op de ICT-prestatie. Hieronder wordt verstaan: alle informatiebeveiligingsincidenten die direct of indirect invloed (kunnen) hebben op de vertrouwelijkheid, integriteit of beschikbaarheid van de gemeentelijke data, de geconfigureerde SIEM/SOC-omgeving of de continuïteit van de overeengekomen dienstverlening. Tevens vallen incidenten binnen de algemene bedrijfsinfrastructuur van de opdrachtnemer hieronder, indien deze infrastructuur wordt ingezet voor het leveren van de diensten aan de opdrachtgever. Incidenten die aantoonbaar geen enkele impact hebben op de veiligheid of uitvoering van de specifieke dienstverlening aan de gemeente, vallen buiten de rapportageplicht van dit artikel.
272	Inkoopvoorwaarden GIBIT-2023		Artikel 31.4	Inschrijver begrijpt dat de gemeente eist dat Dienstverlening op Afstand niet zo maar door Leverancier kan worden opgeschort. Inschrijver acht het echter redelijk als de dienstverlening op te schorten wanneer de gemeente niet voldoet aan de wezenlijke verplichtingen uit hoofde van de overeenkomst (waaronder betalingsverplichtingen) gedurende een periode van tenminste drie maanden. Is de gemeente bereid om de bepaling als volgt te wijzigen? "Leverancier is niet gerechtigd de Dienstverlening op Afstand op te schorten, behalve voor zover voortzetting redelijkerwijs niet gevergd kan worden. Daarvan is in ieder geval sprake in het geval Opdrachtgever haar verplichtingen uit hoofde van de Overeenkomst niet nakomt voor een periode die langer dan drie maanden (voort)duurt."		Akkoord.
273	Bijlage 12 huidige situatie	1	1	Kunt u een detail netwerkendiagram of tekening opleveren?	Eventueel details nodig voor oa de implementatie duur te bepalen en design / schaal bepalen van aanbod.	Aanbestedende dienst acht dit niet noodzakelijk. Zie antwoord op vraag 316.

274	Bijlage 12 huidige situatie	1	1	Hoeveel smartphones (Samsung Galaxy S-serie of de Apple iPhone-series in gebruik)	Tbv scope, design, implementatie, schaal, kosten.	250 iOS devices & 300 Android devices. Deze zijn echter geen onderdeel van de scope. Wij verwijzen u hiervoor naar Bijlage 12 detailinformatie (zie antwoord op vraag 316).
275	Bijlage 12 huidige situatie	1	1	Zijn smartphones in scope voor de dienstverlening, zoniet waarom niet?	Tbv scope, design, implementatie, schaal, kosten.	Zie antwoord op vraag 274.
276	Bijlage 12 huidige situatie	1	1	Binnen moderne SIEM- en SOC-dienstverlening is het monitoren en analyseren van netwerkverkeer via Network Detection & Response (NDR) inmiddels gangbaar om ook kwaadaardig en afwijkend netwerkverkeer tijdig te detecteren. In onze dienstverlening nemen wij dit standaard mee. Kan opdrachtgever aangeven of de inzet van Network Detection & Response (NDR) wordt gezien als een expliciete eis binnen de SIEM/SOC-dienstverlening, of dat dit wordt beschouwd als een kwaliteitsaspect dat kan bijdragen aan een positieve beoordeling bij gunning?	Betere toekomstbestendigheid door toevoegen Network Detection and Response. Tbv scope, design, implementatie, schaal, kosten. Geen plek nu in inschrijving (kwaliteit of eis) en prijsformulier.	De opdrachtgever beschouwt de inzet van Network Detection & Response (NDR) niet als een expliciete harde eis.
277	Bijlage 12 huidige situatie	1	1	Binnen moderne SIEM- en SOC-dienstverlening is het structureel inzichtelijk maken en opvolgen van kwetsbaarheden (Vulnerability Management) inmiddels een gangbaar onderdeel om risico's tijdig te signaleren en gericht te verbeteren. In onze dienstverlening nemen wij dit standaard kostelood mee als onderdeel van het security-overzicht en de doorontwikkeling. DE huidige Qualys kosten kunen hiermee uitgafaseerd worden. Kan opdrachtgever aangeven of Vulnerability Management (inclusief overzicht, prioritering en rapportage van kwetsbaarheden) wordt gezien als een expliciete eis binnen de SIEM/SOC-dienstverlening, of dat dit wordt beschouwd als een kwaliteitsaspect dat kan bijdragen aan een positieve beoordeling bij gunning? Zoja tot wanneer loopt het huidige Qualys contract?	Betere toekomstbestendigheid door toevoegen Network Detection and Response. Tbv scope, design, implementatie, schaal, kosten. Geen plek nu in inschrijving (kwaliteit of eis) en prijsformulier.	De opdrachtgever beschouwt Vulnerability Management op dit moment niet als een expliciete eis.
278	Huidige situatie	Bijlage 12	1	Is het koppelen van Aruba Switches en Aruba Clearpass aan Microsoft Sentinel onderdeel van de scope? Onze ervaring is dat het aansluiten van switches, access points en wireless controllers in de praktijk nauwelijks extra dreigingsinformatie oplevert, deze apparaten genereren namelijk vooral beheer- en statuslogs. Deze zijn relevant voor netwerkbeheer, maar dragen niet bij aan detectie van cyberaanvallen wanneer een organisatie werkt met Microsoft E5-fundamenten, Defender XDR en zero-trustprincipes.	Het antwoord helpt ons om de gewenste scope correct te duiden.	De assets/bronnen zoals genoemd in bijlage 12 detailinformatie dienen te worden gekoppeld tijdens implementatie. Zie verder antwoord op vraag 316.
279	Huidige situatie	Bijlage 12	1	Zijn de huidige virtuele servers onboard in Azure-ARC?	Het antwoord helpt ons om de gewenste scope correct te duiden.	De on-premise virtuele servers zijn op dit moment nog niet (volledig) geonboard in Azure Arc. De opdrachtgever is voornemens om Azure Arc te gebruiken als primair mechanisme voor het beheer van de Defender for Servers-omgeving en de log-ingest naar Microsoft Sentinel. Van de opdrachtnemer wordt verwacht dat zij binnen de implementatiefase adviseert over en ondersteunt bij de verdere uitrol van Azure Arc voor de relevante server-assets, om zo een uniforme monitoring via het Microsoft Defender XDR-platform te realiseren.
280	Bijlage 12 Huidige Situatie	1		Het verzoek aan gemeente om het aantal actieve Entra ID gebruikersaccounts aan te geven. Dat is dus exclusief service accounts en disabled accounts.	Deze informatie is voor leverancier noodzakelijk om de prijsstelling van haar dienstverlening aan de gemeente te kunnen bepalen.	Betreft 561 gebruikeraccounts.
281	Bijlage 12 Huidige Situatie	1		Graag de bevestiging van de gemeente dat leverancier VM's mag installeren op de beschikbare VM-omgeving.	Dit is voor leverancier noodzakelijk om onder andere lokale logs te verzamelen.	De opdrachtgever bevestigt dat de opdrachtnemer de mogelijkheid krijgt om VM's (zoals log collectors of forwarders) te installeren op de door de gemeente beschikbaar gestelde virtualisatie-omgeving, mits dit noodzakelijk is voor de overeengekomen dienstverlening. Hierbij gelden de volgende condities: -De specificaties (OS, resources, netwerksegmentatie) worden vooraf in het technisch ontwerp ter goedkeuring aan de opdrachtgever voorgelegd. -De VM's dienen te voldoen aan de hardening-eisen en het patchbeleid zoals vastgelegd in het Beleid Privacy, informatiebeveiliging en -beheer 2025-2028. -Beheer en onderhoud van de specifieke applicaties/collectors op deze VM's vallen onder de verantwoordelijkheid van de opdrachtnemer. -De gemeente blijft verantwoordelijk voor de onderliggende infrastructuur (hypervisor en hardware).
282	Bijlage 12 Huidige Situatie	1		Heeft gemeente (een deel van) het IT-beheer uitbesteed aan een dienstenleverancier? Zo ja, welke onderdelen en aan wie?		Nee, op dit moment heeft aanbestedende dienst geen IT-beheer uitbesteed.
283	Bijlage 12 Huidige Situatie	1		Is gemeente bereid om de huidige Enterprise EDR / XDR oplossing te vervanging door Windows Defender? Zo ja, is gemeente bereid om bij aanvang van de SOC dienstverlening de huidige oplossing te vervangen?	Om kosten te besparen en het beheer te vereenvoudigen, kan het voor de gemeente aantrekkelijk zijn de huidige Enterprise EDR/XDR-oplossing te vervangen, aangezien Windows Defender al standaard is inbegrepen in de Microsoft E5-licentie.	Ja, de gemeente is bereid en voornemens om de huidige Enterprise EDR/XDR-oplossing te vervangen door Microsoft Defender for Endpoint (en Defender for Servers). De gemeente streeft ernaar om deze transitie bij aanvang van de nieuwe SOC-dienstverlening gerealiseerd te hebben, zodat de opdrachtnemer direct gebruik kan maken van de volledige Microsoft Defender XDR-integratie in Sentinel.
284	Bijlage 12 - Huidige situatie			Kan aangegeven worden welke connectoren er nu in gebruik zijn in Sentinel? En welke er op de planning staan om te gebruiken?		Op dit moment hebben wij Microsoft 365 Insider Risk Management & Microsoft Entra ID actief. Toekomstige connectoren zullen afhankelijk zijn van de aangegeven logbronnen.

285	Bijlage 12 - Huidige situatie			Kan aangegeven worden wat de huidige en verwachte log-ingest is in Sentinel (GB/dag)?		De opdrachtgever beschikt op dit moment niet over volledige historische verbruiksdata die de gehele nieuwe scope afdekt. Om een eerlijke en objectieve prijsvergelijking tussen inschrijvers mogelijk te maken, hanteert de gemeente voor deze aanbesteding het volgende uitgangspunt: Fictief rekenvolume: Inschrijvers dienen hun prijsaanbieding (inclusief eventuele volumekortingen) te baseren op een gemiddelde log-ingest van 50 GB per dag. De opdrachtgever gaat ervan uit dat dit volume representatief is voor de 'Day-1'-scope, inclusief Microsoft 365-bronnen, Defender for Endpoint, serverlogs en de primaire netwerkbronnen (Firewall/ClearPass). De uiteindelijke facturatie zal plaatsvinden op basis van het werkelijke verbruik binnen de Microsoft Sentinel-omgeving van de gemeente.
286	Bijlage 12 - Huidige situatie	2	Netwerkinfrastructuur	Zijn er plannen om de huidige Palo Alto en Aruba-infrastructuur te vervangen tijdens de contractperiode, even als mogelijk andere (grote) infrastructuurwijzigingen.		Op dit moment zijn we niet voornemens om af te wijken van onze infrastructuur.
287	Huidige Situatie.pdf	2	Kengetallen	In hoeverre zijn iOS en Android devices uitgerust met Defender for Endpoint Mobile of welke plannen/ tijdslijnen zijn er voor implementatie?	Voor uitnutten van volledige Defender XDR functionaliteit is het gebruik van Defender for Endpoint Mobile gewenst. Dit verruimt protectie en detectiemogelijkheden voor de opdrachtgever.	Deze zijn er niet, hier zijn ook geen plannen voor.
288	Huidige Situatie.pdf	2	Kengetallen	Gebruikt de opdrachtgever in de huidige situatie Azure Arc voor management van de Linux en Windows Servers?	Voor uitnutten van volledige Defender XDR functionaliteit is het gebruik van Defender for Cloud gewenst. Dit verruimt protectie en detectiemogelijkheden voor de opdrachtgever.	Gedeeltelijk, niet alle beheer taken zullen via Azure Arc plaatsvinden.
289	Huidige Situatie.pdf	2	Kengetallen	Gebruikt de opdrachtgever in de huidige situatie Defender for Cloud (met of zonder Azure Arc) voor hybride/ onprem of cloud resources of welke plannen/ tijdslijnen zijn er voor implementatie?	Voor uitnutten van volledige Defender XDR functionaliteit is het gebruik van Defender for Cloud gewenst. Dit verruimt protectie en detectiemogelijkheden voor de opdrachtgever.	Ja, op dit moment zit de aanbestedende dienst in een overgangsfase. De verwachting is dat dit voor april klaar is. Zie ook het antwoord op vraag 316 voor een gedetailleerder overzicht van soort en aantal assets.
290	Huidige Situatie.pdf	2	Kengetallen	Gebruikt de opdrachtgever in de huidige situatie management tooling voor de Linux servers?	Dit is nodig voor de implementatie inschatting	Nee, dit wordt niet gebruikt.
291	Huidige Situatie.pdf	2	Kengetallen	Is er op dit moment al een syslog/CEF server aanwezig voor het loggen vanuit 3e partij logbronnen naar bijvoorbeeld Microsoft Sentinel?	Dit is nodig voor de implementatie inschatting	Nee, aanbestedende dienst heeft geen syslog server.
292	Huidige Situatie.pdf	2	Kengetallen	Gebruikt de opdrachtgever op dit moment de Qualys omgeving alleen voor de servers of wordt deze voor de gehele omgeving gebruikt?	Dit is nodig voor de implementatie inschatting	Dit wordt alleen voor servers gebruikt.
293	Huidige Situatie.pdf	2	Kengetallen	Wat zijn de groeiverwachtingen qua aantal endpoints, servers en cloud resources?	Dit is nodig voor de implementatie inschatting	Aantal endpoints zal ongeveer gelijk blijven (bij migraties kunnen er tijdelijk meer endpoints zijn). We verwachten dat het aantal servers gelijk zal blijven of zal afnemen. Het aantal cloudresources zal naar verwachting toenemen.
294	Huidige Situatie.pdf	2	Kengetallen	Zijn er plannen voor uitbreiding of migratie van IT-omgevingen die relevant zijn voor de SOC/SIEM?	Dit is nodig voor de implementatie inschatting	Nee, die zijn er op dit moment niet.
295	Bijlage 12 - Huidige situatie (kengetallen)	2	Kengetallen	Inschrijver verzoekt de Aanbestedende Dienst het totale aantal Office 365 / Microsoft 365-accounts te delen, uitgesplitst per licentietype (E1, E3, E5, F1, F3, F5), zodat een juiste prijsbepaling kan worden gemaakt.	Deze informatie is nodig om een correcte prijsstelling te bepalen.	561 E5, 39 E3, 11 F3.
296	Bijlage 12 - Huidige situatie (kengetallen)	2	Kengetallen	Inschrijver verzoekt de Aanbestedende Dienst het totaal aantal (interne) gebruikers in Entra ID (inclusief gebruikersaccounts, beheerdersaccounts en serviceaccounts, exclusief gastaccounts) te delen, zodat een juiste prijsbepaling kan worden gemaakt.	Deze informatie is nodig om een correcte prijsstelling te bepalen.	Het gehele aantal komt neer op 849 gebuikers/objecten (exc. gastaccounts).
297	Bijlage 12			Wat is er van de aangegeven scope nu al op de Sentinel aangesloten? Danwel wat moet er nog aangesloten worden?	Nodig om goede inschatting te kunnen maken over de hoeveelheid werk	Op dit moment zijn de standaard Microsoft 365-bronnen geactiveerd, waaronder Entra ID (Azure AD), Office 365 (Exchange, SharePoint, Teams) en Azure Activity Logs. Tevens zijn de eerste integraties met Microsoft Defender for Endpoint en Defender for Servers gerealiseerd.
298	Bijlage 12			Hoeveel usecases en van welke type zijn er op dit moment geimplementeerd?	Nodig om goede inschatting te kunnen maken over de hoeveelheid werk	Er zijn op dit moment geen usecases geimplementeerd.
299	Bijlage 12			Hoeveel incidenten zijn er nu per maand (per prioriteit)?	Nodig om goede inschatting te kunnen maken over de hoeveelheid werk	Dit is bedrijfsgevoelige informatie, waardoor wij dit niet kunnen delen.
300	Algemeen			Welke rol speelt aansluiting bij het Nationaal Cyber Security Centrum (NCSC) in uw beoordeling, met name ten aanzien van dreigingsinformatie, responsafstemming en naleving van nationale securityrichtlijnen?		De opdrachtgever hecht groot belang aan een effectieve uitwisseling van dreigingsinformatie. Een leverancier die aantoonbaar ervaring heeft met het verwerken van informatie van het Nationaal Cyber Security Centrum (NCSC) en andere relevante (overheids)partners, zoals de Informatiebeveiligingsdienst (IBD), kan meerwaarde bieden. De gemeente Steenwijkerland streeft conform haar informatiebeveiligingsbeleid naar een hoog niveau van weerbaarheid; de snelheid waarmee nationale dreigingsinformatie vertaald wordt naar specifieke detectieregels in de Sentinel-omgeving is hierbij essentieel.

301	Algemeen			Hoe weegt u het belang van NCSC-richtlijnen en -samenwerking ten opzichte van internationale normen zoals ISO of SOC, met name voor organisaties binnen de Nederlandse publieke en vitale sector?		Aanbestedende dienst vraagt om een ISO 27001 certificaat of vergelijkbaar als geschiktheidseis. Voor de uitvoering van de specifieke dienstverlening aan de gemeente Steenwijkerland hecht de opdrachtgever extra waarde aan de actieve toepassing van NCSC-richtlijnen en de aansluiting bij het nationale security-ecosysteem (zoals de IBD).
302	Algemeen			In hoeverre zoekt u binnen deze aanbesteding een strategische securitypartner die meedenkt over continue verbetering, roadmaps en volwassenheidsontwikkeling, versus een leverancier die uitsluitend de SOC-dienst uitvoert conform SLA?		De opdrachtgever is uitdrukkelijk op zoek naar een strategische securitypartner. Hoewel de basisdienstverlening (SOC-monitoring en incidentrespons) uiteraard conform de afgesproken SLA en PVE moet worden uitgevoerd, hecht de gemeente grote waarde aan de adviserende rol van de opdrachtnemer. Dit betekent concreet dat van de partner wordt verwacht dat zij actief meedenkt over de volwassenheidsontwikkeling (bijv. op basis van de BIO-normen of het NIST-framework); periodiek adviseert over de optimalisatie van de Sentinel-architectuur en de inzet van nieuwe Microsoft-securityfunctionaliteiten (roadmap-advisering); in de rapportages niet alleen kwantitatieve data levert, maar ook kwalitatieve duiding en verbetervoorstellen doet om de weerbaarheid van de gemeente structureel te verhogen.
303	Algemeen			Is het een vereiste dat de SOC-dienst SOC 2-gecertificeerd is, en zo ja: welke Trust Service Criteria (Security, Availability, Confidentiality) zijn voor u doorslaggevend?		Het is geen harde eis dat de SOC-dienst specifiek SOC 2-gecertificeerd is. De primaire eis is dat de dienstverlening aantoonbaar voldoet aan de BIO (Baseline Informatiebeveiliging Overheid), welke is gestoeld op de ISO 27001-normering.
304	Uitnodiging tot inschrijving SIEM-SOC	6	1.3.1	Is het toegestaan om naast Microsoft Sentinel ook andere SIEM- of SIEM-achtige oplossingen (on-premises of in de cloud) in te zetten, wanneer dit aantoonbaar leidt tot een snellere en accuratere SOC-dienstverlening? Zonder dat dit extra kosten met zich mee brengt. Wat ten gunste komt van de publieke investeringen. Indien dit niet is toegestaan, kan opdrachtgever toelichten waarom niet, gezien de uitvraag primair gericht is op de kwaliteit van de SIEM/SOC-dienstverlening en niet op het technische gebruik van één specifiek SIEM-platform? Het uitsluiten hiervan kan namelijk leiden tot uitsluiting van inschrijvers. Dit wringt met de aanbestedingswet.	Onze dienst maakt gebruik van een eigen volledig kosteloze directe SIEM-oplossing. Hierdoor is de data-ingest kosteloos, ongeacht de hoeveelheid data en ook wanneer er tijdens een incident sprake is van een sterke groei in het aantal gigabytes dat wordt verwerkt. Dit is gunstig en in het belang van de opdrachtgever. Deze directe SIEM zorgt daarnaast voor een snellere en meer volledige data-ingest richting het SOC, wat bijdraagt aan een betere kwaliteit van de SOC-dienstverlening, dan een waarin de tussenstap van de Sentinel plaatsvindt. De oplossing kan parallel draaien aan bestaande Microsoft Sentinel SIEM-omgevingen en verwerkt en correleert data onafhankelijk en parallel. Microsoft Sentinel behoudt daarbij zijn rol voor Microsoft Defender en andere specifieke of maatwerk use cases. De primaire datastroom voor snelle detectie en SOC-analyse verloopt via een parallelle route, zonder extra kosten, ongeacht de hoeveelheid data-ingest (in tegenstelling tot Sentinel). Dit maakt de dienstverlening schaalbaar en beter toekomstbestendig.	De opdrachtgever hecht grote waarde aan datasoevereiniteit, compliance aan de BIO en de borging van continuïteit (exit-strategie). In de uitvraag is Microsoft Sentinel binnen de eigen tenant van de gemeente aangewezen als het centrale platform voor log-aggregatie en detectie. Het is een inschrijver toegestaan om aanvullende SIEM- of SOC-tooling in te zetten, mits dit aantoonbaar bijdraagt aan de kwaliteit, onder de volgende strikte voorwaarden: Data-ingest: alle relevante logbronnen die binnen de scope vallen, moeten primair en onbewerkt in de Microsoft Sentinel-omgeving van de gemeente worden ingelezen en opgeslagen. Het bypassen van de gemeentelijke tenant voor primaire detectie is niet toegestaan. Intellectueel eigendom & beheer: alle ingerichte detectielogica (use cases), dashboards en configuraties dienen binnen de Sentinel-omgeving van de gemeente te worden opgebouwd en gedocumenteerd. Deze moeten bij het einde van de overeenkomst volledig eigendom blijven van de gemeente en onmiddellijk overdraagbaar zijn aan een opvolgende partij. Geen black box: de volledige SOC-dienstverlening (analyse, opvolging, rapportage) moet transparant en controleerbaar zijn voor de gemeente. Een externe SIEM-oplossing mag nooit leiden tot een situatie waarbij de gemeente voor haar historische securitydata of actuele status afhankelijk wordt van het platform van opdrachtnemer. Compliance: de inzet van een parallelle oplossing dient volledig te passen binnen de afspraken in de verwerkersovereenkomst (bijlage 9), waarbij data-residency binnen de EU/EER gewaarborgd is. De gemeente benadrukt dat de kosten voor het gebruik van Microsoft Sentinel (Azure consumption) buiten de scope van deze aanbesteding vallen en reeds door de opdrachtgever worden gedragen. Het argument van kostenbesparing op data-ingest door de inzet van een extern SIEM-platform is voor de opdrachtgever dan ook niet van toepassing.
305	Uitnodiging tot inschrijving SIEM-SOC	8	1.3.5	In de uitvraag wordt gesproken over het implementeren van een oplossing die overdraagbaar is naar het eigen beheerteam van de gemeente of naar een opvolgende leverancier. Een SOC-dienstverlening zelf is echter niet één-op-één overdraagbaar naar een andere leverancier. Kunt u toelichten wat opdrachtgever hiermee precies bedoelt en welke onderdelen volgens u overdraagbaar moeten zijn?	Onduidelijkheid bij verwachting van de dienst.	De opdrachtgever erkent dat de menselijke component van de SOC-dienstverlening (de expertise en interne processen van de opdrachtnemer) niet één-op-één overdraagbaar is. Met 'overdraagbaarheid' doelt de opdrachtgever op de technische inrichting en de operationele kennis die nodig is om de continuïteit van de beveiliging te waarborgen bij een eventuele overstap. Onder de overdraagbaarheid vallen in ieder geval de volgende onderdelen: Technische assets: alle binnen de Microsoft Sentinel-tenant van de gemeente ingerichte onderdelen, waaronder (maar niet beperkt tot) detectieregels (KQL), analytische regels, playbooks, workbooks/dashboards en data-connectoren. Documentatie: up-to-date runbooks voor incidentafhandeling, architectuurtekeningen van de koppelingen en beschrijvingen van de actieve use cases (welke dreigingen worden gedekt?). Data: volledige toegang tot en eigenaarschap van de historische logdata en incidenthistorie (audittrail). Kennisoverdracht: een gestructureerde overdrachtsperiode waarin de vertrekkende opdrachtnemer de beheerders van de gemeente (of de opvolgende leverancier) meeneemt in de specifieke inrichting van de omgeving. In lijn met de GIBIT 2023 (artikel 36) en de doelstellingen van deze aanbesteding, dient de oplossing zo te worden ingericht dat de gemeente na beëindiging van het contract niet opnieuw hoeft te beginnen met de technische inrichting van haar SIEM-platform.
306	Uitnodiging tot Inschrijving	24	2.2.1	Onze eerste inschatting is dat de maximale opdrachtsom erg laag is om alle eisen waar te kunnen maken. Kunt u nader toelichten hoe de gemeente tot dit bedrag is gekomen?		Voor het vaststellen van het plafondbedrag heeft aanbestedende dienst vergelijkbare gemeenten benaderd die in het recente verleden vergelijkbare opdrachten in de markt hebben gezet. Tevens zijn een aantal marktpartijen benaderd. Zie hiervoor antwoord op vraag 354.

307	Bijlage 2	1	Kerncompetentie 3	Aanbeider gebruikt een eigen directe koppeling met onderdelen ten behoeve van nauwkeurigheid snelheid en betrouwbaarheid. Sentinel blijftin stand maar is niet essentieel en geen bottelneck voor dienst. Kerncompetentie 3 is dan overbodig. Sentinel SIEM is dan niet de bottleneck. Kan dan de competentie 3 overbodg worden verklaard?	Kerncompetentie 3 is voor de kwaliteit en snelheid van de dienstverlening overbodig.	De opdrachtgever gaat niet akkoord met het vervallen van Kerncompetentie 3. De keuze voor Microsoft Sentinel als centraal SIEM-platform is een strategische keuze van de gemeente Steenwijkerland. De doelstelling is niet alleen het detecteren van incidenten, maar ook het opbouwen van een duurzame, overdraagbare en transparante securityvoorziening binnen de eigen Azure-tenant van de gemeente.
308	Bijlage 3 Prijsinvulformulier	1	1	De kosten voor Incident Response (IR), waaronder het coördineren en uitvoeren van de respons bij beveiligingsincidenten, zijn sterk afhankelijk van de aard en omvang van het incident en worden doorgaans bepaald op basis van een uurtarief of per incident. In de huidige uitvraag is de verwachte scope hiervan niet duidelijk beschreven. Kan opdrachtgever aangeven hoe Incident Response wordt verwacht te worden geprijsd en of deze kosten separaat mogen worden opgevoerd, bijvoorbeeld buiten de vaste SIEM/SOC-dienstverlening?	Kosten kunnen nu niet opgevoerd worden.	Zie antwoord op vraag 9 en vraag 83.
309	Bijlage 3 Prijsinvulformulier	1	1	De kosten voor forensische onderzoek, zijn sterk afhankelijk van de aard en omvang en worden doorgaans bepaald op basis van een uurtarief. In de huidige uitvraag is de verwachte scope hiervan niet duidelijk beschreven. Kan opdrachtgever aangeven hoe forensische onderzoek verwacht dient te worden geprijsd en of deze kosten separaat mogen worden opgevoerd, bijvoorbeeld buiten de vaste SIEM/SOC-dienstverlening?	Kosten kunnen nu niet opgevoerd worden.	Zie antwoord op vraag 83.
310	Bijlage 3 Prijsinvulformulier	1	1	De kosten voor herstelmaatregelen zijn sterk afhankelijk van de aard en omvang en worden doorgaans bepaald op basis van een uurtarief. In de huidige uitvraag is de verwachte scope hiervan niet duidelijk beschreven. Kan opdrachtgever aangeven hoe (advies over) herstelmaatregelen dient te worden geprijsd en of deze kosten separaat mogen worden opgevoerd, bijvoorbeeld buiten de vaste SIEM/SOC-dienstverlening?	Kosten kunnen nu niet opgevoerd worden.	Zie antwoord op vraag 83.
311	Bijlage 3 - Prijsinvulformulier	1	Prijsformulier	De Aanbestedende Dienst vraagt om een Incident Response retainer. Op welke plek in het prijsinvulformulier kan de inschrijver de bijbehorende kosten (abonnementsprijs en tarieven) opnemen?	Om duidelijkheid te verkrijgen over de prijsopbouw en een correcte invulling van het prijsformulier te waarborgen.	Zie antwoord op vraag 83.
312	Prijsinvulformulier / PvE			In het pricingdocument lijkt nu geen ruimte voor de details van de Incident Response dienst. Vanwege het onvoorspelbare karakter van deze activiteit worden hier meestal afspraken gemaakt over uurtarieven en dergelijke. Kunt u dit toelichten?		Zie antwoord op vraag 83.
313	Prijsinvulformulier / Programma van Eisen – Incidentvolume			Uit de pricingdocumenten blijkt niet expliciet hoe het aantal incidenten en acties doorwerkt in de jaarlijkse vergoeding. Is de operationele vergoeding gebaseerd op een verwacht incidentvolume, en zo ja: welke aannames hanteert de aanbestedende dienst hierbij en hoe wordt omgegaan met structurele overschrijding hiervan?		Zie antwoord op vraag 83.
314	PvE	alle	alle	Wordt de bestaande Microsoft Sentinel-omgeving verplicht gebruikt?	Als Sentinel verplicht is, moeten we onze architectuur en integratie hierop afstemmen. Dit beinvloedt licentiekosten, use-case ontwikkeling en technische afhankelijkheden.	ja, dit is een eis.
315	Bijlage 12 huidige situatie	1	1	Hoeveel E5 gebrukers momenteel?	Tbv scope, design, implementatie, schaal, kosten.	Momenteel zijn er 561 E5-gebruikers.
316	Bijlage 5 - Programma van Eisen/Bijlage 12 - Huidige situatie	1	2.1	Wordt met de lijst van logbronnen het overzicht van de kentallen bedoeld? Een andere logbronlijst zien wij niet.		De opdrachtgever heeft in het vertrouwelijke document Detailinformatie bijlage 12 een gedetailleerd overzicht gegeven van de aanwezige infrastructuur en de aan te sluiten bronnen. **Dit document is uitsluitend beschikbaar voor geinteresseerde partijen en kan tot uiterlijk de deadline van inschrijvingen worden opgevraagd via TenderNed (berichtenmodule).** De geinteresseerde partij verklaart dat het verstrekte document uitsluitend zal worden gebruikt ten behoeve van het voorbereiden en indienen van een inschrijving in het kader van deze aanbesteding. De partij zal het document niet aan derden verstrekken, noch geheel of gedeeltelijk kopiëren of anderszins gebruiken voor andere doeleinden. Na afronding van de aanbestedingsprocedure, ongeacht de uitkomst daarvan, zal de partij het document onverwijld vernietigen.
317	Bijlage 12 huidige situatie	1	1	Hoveel specifieke actieve en niet actieve M365 online gebruikers zijn er?	Tbv scope, design, implementatie, schaal, kosten.	Momenteel zijn er 561 E5-gebruikers. Niet-actieve gebruikers online hebben we niet. Personen uit dienst worden direct vanuit online verwijderd.

318	Programma van Eisen		Monitoring en use-case ontwikkeling	In de stukken wordt ruimte gelaten voor groei in monitoring en use-cases gedurende de looptijd. Kunt u aangeven hoe uitbreiding van logbronnen, use-cases en monitoringcapaciteit wordt gefaciliteerd en geprijsd binnen de bestaande overeenkomst?		De opdrachtgever voorziet gedurende de looptijd een natuurlijke groei en evolutie van het security-landschap. Dit wordt als volgt gefaciliteerd en geprijsd: Use-cases (dreigingslandschap): de opdrachtnemer is verantwoordelijk voor het proactief actueel houden van de use-case-library op basis van het veranderende dreigingslandschap. Het toevoegen van nieuwe detectielogica voor bestaande bronnen (om actuele dreigingen het hoofd te bieden) wordt beschouwd als onderdeel van de vaste maandelijkse dienstverlening. Groei van bestaande bronnen: een toename in datavolume van reeds aangesloten bronnen (bijv. meer gebruikers in Microsoft 365 of meer verkeer over de firewalls) dient binnen de vaste maandprijs te worden opgevangen (onder voorbehoud van 'fair use'). Nieuwe logbronnen: indien de gemeente besluit nieuwe typen bronnen toe te voegen, wordt de eenmalige inrichting afgehandeld via de wijzigingsprocedure tegen de overeengekomen tarieven zoals opgenomen in het prijzenblad. Monitoringcapaciteit: de opdrachtgever verwacht dat de SOC-dienstverlening schaalbaar is ingericht. Eventuele noodzakelijke uitbreiding van de monitoringcapaciteit wordt jaarlijks besproken tijdens het tactisch overleg. Inschrijvers worden gevraagd om in hun plan van aanpak toe te lichten hoe zij omgaan met 'Continuous Improvement' en hoe zij borgen dat de gemeente Steenwijkerland altijd beschermd blijft tegen de nieuwste dreigingen, zonder dat elke nieuwe regel tot een changeverzoek leidt.
319	Bijlage 5 Programma van Eisen		2.1.6 eisen met betrekking tot beroepsbekwaamheid	In uw eis stelt u bij kerncompetenties 1 en 2 dat wij onze bekwaamheid moeten aantonen door het overhandigen van een overheidsorganisatie als referent. Het inrichten van een SIEM/SOC center is tegenwoordig voor iedere organisatie noodzakelijk en de bekwaamheid zou daardoor los moeten staan van de branche waarin een gegadigde opereert. Kunt u aangeven waarom de eis zo gesteld is dat een deel van de aanbieders niet kan voldoen en bent u bereid om de eis algemener te formuleren zodat u ook andere partijen in de gelegenheid stelt mee te dingen naar de opdracht?		De aanbestedende dienst handhaaft de eis voor een referentie binnen de overheidssector (of een vergelijkbare complexe publieke organisatie). De motivatie hiervoor is dat de SIEM/SOC-dienstverlening voor een gemeente niet uitsluitend een technische exercitie is, maar diep verankerd is in specifieke kaders en wetgeving: BIO-compliance: een gemeente moet voldoen aan de Baseline Informatiebeveiliging Overheid (BIO). Ervaring met de specifieke auditeisen (zoals de ENSIA-verantwoording) en de bijbehorende rapportageverplichtingen is essentieel voor een succesvolle samenwerking. Keten-ecosysteem: in tegenstelling tot commerciële organisaties opereren gemeenten in een uniek ecosysteem. Van de opdrachtnemer wordt verwacht dat zij bekend is met de rol van partijen zoals de IBD (Informatiebeveiligingsdienst) en kan acteren binnen de landelijke crisisstructuren voor overheden. Politiek-bestuurlijke context: incidenten bij een overheidsinstantie hebben een ander maatschappelijk en politiek afbreukrisico dan in de private sector. Dit stelt specifieke eisen aan de communicatie en de prioritering van incidenten. De aanbestedende dienst is van mening dat deze eis proportioneel is, gezien de specifieke risico's en de wettelijke taken van de gemeente Steenwijkerland. Er zijn voldoende marktpartijen die over deze specifieke overheidservaring beschikken, waardoor de mededinging niet onnodig wordt beperkt. Zie ook het antwoord op vraag 356 voor wat onder overheidsorganisatie wordt verstaan.
320	Bijlage 5 Programma van Eisen	1	eis 2.2	Kan de gemeente bevestigen dat het toevoegen van specifieke nieuwe logbronnen of use cases gedurende de looptijd van de overeenkomst tot hogere kosten leidt en dat de gemeente die kosten dan zal dragen na afstemming met leverancier?	In het geval er gedurende de looptijd van de overeenkomst nieuwe logbronnen of specifieke use cases op verzoek van de gemeente worden toegevoegd, brengt dit extra kosten met zich mee. Dit staat los van eis 3.3.	De opdrachtgever maakt een strikt onderscheid tussen het actueel houden van de dienstverlening en het uitbreiden van de technische scope: Actualisatie (Inclusief): Conform eis 3.3 wordt verwacht dat de opdrachtnemer de bestaande monitoring en use-cases continu aanpast aan het veranderende dreigingslandschap. Het toevoegen van nieuwe detectielogica op bestaande logbronnen (om nieuwe typen aanvallen te detecteren) leidt niet tot additionele kosten. Dit behoort tot de kern van een professionele SOC-dienstverlening. Uitbreiding (Additioneel): Indien de opdrachtgever gedurende de looptijd besluit om nieuwe systemen of applicaties (die thans niet aanwezig zijn en niet in Bijlage 12 zijn vermeld) te ontsluiten, dan zijn prijzen van toepassing voor koppeling caterogie A, B of C zoals opgegeven in het prijzenblad. Zie antwoord op vraag 60 voor koppelingen die niet onder categorie A, B of C vallen.
321	Programma van Eisen (Bijlage 5)	3	4.12	Kan expliciet worden bevestigd dat het niet aanbieden van Microsoft Sentinel als primaire SIEM leidt tot uitsluiting van verdere beoordeling?	Dit om knock out risico's eenduidig vast te stellen	Aanbestedende dienst beschikt over Microsoft, waarbij het gebruik van Microsoft Sentinel is inbegrepen. Inschrijver dient gebruik te maken van de bestaande Microsoft Sentinel-omgeving (eis 4.12). Eisen uit het Programma van Eisen zijn knock-outcriteria waaraan inschrijving moet voldoen. Het niet voldoen aan één of meer eisen leidt tot uitsluiting.
322	Bijlage 5 Programma van Eisen	Algemeen	3.2	Kunt u aangeven hoeveel use cases minimaal worden verwacht binnen de SIEM/SOC-dienstverlening en of er een overzicht is van de specifieke use cases die moeten worden ingericht (bijvoorbeeld 2, 10 of 20 use cases)? Aangezien de ontwikkeling en het beheer van use cases doorgaans kosten met zich meebrengt en dit niet expliciet is gespecificeerd in de eisen, ontvangen wij graag verduidelijking om interpretatieverschillen te voorkomen.	Kosten usecases en defintitie uses cases. Voorkoming onverwachte additionele kosten?	De opdrachtgever hanteert geen hard minimumaantal voor use cases, aangezien kwaliteit en relevantie prevaleren boven kwantiteit. In plaats van een numeriek overzicht, verwacht de opdrachtgever de volgende aanpak: Risico-gebaseerde dekking: de opdrachtnemer dient een set aan use cases/detectieregels te leveren die een substantiële dekking biedt voor de meest relevante dreigingen voor een Nederlandse gemeente. Hierbij dienen de BIO-beheersmaatregelen en het MITRE ATT&CK-framework als leidraad. Standaard library: de opdrachtgever verwacht dat de opdrachtnemer bij aanvang een 'best practice' set aan use cases activeert voor de ontsloten bronnen (o.a. Microsoft 365, Defender, Identity en de firewalls). Inbegrepen in de prijs: het inrichten, finetunen en actueel houden van deze use-case-library (inclusief het toevoegen van nieuwe detectieregels voor opkomende dreigingen op bestaande bronnen) maakt integraal onderdeel uit van de vaste maandelijkse SOC-dienstverlening. Er zijn dus geen additionele kosten per use case binnen de overeengekomen scope. Maatwerk: mocht de gemeente specifiek verzoeken om de ontwikkeling van complexe, gemeente-specifieke businesslogica die buiten de standaard security-monitoring valt, dan zal dit via de wijzigingsprocedure worden afgehandeld.

323	Bijlage 5 Programma van Eisen	Algemeen	4.17	De kosten voor Incident Response (IR), waaronder het coördineren en uitvoeren van de respons bij beveiligingsincidenten, zijn sterk afhankelijk van de aard en omvang van het incident en worden doorgaans bepaald op basis van een uurtarief of per incident. In de huidige uitvraag is de verwachte scope hiervan niet duidelijk beschreven. Kunt u de verwachte scope van deze IR-retainer toelichten en aangeven of dit een integraal onderdeel is van de SIEM/SOC-dienstverlening of een separaat te prijzen component? Daarnaast ontvangen wij graag verduidelijking over de wijze van aanbieden: wordt een all-in jaarprijs verwacht, een prijs per uur, Dagprijs en weekend prijs, per incident, fair use / maximum inzet, of een andere prijsstructuur?	Onduidelijk hoe dit ingeprijst moet worden en of het retainer met additionkele of all-in	Zie antwoord op vraag 83.
324	Programma van Eisen	4.17	4.17	Dient deze Incident Response (IR) retainer onderdeel te zijn van de inschrijfprijs? M.a.w onderdeel te zijn van het prijsinvulformulier? Zo ja, kan Gemeente Steenwijkerhout de hoogte van de retainer aangeven die zij wensen af te nemen?	Het antwoord helpt ons om het prijsinvulformulier in te vullen.	Zie antwoord op vraag 83. Het is voor aanbestedende dienst niet duidelijk wat u bedoelt met de hoogte van de retainer.
325	Bijlage 5 - Programma van Eisen		4.1	Wat wordt hier bedoeld met levering, gezien gebruik gemaakt dient te worden van de Sentinel van opdrachtgever, zijnde een SIEM?		Hoewel het platform (Microsoft Sentinel) door de opdrachtgever ter beschikking wordt gesteld, omvat de 'levering' de volledige inrichting en operationalisering van de SIEM/SOC-dienstverlening.
326	Programma van Eisen		4.17 Incident Response	In 4.17 wordt verwezen naar Incident Response-dienstverlening met vooraf vastgestelde reactietijden en tarieven. Kunt u toelichten hoe deze IR-dienstverlening is ingericht, hoe dit zich verhoudt tot de SOC-dienstverlening en op welke wijze deze inzet financieel is geborgd binnen de budgettering van deze aanbesteding?		De IR-dienstverlening fungeert als escalatieniveau boven de reguliere SOC-dienst: Relatie tot SOC: de 24x7 SOC-dienst verzorgt detectie en eerste respons (containment). Bij complexe incidenten waarvoor diepgaand forensisch onderzoek of crisismanagement nodig is, wordt de IR-dienst geactiveerd. Inrichting: de opdrachtnemer garandeert de beschikbaarheid van een gespecialiseerd IR-team binnen de in de SLA vastgestelde reactietijden. Financiële borging: de paraatheid (beschikbaarheid) van het IR-team dient onderdeel te zijn van de vaste periodieke kosten (retainer). De feitelijke inzeturen bij een incident worden op basis van nacalculatie tegen de vooraf vastgestelde tarieven verrekend. Inschrijvers dienen de bijbehorende tarieven in het prijsinvulformulier op te nemen; hiervoor is een aparte post opgenomen.
327	Programma van Eisen (Bijlage 5)	3	4.12	Klopt het dat uitsluitend gebruik mag worden gemaakt van de bestaande Microsoft Sentinel omgeving en dat het aanbieden van een andere SIEM oplossing, ook als deze volledig door Microsoft wordt ondersteund en geïntegreerd, niet is toegestaan?	Om vast te stellen of eis 4.12 alternatieve SIEM oplossingen volledig uitsluit, ongeacht technische of functionele gelijkwaardigheid	De opdrachtgever bevestigt dat het gebruik van de eigen Microsoft Sentinel-omgeving (binnen de Azure-tenant van de gemeente) een harde eis is. Het aanbieden van een alternatieve SIEM-oplossing is niet toegestaan.
328	Programma van Eisen (Bijlage 5)	4	4.12 en 3.9	Wordt het inzetten van een aanvullende SIEM oplossing naast Microsoft Sentinel (bijvoorbeeld voor specifieke use cases of logopslag) gezien als een afwijking van eis 4.12?	Ter verduidelijking of een hybride SIEM architectuur binnen de kaders van de aanbesteding is toegestaan.	Het inzetten van een aanvullende SIEM-oplossing naast Microsoft Sentinel (bijvoorbeeld voor specifieke use cases of logopslag) wordt gezien als een afwijking van de eis. De aanbestedende dienst vereist dat Microsoft Sentinel de centrale en integrale SIEM-oplossing is voor alle logopslag, correlatie- en detectieactiviteiten binnen de scope van deze opdracht. Een hybride architectuur waarbij logopslag of actieve detectielogica buiten de Azure-tenant van de gemeente plaatsvindt, is niet toegestaan. Dit om de integrale veiligheidsregie, datasoevereiniteit en de beheersbaarheid van het IT-landschap te borgen. Het gebruik van aanvullende analysetooling door de opdrachtnemer is uitsluitend toegestaan, mits dit geen afbreuk doet aan de centrale rol en volledige vulling van de Microsoft Sentinel-omgeving van de gemeente.
329	Programma van Eisen (Bijlage 5)	3	4.12	Is het toegestaan om Microsoft Sentinel vooral te gebruiken voor correlatie en visualisatie, terwijl de feitelijke logverzameling en opslag in een ander platform plaatsvindt?	Om interpretatieverschillen over de rol en positie van Microsoft Sentinel binnen de architectuur te voorkomen.	Nee, dat is niet toegestaan. Een ander platform zal niet overdraagbaar zijn wanneer dienstverlening om welke reden dan ook beëindigd wordt.
330	Programma van Eisen (Bijlage 5)	3-4	4.1 - 4.2 - 4.12	Is het toegestaan dat de 24/7 SOC-dienstverlening wordt geleverd door een (onder)aannemer met een eigen SOC-platform, zolang Microsoft Sentinel het primaire SIEM blijft en alle configuraties overdraagbaar zijn?	Dit om ruimte te verduidelijken voor inzet van externe MDR/SOC-partijen.	De inzet van externe MDR/SOC-partijen is mogelijk. Echter, het is niet toegestaan als tussen additioneel MDR een extra SIEM wordt toegevoegd.
331	GIBIT 2023		Algemeen	Algemeen: Aanbieder meent dat de GIBIT voorwaarden zeer specifiek zijn geschreven voor ICT contracten en derhalve niet geschikt zijn voor, bijvoorbeeld, telecommunicatiediensten en daaraan verbonden diensten. In het commentaar heeft aanbieder niet alleen rekening gehouden met de in de eerste zin genoemde vaststelling, maar ook met het commentaar dat door Nederland ICT is gegeven op de (concept) voorwaarden voor zover dit commentaar voor aanbieder relevant is en niet reeds in de definitieve tekst opgenomen is.		De GIBIT-voorwaarden blijven onverminderd van toepassing.
332	Bijlage 5	4	4.14	Deze eis zijn we nog niet eerder tegenkomen. Wij zijn benieuwd wat de gedachte achter deze eis is. In de praktijk is het de verantwoordelijkheid van de systemen die de logbronnen sturen, het soc kan alleen opvolging doen. Kunt u dit nader toelichten?		De gedachte achter deze eis is het borgen van de continuïteit van de monitoring (health monitoring). De aanbestedende dienst verwacht niet dat de opdrachtnemer technische herstelwerkzaamheden uitvoert aan de bronsystemen van de gemeente. Wel wordt verwacht dat de opdrachtnemer proactief bewaakt of de afgesproken logbronnen daadwerkelijk en ononderbroken data aanleveren aan Microsoft Sentinel. Indien een logstroom onderbroken wordt, dient de opdrachtnemer dit als incident te signaleren aan de gemeente, zodat gezamenlijk actie kan worden ondernomen. Zonder deze controle kan een kritieke 'blind spot' ontstaan zonder dat de gemeente zich hiervan bewust is.
333	Programma van Eisen (Bijlage 5)	10	13	Indien een alternatieve SIEM-oplossing structureel lagere exploitatiekosten oplevert dan Microsoft Sentinel, mag dit financiële voordeel dan worden meegenomen in de beoordeling?	Ter verduidelijking van de rol van kostenoptimalisatie binnen de aanbesteding.	Nee, dit is niet toegestaan. De aanbestedende dienst heeft in de aanbestedingsstukken expliciet gevraagd om een managed dienstverlening op basis van de reeds aanwezige Microsoft Sentinel-tenant van de gemeente. Voorstellen gebaseerd op alternatieve SIEM-oplossingen worden als terzijde gelegd beschouwd, omdat deze niet voldoen aan de gestelde technische uitgangspunten en de gewenste integratie met de bestaande Microsoft-architectuur van de aanbestedende dienst. De financiële beoordeling vindt uitsluitend plaats op basis van de gevraagde dienstverlening conform de besteksvoorwaarden.
334	Bijlage 11 inkoopvoorwaarden GIBIT	26	GIBIT 2023, Art 29 Informatiebeveiliging	Op dit moment lijkt de inschrijver geen toegang tot de het docuemnt informatiebeveiliging en Gemeentelijke ICT-kwaliteitsnormen te hebben. Daarom moeten deze documenten eerst beoordeeld worden door de Inschrijver voordat er enige vorm van goedkeuring kan worden gegeven. Is het mogelijk om deze documenten in te zien of voor nu te laten vervallen?	Verduidelijking of aanpassing op artikel	De aanbestedende dienst gaat niet akkoord met het laten vervallen van de eisen met betrekking tot informatiebeveiliging en de gemeentelijke ICT-kwaliteitsnormen. Deze normen zijn essentieel voor de integriteit en veiligheid van de gemeentelijke infrastructuur. Zie het antwoord op vraag 184. Daarnaast wordt bij deze Nota van Inlichtingen het document Beleid Privacy, informatiebeveiliging en -beheer 2025-2028 gevoegd. Dit document vormt het strategische kader en bevestigt dat de gemeente de BIO (en op termijn de BIO2/Cyberbeveiligingswet) als dwingend normenkader hanteert. Voor zover de inschrijver doelt op de onderliggende tactische uitwerkingen, stelt de aanbestedende dienst vast dat de in dit strategisch beleid genoemde principes (zoals het 'need-to-know'-principe en de 10 bestuurlijke principes) leidend zijn voor de uitvoering van de opdracht. De inschrijver wordt hiermee voldoende in de gelegenheid gesteld om de normen te beoordelen en de naleving ervan te bevestigen.

335	Bijlage 12	alle	alle	Welke logbronnen uit Bijlage 12 zijn verplicht bij livegang? (day-1)?	Dit is cruciaal voor planning en resourceallocatie. Het bepaalt welke connectors en parsingregels direct operationeel moeten zijn om aan de minimale detectiecapaciteit te voldoen.	Zie antwoord op vraag 316.
336	Bijlage 12 huidige situatie	1	1	Graag specificerern op type en aantal:	Tbv scope, design, implementatie, schaal, kosten.	We hebben de bedrijfsgevoelige informatie uit uw vraag gefilterd. Zie antwoord op vraag 316.
337	Bijlage 12 huidige situatie	1	1	Hoeveel netwerken, aub specificeren.	Tbv scope, design, implementatie, schaal, kosten.	Het is voor de aanbestedende dienst niet geheel duidelijk waarom u deze vraag stelt. Graag ontvangt de aanbestedende dienst een toelichting door een vervolgvraag te stellen t.b.v. Nota van Inlichtingen 2.
338	Bijlage 12 huidige situatie	1	1	Zijn netwerken in scope voor deze dienstverlening, zoniet waarom niet?	Tbv scope, design, implementatie, schaal, kosten.	Het is voor de aanbestedende dienst niet geheel duidelijk waarom u deze vraag stelt. Graag ontvangt de aanbestedende dienst een toelichting door een vervolgvraag te stellen t.b.v. Nota van Inlichtingen 2.
339	Bijlage 12 huidige situatie	1	1	Welke Intrusion detection / prevention-systemen worden er gebruikt en zijn deze binnen scope (aantal merk en type)	Tbv scope, design, implementatie, schaal, kosten.	Het is voor de aanbestedende dienst niet geheel duidelijk waarom u deze vraag stelt. Graag ontvangt de aanbestedende dienst een toelichting door een vervolgvraag te stellen t.b.v. Nota van Inlichtingen 2.
340	Bijlage 12 huidige situatie	1	1	Hoeveel medewerkers (op IT netwerken)	Tbv scope, design, implementatie, schaal, kosten.	Aanbestedende dienst is van mening dat deze informatie niet noodzakelijk is voor deze aanbesteding.
341	Bijlage 12 huidige situatie	1	1	Welke netwerkrouters zijn er specifiek in dienst (aantal, merk en type)	Tbv scope, design, implementatie, schaal, kosten.	Het is voor de aanbestedende dienst niet geheel duidelijk waarom u deze vraag stelt. Graag ontvangt de aanbestedende dienst een toelichting door een vervolgvraag te stellen t.b.v. Nota van Inlichtingen 2.
342	Bijlage 12 huidige situatie	1	1	Welke firewall zijn er specifek in dienst (aantal, merk en type)	Tbv scope, design, implementatie, schaal, kosten.	Het is voor de aanbestedende dienst niet geheel duidelijk waarom u deze vraag stelt. Graag ontvangt de aanbestedende dienst een toelichting door een vervolgvraag te stellen t.b.v. Nota van Inlichtingen 2.
343	Bijlage 12	1		Kunt u aangeven hoeveel identities zich binnen de Microsoft-tenant bevinden?		Het is voor de aanbestedende dienst niet geheel duidelijk waarom u deze vraag stelt. Graag ontvangt de aanbestedende dienst een toelichting door een vervolgvraag te stellen t.b.v. Nota van Inlichtingen 2.
344	Huidige situatie	Bijlage 12	1	Kunt u het aantal actieve E5 licenties opgeven?	Het antwoord helpt ons om de gewenste scope correct te duiden.	Op dit moment zijn er 561 van de 600 Microsoft E5 licenties actief.
345	Algemeen			Welke meerwaarde hecht u binnen deze aanbesteding aan een leverancier die aantoonbaar is aangesloten bij het Microsoft Intelligent Security Association (MISA), en daarmee directe toegang heeft tot Microsoft security roadmaps, productteams en best practices rondom XDR, SIEM en identity security?		De aanbestedende dienst hecht waarde aan de mate waarin een leverancier aantoonbaar over diepgaande en actuele expertise van het Microsoft-ecosysteem beschikt. Een lidmaatschap van de Microsoft Intelligent Security Association (MISA) wordt gezien als een positief kwaliteitsaspect dat bijdraagt aan de borging van die expertise en de toekomstbestendigheid van de dienstverlening. De meerwaarde wordt door de aanbestedende dienst met name gezien in de proactieve houding van de leverancier ten aanzien van de Microsoft-roadmap. Dit stelt de leverancier in staat om de gemeente tijdig te adviseren over nieuwe functionaliteiten en noodzakelijke aanpassingen in de SIEM/SOC-configuratie (conform de zorgplicht zoals besproken bij art. 34.4 GIBIT). Het MISA-lidmaatschap is echter geen uitsluitingsgrond of harde eis. Inschrijvers die op andere wijze kunnen aantonen over vergelijkbare toegang tot expertise en best practices te beschikken, worden eveneens uitgenodigd dit toe te lichten in hun kwaliteitsplan.
346	Uitnodiging tot inschrijving	7	1.3.1	Welke plannen/ tijdslijnen zijn er voor de implementatie van Defender for Office 365 P2?	Voor uitnutten van volledige Defender XDR functionaliteit is het gebruik van Defender for Office 365 gewenst. Dit verruimt protectie en detectiemogelijkheden voor de opdrachtgever.	Het door uw genoemde onderdeel valt niet binnen de scope van de opdracht.
347	Uitnodiging tot inschrijving	7	1.3.1	Welke plannen/ tijdslijnen zijn er voor de implementatie van Defender for Cloud Apps?	Voor uitnutten van volledige Defender XDR functionaliteit is het gebruik van Defender for Cloud Apps gewenst. Dit verruimt protectie en detectiemogelijkheden voor de opdrachtgever.	Het door uw genoemde onderdeel valt niet binnen de scope van de opdracht.
348	Uitnodiging tot inschrijving	7	1.3.1	Welke plannen/ tijdslijnen zijn er voor de implementatie van Defender for Servers?	Voor uitnutten van volledige Defender XDR functionaliteit is het gebruik van Defender for Servers gewenst. Dit verruimt protectie en detectiemogelijkheden voor de opdrachtgever.	Serverpark gaat volledig over op Defender for Servers vanaf April 2026. Opdrachtnemer dient hier rekening mee te houden. Zie antwoord op vraag 316 voor meer informatie.
349	Uitnodiging tot inschrijving	7	1.3.1	Kunnen jullie beschrijven hoe Entra ID P2 functionaliteiten zoals Conditional Access, PIM en Access Packages op dit moment gebruikt worden?	Voor uitnutten van volledige Defender XDR functionaliteit is het gebruik van Entra ID P2 gewenst. Dit verruimt protectie en detectiemogelijkheden voor de opdrachtgever.	Conditional Access Policies worden gebruikt voor het verlenen van toegang tot de Microsoft-omgeving. PIM wordt gebruikt door de beheerders voor het aanvragen van administrator-rechten wanneer zij dit nodig hebben. Access Packages worden niet gebruikt.
350	Uitnodiging tot inschrijving	7	1.3.1	Kunnen jullie beschrijven hoe Microsoft Sentinel op dit moment is ingericht? Met name separate subscriptie, Azure Landing Zone?	Om te bepalen of de huidige implementatie van Sentinel herbruikbaar is voor de nieuwe dienstverlening is het belangrijk te weten of de huidige inrichting conform de recommended practices is uitgevoerd.	De huidige inrichting van Microsoft Sentinel is beperkt van opzet en dient door de nieuwe opdrachtnemer gevalideerd en, waar nodig, opnieuw ingericht te worden conform Microsoft Best Practices. Ter verduidelijking van de huidige status: Architectuur: er is momenteel geen sprake van een formele Azure Landing Zone (ALZ) of een separate Azure-subscriptie voor Sentinel. Inrichting: de huidige implementatie is minimaal, waarbij er momenteel 4 actieve data-connectoren operationeel zijn. De opdrachtgever verwacht van de inschrijver dat de transitie en implementatie voorzien in het naar best practices inrichten van de Sentinel-omgeving (inclusief eventuele subscriptiescheiding en integratie in de Azure-omgeving), zodat een schaalbaar en veilig fundament ontstaat voor de 24/7-dienstverlening.
351	Uitnodiging tot inschrijving	7	1.3.1	Wat zijn de huidige procedures voor incidentdetectie en -afhandeling?	Dit is nodig voor de implementatie inschatting	Incidenten in Defender/Sentinel worden bekeken en uitgezocht na ontvangst van de security-threat-notificatie.

352	Uitnodiging tot inschrijving	7	1.3.1	Welke rapportages zijn verplicht en met welke frequentie moeten deze worden aangeleverd?	Dit is nodig voor de implementatie inschatting	De opdrachtgever stelt de volgende eisen aan de rapportagecyclus, mede ter ondersteuning van de jaarlijkse ENSIA-verantwoording en de BIO-normatiek: Maandelijkse Service Rapportage (MSR): een maandelijks op te leveren rapport (formaat PDF) bevattende: Managementsamenvatting: hoofdlijnen over het dreigingsbeeld en de prestaties van de dienst. Operationele statistieken: aantal alerts, incidenten (onderverdeeld naar prioriteit) en de behaalde responstijden (SLA-meting). Trendanalyse: vergelijking met voorgaande periodes. Technisch rapport (op verzoek of via dashboard): inzicht in actieve use cases, bronstatus (health-check van koppelingen) en uitgevoerde wijzigingen in de SIEM-configuratie. Jaarlijks Assurance Rapport (audit-support): een geaggregeerd jaarverslag dat specifiek ingaat op de voor de ENSIA relevante beheersmaatregelen (zoals log-integriteit, monitoringcontinuiteit en incidentafhandeling). Opdrachtnemer dient op verzoek van de auditor van opdrachtgever medewerking te verlenen aan het aanleveren van steekproefsgewijze bewijslast. Incidentrapportage (PIR): na een Prio-1-incident dient binnen 10 werkdagen een Post-Incident Report te worden aangeleverd met een analyse van de oorzaak en aanbevelingen voor preventie. Aanvullend op deze statische rapportages heeft een live dashboard in de Microsoft Sentinel-omgeving de voorkeur voor dagelijks inzicht, mits hieruit ook de bovenstaande rapportages (management en technisch) gegenereerd kunnen worden.
353	Uitnodiging tot inschrijving	7		U geeft aan dat de "verdere inrichting" van Microsoft Sentinel dient plaats te vinden. Maakt de gemeente momenteel al gebruik van Microsoft Sentinel?	Een goed beeld van de Ist situatie draagt bij aan de inschatting van de werkzaamheden voor de onboarding.	De opdrachtgever maakt op dit moment gebruik van Sentinel maar wenst dit uit te breiden.
354	Uitnodiging tot inschrijving SIEM-SOC	8	1.3.3	Aangezien dit een openbare aanbesteding betreft, ontvangen wij graag inzicht in de marktverkenning die aan deze uitvraag is voorafgegaan. Kunt u aangeven welke marktpartijen input hebben geleverd aan deze marktverkenning en hoe is geborgd dat deze partijen geen oneigenlijk voordeel hebben ten opzichte van andere inschrijvers?	Aanbestedingswet, gelijkheids- en transparantiebeginsel	Voor deze marktverkenning heeft de aanbestedende dienst de volgende marktpartijen benaderd: NFIR, ON2IT, IVD, PQR en Orange Cyberdefence. Het doel van de marktverkenning was het verkrijgen van informatie over: (1) de mogelijkheden van SIEM- en SOC-dienstverlening en (2) een indicatie van de daarbij behorende kosten. Tijdens de marktverkenning is geen strategische, essentiële of anderszins inhoudelijke informatie gedeeld die voor één of meerdere deelnemers zou kunnen leiden tot een oneigenlijk voordeel. De aanbestedende dienst ziet derhalve geen risico's ten aanzien van de naleving van het gelijkheids- en transparantiebeginsel.
355	Uitnodiging tot Inschrijving	9	Paragraaf 1.4	U geeft aan de overeenkomst eenzijdig te kunnen verlengen onder gelijkblijvende voorwaarden. Uiteraard wensen we ook een langdurige relatie, maar wensen de eenzijdigheid te vervangen door een wederzijdse instemming. Kunt u dit aanpassen?	Opdrachten met een looptijd van 10 jaar of langer kennen een ander beleid dat aanleiding is tot een verhoogde prijsstelling. Een tweezijdige instemming tot verlenging kent dit niet.	Nee, hier stemt aanbestedende dienst niet mee in.
356	Uitnodiging tot inschrijving	22 en 23	2.1.6 Eisen m.b.t. technische- en beroepsbekwaamheid	In de eisen wordt gesproken over "een overheidsorganisatie met een minimaal aantal van 350 medewerkers". Dit begrip is in de aanbestedingsdocumenten niet nader gedefinieerd. a) Kunt u bevestigen dat onder "overheidsorganisatie" in de context van deze referentie-eis tevens worden verstaan: (i) zelfstandig bestuursorganen, (ii) publiekrechtelijke instellingen, (iii) semipublieke instellingen zoals zorginstellingen en onderwijsinstellingen, en (iv) deelnemingen waarin (lagere) overheden overwegende zeggenschap hebben? b) Indien u bepaalde typen semipublieke organisaties niet onder het begrip "overheidsorganisatie" wenst te laten vallen, verzoeken wij u helder aan te geven welke typen organisaties wél en welke niet worden geaccepteerd als referent, zodat hierover geen interpretatieverschillen kunnen ontstaan bij de beoordeling van de inschrijvingen.	Wij stellen deze vraag om te voorkomen dat door een onduidelijke omschrijving van 'overheidsorganisatie' inschrijvers met relevante ervaring onterecht worden uitgesloten, en om zeker te stellen dat de eis in overeenstemming is met het gelijkheids- en proportionaliteitsbeginsel.	Onder overheidsorganisatie wordt verstaan: 1) zelfstandig bestuursorganen 2) publiekrechtelijke instellingen 3) zorginstellingen, onderwijsinstellingen en woningcorporaties Onder overheidsorganisatie wordt niet verstaan: 4) deelnemingen waarin (lagere) overheden overwegende zeggenschap hebben
357	Uitnodiging tot inschrijving	22 en 23	2.1.6 Eisen m.b.t. technische- en beroepsbekwaamheid	In de eisen bij de kerncompetenties 1 en 2 is bepaald dat de referentieopdracht betrekking moet hebben op "een overheidsorganisatie met een minimaal aantal van 350 medewerkers". Dit sluit referenties uit bij grotere niet-publieke organisaties (bijvoorbeeld commerciële ondernemingen met 500+ medewerkers) die qua schaal, complexiteit, beveiligingsniveau en governance minimaal vergelijkbaar zijn met de nu aanbestede opdracht. a) Kunt u bevestigen dat ook referenties bij niet-overheidsorganisaties zijn toegestaan, mits de organisatie qua omvang, aard van de dienstverlening, beveiligings- en compliancenniveau en complexiteit van de SIEM/SOC-omgeving minimaal vergelijkbaar is met de nu aanbestede opdracht? b) Indien u van mening bent dat uitsluitend referenties bij overheidsorganisaties zijn toegestaan, verzoeken wij u dit nader te motiveren in het licht van het proportionaliteitsbeginsel en de Gids Proportionaliteit, waarin is opgenomen dat geschiktheidseisen in redelijke verhouding moeten staan tot het voorwerp van de opdracht en niet onnodig marktbeperkend mogen zijn.	Wij stellen deze vraag om te voorkomen dat relevante inschrijvers met vergelijkbare ervaring onterecht worden uitgesloten, en om zeker te stellen dat de eis proportioneel is en niet onnodig marktbeperkend werkt, conform het proportionaliteitsbeginsel en de Gids Proportionaliteit.	Niet akkoord, zie de antwoorden op vragen 319 en 356.
358	Uitnodiging tot inschrijving	24	2.2.1 Exploitatiekosten	In de exploitatiekosten wordt Incident Response niet expliciet als afzonderlijke dienst benoemd. Kunt u bevestigen of Incident Response-dienstverlening onderdeel uitmaakt van de exploitatiekosten en, zo ja, onder welke voorwaarden deze dienstverlening binnen scope valt?		Zie antwoord op vraag 83.
359	Prijsinvulformulier / Conceptovereenkomst – Prijsstructuur			De prijsopbouw lijkt deels vast en deels afhankelijk van gebruik en incidentafhandeling. Kunt u bevestigen welke onderdelen van de dienstverlening als vast worden beschouwd en welke variabel zijn, en hoe dit contractueel wordt vastgelegd?		Zie antwoord op vraag 9.
360	PvE	alle	alle	Mogen logbronnen gefaseerd worden aangesloten na livegang? En gaat dit nog veranderen tijden de contractduur?	Deze vraag is belangrijk om de implementatiestrategie en resourceplanning goed af te stemmen. Als gefaseerde aansluiting is toegestaan, kunnen we prioriteit geven aan kritieke bronnen en risico's beter beheersen. Daarnaast willen we weten of de scope van logbronnen tijdens de contractduur kan wijzigen, omdat dit impact heeft op capaciteit, kosten, integratieplanning en SLA-afspraken.	Zie antwoord op vraag 316 voor scope t.b.v. aan te sluiten logbronnen. Het kan voorkomen dat er gedurende de uitvoering van de overeenkomst behoefte is aan het aansluiten van nieuwe logbronnen. Hiervoor worden prijzen gebruikt zoals ingediend in het prijzenblad voor categrie A, B en C logbronnen. Alle logbronnen, vallend binnen de scope van de opdracht, dienen zo snel mogelijk en op een logische volgorde te worden gekoppeld/geïmplementeerd.
361	Bijlage 5 Programma van Eisen	1	eis 2.1	Het verzoek aan gemeente om het aantal aan te sluiten logbronnen te beperken tot degene die daadwerkelijk relevante securityinformatie leveren. Het advies van leverancier is om initieel de volgende logbronnen aan te sluiten: Microsoft Cloud bronnen, firewall, Enterprise EDR / XDR oplossing, NAC platform en Windows servers. Gaat gemeente hiermee akkoord?	Het aansluiten van logbronnen die volgens leverancier nauwelijks bijdragen aan relevante security-informatie leidt uitsluitend tot hogere kosten en levert de gemeente geen enkele meerwaarde op.	Zie antwoord op vraag 316 voor scope t.b.v. aan te sluiten logbronnen. Alle logbronnen, vallend binnen de scope van de opdracht, dienen zo snel mogelijk en op een logische volgorde te worden gekoppeld/geïmplementeerd.

362	PvE	2	3.12	Zijn er agents of hardwarecomponenten uitgesloten conform PvE?	Agents en hardware hebben impact op implementatietijd, beheerlast en security. We willen weten of aanvullende componenten toegestaan zijn om functionaliteit of performance te waarborgen.	De opdrachtgever hanteert het principe van 'cloud-native waar mogelijk' en streeft naar een minimale voetafdruk op de eigen infrastructuur. Agents: de voorkeur gaat uit naar het gebruik van de standaard Microsoft Sentinel-agents (zoals de Azure Monitor Agent – AMA). Het installeren van eigen, bedrijfsspecifieke agents van de opdrachtnemer op servers van de gemeente is in de basis niet toegestaan, tenzij de opdrachtnemer kan aantonen dat dit strikt noodzakelijk is voor de gevraagde functionaliteit en er geen cloud-native alternatief beschikbaar is. Dit vereist expliciete goedkeuring van de TISO. Hardware: het plaatsen van fysieke hardwarecomponenten in het datacenter van de gemeente is uitgesloten. Indien er behoefte is aan een 'log collector' of 'forwarder' op locatie, dient dit te worden gerealiseerd als een virtuele appliance op de bestaande virtualisatie-omgeving van de gemeente. Verantwoordelijkheid: indien de opdrachtnemer aanvullende softwarecomponenten voorschrijft, is de opdrachtnemer volledig verantwoordelijk voor de security, updates en lifecycle-management van deze componenten. Inschrijvers dienen in hun plan van aanpak expliciet te vermelden welke aanvullende componenten (virtueel of softwarematig) zij noodzakelijk achten en hoe de veiligheid en beheerlast daarvan gewaarborgd blijven.
363	Programma van Eisen (Bijlage 5)	1 en 2	3.1 / 3.2	Indien een andere SIEM oplossing aantoonbaar meer standaard use cases en diepere MITRE ATTCK dekking biedt dan Microsoft Sentinel, kan deze dan alsnog worden overwogen binnen de aanbesteding?	Ter verduidelijking of functionele meerwaarde een rol mag spelen naast de voorgeschreven platformkeuze.	Het gebruik van Sentinel staat vast en is een eis,
364	Bijlage 5 Programma van Eisen	1	eis 3.3	Kan de gemeente duidelijkheid geven wat wordt bedoeld met "netwerkdetectie" aangezien dit niet in het document "uitnodiging tot inschrijving" voorkomt?	Leverancier associeert "netwerkdetectie" met Network Detection & Response (NDR). Indien de gemeente verwacht dat leverancier ook NDR aanbied, dan het verzoek aan de gemeente om het aantal actieve systemen op de netwerken en het aantal locaties waar sensoren geplaatst moeten worden te delen met leverancier.	Met de term 'netwerkdetectie' wordt binnen deze uitvraag gedoeld op het monitoren en analyseren van relevante beveiligingsgebeurtenissen op basis van loggegevens afkomstig van de netwerkinfrastructuur (zoals firewalls, switches en VPN-gateways). Dit is een integraal onderdeel van de gevraagde SIEM/SOC-dienstverlening.
365	Bijlage 5 Programma van Eisen	2	eis 3.6	De uitvraag is voor SIEM / SOC dienstverlening. Is de conclusie van leverancier juist dat naast deze dienstverlening gemeente aanvullende dienstverlening wenst? Zo ja, welke additionele dienstverlening wenst gemeente af te nemen?	Deze eis suggereert dat gemeente wellicht aanvullende diensten zoals Web Filtering, Application Control en NDR wil afnemen. Leverancier zou verwachten dat de functionaliteit van de eerste twee diensten onderdeel zijn van de firewall oplossing van de gemeente. Graag zien wij een verduidelijking van deze eis gericht op de uitgevraagde SOC / SIEM dienstverlening.	De opdrachtgever wenst dat de opdrachtnemer niet alleen detecteert, maar ook actieve ondersteuning biedt bij de respons, met name bij P1-incidenten buiten kantoortijden. Geautoriseerde acties: de opdrachtgever verwacht dat de opdrachtnemer in staat is om direct mitigerende maatregelen te nemen op basis van vooraf overeengekomen playbooks. Denk hierbij aan het isoleren van endpoints via Microsoft Defender of het tijdelijk blokkeren van accounts in de cloud-tenant. Netwerkingrijpen: voor ingrepen op netwerkniveau (zoals firewalls) dient de opdrachtnemer de technische expertise in huis te hebben om de ernst te beoordelen en voorstellen te doen voor onmiddellijke blokkades. De feitelijke uitvoering hiervan wordt in overleg met de bereikbaarheidsdienst van de gemeente (of haar beheerder) gedaan, tenzij in de implementatiefase specifieke 'emergency-access'-procedures worden afgesproken. Kwaliteitsborging: inschrijvers dienen in hun plan van aanpak toe te lichten hoe zij deze actieve respons vormgeven en hoe zij de balans bewaken tussen snelheid van ingrijpen en de continuïteit van de gemeentelijke dienstverlening.
366	Bijlage 5 Programma van Eisen	2	eis 3.9	Kan de gemeente bevestigen dat met deze toelichting afdoende aan deze eis wordt voldaan?	Leverancier begrijpt deze eis. Maar in de praktijk zal er altijd enige vorm van afstemming op de systemen en netwerken van de klant moeten plaatsvinden, waardoor het naar overtuiging van leverancier onmogelijk is om geen enkele afhankelijkheid te creëren. Dat is immers inherent aan outscourcing. Wel kan leverancier bevestigen dat er een exit plan zal worden opgesteld en dat het natuurlijk altijd mogelijk is om bij einde van de overeenkomst naar een andere leverancier over te stappen.	De opdrachtgever kan niet bevestigen dat de gegeven toelichting zonder meer afdoende is. De opdrachtgever erkent dat er bij outsourcing altijd sprake is van een operationele relatie, maar eis 3.9 richt zich specifiek op het voorkomen van een technische en intellectuele lock-in. Om aan deze eis te voldoen, dient de opdrachtnemer aan te tonen dat: Standaardisatie: de dienstverlening volledig wordt ingericht binnen de Microsoft Sentinel-tenant van de opdrachtgever, gebruikmakend van standaardfunctionaliteiten (zoals KQL) die zonder propriëtaire tussenkomst van de opdrachtnemer functioneren. Overdraagbaarheid: bij beëindiging van de overeenkomst alle configuraties, scripts, playbooks en use-cases eigendom blijven van (of in onherroepelijk gebruiksrecht zijn bij) de gemeente en direct bruikbaar zijn voor een opvolgende partij. Geen eigendomsbarrières: er geen gebruik wordt gemaakt van specifieke software of licentievormen die eigendom zijn van de opdrachtnemer en die essentieel zijn voor de toegang tot of het gebruik van de verzamelde securitydata. De opdrachtgever verwacht dat de opdrachtnemer in het plan van aanpak expliciet beschrijft hoe deze technische onafhankelijkheid wordt geborgd, ondanks de inherente operationele samenwerking.
367	Programma van Eisen		4.17 Incident Response	In 4.17 wordt een Incident Response-retainer genoemd, maar de scope en inzetvoorwaarden zijn beperkt uitgewerkt. Kunt u verduidelijken welke IR-activiteiten onder de retainer vallen (bijv. voorbereiding, triage, containment, forensics) en hoe deze zich verhouden tot incidentafhandeling binnen de 24×7 SOC-dienstverlening?		Zie antwoord op vraag 9.
368	Bijlage 5 - Programma van Eisen	3	4.3	De Aanbestedende dienst stelt als eis dat contactpersonen en uitvoerende medewerkers van de Opdrachtnemer de Nederlandse taal op niveau B1 beheersen, zowel mondeling als schriftelijk. Binnen de organisatie van Inschrijver is Nederlands de standaard voertaal. Het merendeel van het personeel is Nederlandstalig, aangevuld met enkele Engelstalige SOC-analisten. Indien Inschrijver garandeert dat alle communicatie met de Aanbestedende Dienst in het Nederlands plaatsvindt en uitsluitend in uitzonderlijke situaties (bijvoorbeeld bij incidenten buiten kantoortijden) tijdelijk in het Engels wordt gecommuniceerd om snel te kunnen handelen, is dit dan voor de Aanbestedende Dienst acceptabel?	Om te borgen dat aan deze eis kan worden voldaan en de snelheid van handelen buiten kantoortijden te borgen.	De eis dat communicatie met de aanbestedende dienst in het Nederlands plaatsvindt, blijft onverkort van kracht. De opdrachtgever staat echter toe dat bij incidenten buiten kantoortijden de operationele, technische afstemming tussen de analist van de opdrachtnemer en de technische contactpersoon van de opdrachtgever tijdelijk in het Engels geschiedt, mits dit de snelheid van handelen bevordert. Hierbij gelden de volgende randvoorwaarden: Alle formele berichtgeving, rapportages, overleggen en de uiteindelijke incident-evaluaties dienen in het Nederlands te worden opgeleverd. De vaste contactpersonen (Service Manager, Lead Analist) moeten de Nederlandse taal op minimaal B1-niveau beheersen. Inschrijvers dienen in hun plan van aanpak te beschrijven hoe zij de taalbarrière bij nachtelijke incidenten minimaliseren.
369	Programma van Eisen		Taalvereisten	In de aanbestedingsstukken worden eisen gesteld aan Nederlandstalige communicatie. Kunt u bevestigen of deze eis uitsluitend geldt voor rapportages, documentatie en overleg, en niet voor de operationele bezetting van het SOC?		Zie antwoord op vraag 368.

370	Programma van Eisen		4.3 Taalvereisten	In 4.3 wordt gesteld dat contactpersonen en uitvoerende medewerkers de Nederlandse taal op niveau B1 beheersen, mondeling en schriftelijk. Kunt u toelichten welke medewerkers hiermee concreet worden bedoeld (bijvoorbeeld vaste contactpersonen en overlegrollen versus operationele SOC-medewerkers)?		Onder de taaleis (B1 of hoger) worden de volgende rollen verstaan: Vaste contactpersonen: de Service Manager en Lead Analist/Security Consultant die de tactische en strategische overleggen voeren. Rapportage-rollen: medewerkers verantwoordelijk voor de Nederlandstalige rapportages en documentatie. Voor de operationele SOC-medewerkers (analisten en engineers) die zorgdragen voor de 24x7-monitoring en technische afhandeling, is de beheersing van de Engelse taal acceptabel. De opdrachtnemer dient er echter voor zorg te dragen dat de communicatie bij incidenten te allen tijde begrijpelijk is voor de contactpersonen van de gemeente.
371	Programma van Eisen		4.6 Responstijd	In 4.6 wordt een responstijd van 30 minuten genoemd. Kunt u bevestigen dat deze responstijd betrekking heeft op SOC-dienstverlening (detectie, analyse en escalatie van security events) en niet op de inhoudelijke afhandeling van incidenten of herstelwerkzaamheden?		De responstijd van 30 minuten voor P1-incidenten omvat de volledige keten van detectie, triage, initiële analyse en de eerste noodzakelijke acties tot indamming (containment), zoals beschreven bij de mandaat-acties. De opdrachtgever bevestigt dat deze tijdstelling niet geldt voor de volledige inhoudelijke afhandeling of definitieve herstelwerkzaamheden (remediation), aangezien de doorlooptijd daarvan afhankelijk is van de complexiteit van het incident. Wel wordt verwacht dat de opdrachtnemer na de eerste respons ononderbroken doorwerkt aan de afhandeling conform de afgesproken hersteltijden (SLA).
372	Programma van Eisen		4.8 Contactpersoon	In 4.8 wordt een contactpersoon benoemd. Kunt u bevestigen dat deze rol geen operationele 24×7-functie betreft, maar een aanspreekpunt voor communicatie en afstemming?		De opdrachtgever bevestigt dat de in 4.8 genoemde contactpersoon een tactische en procesmatige rol betreft (bijv. Service Manager of Lead Analist). Deze persoon fungeert als vast aanspreekpunt voor de algemene dienstverlening, rapportages en escalaties tijdens kantoortijden. Voor de operationele 24x7-dienstverlening en acute incidentmeldingen buiten kantoortijden dient de opdrachtnemer te voorzien in een aparte, continu bereikbare ingang (SOC-desk).
373	Programma van Eisen	3	4.8	U geeft aan dat de opdrachtnemer een vast contactpersoon (en vervanger) dient aan te stellen voor o.a. de afhandeling van alle meldingen. Om een 24/7 ondersteuning te kunnen waarborgen werkt onze Security Operation Center (SOC) met ploegendiensten en een model gebaseerd op 1e lijns, 2e lijns en 3e lijns opvolging. Het 24/7 waarborgen van een vast contactpersoon wordt hierdoor lastig. Ons verzoek is om deze specifieke eis te laten vervalllen. Uiteraard stellen wij wel een vast contactpersoon tijdens de implementatie fase aan in de vorm van een projectmanager, en in de operationele fase in de vorm van een Service Delivery Manager.	Het waarborgen van een vastcontactpersoon voor het 24/7 afhandelen van meldingen is niet haalbaar.	De gemeente trekt de eis voor een vaste contactpersoon niet in, maar verduidelijkt deze als volgt: De vaste contactpersoon (en vervanger) is verantwoordelijk voor de tactische en procesmatige regie op de dienstverlening (zoals de genoemde Service Delivery Manager). Deze persoon is het vaste aanspreekpunt tijdens kantoortijden. Voor de operationele 24/7-afhandeling van individuele meldingen en incidenten accepteert de gemeente dat dit wordt uitgevoerd door het roulerende team van het SOC (1e, 2e en 3e lijn). De opdrachtnemer dient er echter voor zorg te dragen dat elke dienstdoende analist toegang heeft tot de klantspecifieke informatie van de gemeente, zodat de continuïteit en kwaliteit van de afhandeling gebordgd zijn.
374	Bijlage 5	9	11.6	Het SOC is 24/7 operationeel. Het SOC is op werkdagen fysiek bemand tot 18:00 uur. Monitoring en detectie vinden continu (24/7) plaats via geavanceerde security tooling. Buiten kantoortijden worden meldingen en alerts 24/7 opgevolgd via de Service Desk, die fungeert als eerste aanspreekpunt en zorgdraagt voor directe triage en doorzetting. Indien een (vermoedde) inbreuk dit vereist, wordt het incident onverwijld geëscaleerd naar SOC-specialisten (Tier-2/Tier-3) en threat hunters, waarna de opdrachtgever conform afspraken wordt geinformeerd. Vraag Wordt binnen deze aanbesteding onder “24/7 bemand SOC” ook een hybride invulling geaccepteerd waarbij het SOC overdag fysiek bemand is, en waarbij buiten kantooruren 24/7 monitoring, Service Desk-triage en directe escalatie naar SOC-specialisten is geborgd, of is een permanent fysiek 24/7 bemande SOC-positie met SOC-analisten een expliciete eis?	In moderne SOC-omgevingen binnen het Microsoft-ecosysteem vindt continue monitoring en detectie grotendeels geautomatiseerd en AI-gedreven plaats. Wij zijn van mening dat het direct escaleren naar een stand-by team met gespecialiseerde SOC-, Tier-2/Tier-3-analisten en threat hunters effectiever is dan een permanente passieve monitoring door één analist. Dit model leidt tot snellere, inhoudelijk sterkere triage en besluitvorming bij (vermoede) inbreuken. Met deze vraag toetsen wij of binnen de aanbesteding ruimte bestaat voor een functioneel gelijkwaardige of effectievere invulling van de 24/7 SOC-eis, waarbij responscapaciteit en kwaliteit centraal staan.	De opdrachtgever stelt als harde eis dat de monitoring, triage en initiële opvolging van security-alerts 24/7 door gekwalificeerde security-analisten (minimaal Tier-1 SOC) wordt uitgevoerd. Een hybride model waarbij de eerste triage buiten kantoortijden wordt uitgevoerd door een generieke (niet-securitygespecialiseerde) Service Desk, wordt niet geaccepteerd als gelijkwaardig. De reden hiervoor is dat de opdrachtgever directe, deskundige beoordeling van alerts vereist om de ‘mean time to detect’ (MTTD) en ‘mean time to respond’ (MTTR) te minimaliseren. Het is de opdrachtnemer toegestaan om de 24/7-bezetting technisch of organisatorisch in te vullen (bijvoorbeeld via een ‘follow-the-sun’-model of een gespecialiseerd nachtteam), mits de functionarissen die de alerts beoordelen aantoonbaar over de juiste security-expertise beschikken. Het escaleren naar Tier-2/Tier-3-specialisten dient onverwijld plaats te vinden na de initiële security-triage.
375	Bijlage 5 Programma van Eisen	9	11.6	Bedoelt u hier 24/7 eyes on glass of is stand-by bij P1 meldingen voldoende?		De opdrachtgever vereist geen continue ‘eyes-on-glass’ bezetting waarbij medewerkers 24/7 fysiek schermen monitoren. Een stand-by/consignatiedienst is acceptabel, mits deze zodanig is ingericht dat de overeengekomen SLA-reactietijden voor P1- en P2-meldingen (bijv. 30 minuten) 24 uur per dag, 7 dagen per week onverkort worden gehaald. De opdrachtnemer dient technisch aan te tonen dat de alarmering (bijv. via automatische paging of telefonische notificatie vanuit de SIEM) robuust genoeg is om deze reactietijden te garanderen zonder constante menselijke observatie.
376	Bijlage 6: CONCEPTOVEREENKOMST	2	2.3	Geldt deze maximale verlenging van 6 maanden na de totale duur van 4 + 3 x 2 jaar is 10 jaar?	Er zijn al 3 reguliere verlengingen in conract waarin discontinuering van de dienstverlening kan worden verkomen.	Dat is correct. De in artikel 2.3 opgenomen verlengingsoptie is aanvullend op de verlengingsoptie(s) uit artikel 2.2. Als na de maximale looptijd van tien jaar zich een situatie voordoet waarin beëindiging van de overeenkomst tot discontinuering van de dienstverlening leidt, kan de overeenkomst door opdrachtgever voor de duur van maximaal zes maanden worden verlengd op grond van artikel 2.3.
377	Bijlage 6: CONCEPTOVEREENKOMST	2	2.5	Naar welk juridisch recht (artikel) van ontbinding wordt verwezen?	Welke voorwaarden van ontbindingn gelden er?	Artikel 2.5 ziet op artikel 4 van de overeenkomst en alle gronden die in de GIBIT-voorwaarden zijn opgenomen voor ontbinding en vernietiging.
378	Bijlage 6: CONCEPTOVEREENKOMST	2	3.2	Kunt u bevestigen dat de eplointatie kosten per jaar vooraf gefactureerd mogen worden?	Duidelijkheid in facturatie schema	Nee, aanbestedende dienst gaat niet akkoord.
379	Conceptovereenkomst	2	4.1 en 4.2	Wij verzoeken u artikel 4.2 te laten vervallen.	De artikelen 4.1 en 4.2 lijken niet met elkaar in overeenstemming. In 4.1 is aangegeven dat in geval van een tekortkoming in de nakoming door een partij, de andere partij hem - uitzonderingen daargelaten - in gebreke zal stellen. In 4.2 is aangegeven dat niet nakoming als een tekortkoming kwalificeert en dat de andere partij alsdan bevoegd is per direct (dus zonder voorafgaande ingebrekestelling) te ontbinden. Wij menen dat de in artikel 4.1 neergelegde regeling, die in feite overeenkomt met de wettelijke regeling, zou moeten worden gehandhaafd en de regeling in 4.2 zou moeten vervallen. In ieder geval zou moeten worden verduidelijkt wat in welk geval geldt.	Niet akkoord. Zie het antwoord op vraag 138.

380	conceptovereenkomst		4.2	Is de aanbestedende dienst bereid om: a) Audit-frequentie te beperken tot maximaal 1x per jaar (tenzij gegronde vermoeden van schending)? b) Audits alleen tijdens normale kantooruren toe te staan met minimaal 2 weken vooraankondiging? c) Kosten van audits voor rekening van opdrachtgever te laten komen, tenzij de auditor materiële tekortkomingen constateert? d) Bij Dienstverlening op Afstand opdrachtnemer toe te staan om te volstaan met een jaarlijkse TPM/ISAE3402 rapportage in plaats van klant-specifieke audits?	Artikel 4.2 concept verwerkersovereenkomst en artikel 25 GIBIT 2023 geven opdrachtgever uitgebreide auditrechten zonder beperkingen.	a. Niet akkoord, de audit frequentie zal naar redelijkheid worden ingevuld. De frequentie hangt mede af van externe ontwikkelingen die buiten de invloedssfeer van de opdrachtgever liggen (o.a. nieuwe dreigingsbeelden / inzichten). b.De aanbestedende dienst gaat gedeeltelijk akkoord. De audits mogen alleen plaatsvinden tijdens normale kantooruren en met een vooraankondiging van ten minste 30 dagen. c. Niet akkoord. Zie artikel 4.2: De kosten van deze audit worden gedragen door Verwerkingsverantwoordelijke (zowel eigen kosten als kosten van Verwerker), tenzij de auditor één of meer tekortkomingen van niet ondergeschikte aard van Verwerker constateert die ten nadele zijn van Verwerkingsverantwoordelijke. d. Niet akkoord. Externe audits en de invulling hiervan gebeurd in samenspraak met de opdrachtgever. Het is de aanbestedende dienst onduidlijk wat er met dienstverlening op afstand bedoeld wordt.
381	conceptovereenkomst		4.3	Kan de aanbestedende dienst bevestigen dat: a) Verwerking binnen de EU/EER voldoende is (geen specifieke landvereisten)? b) Microsoft's Standard Contractual Clauses en EU-US Data Privacy Framework voldoende waarborgen bieden? c) Opdrachtnemer niet verantwoordelijk is voor wijzigingen in Microsoft's datacenter-locaties zolang deze binnen EER blijven?	Artikel 4.3 concept verwerkersovereenkomst staat verwerking buiten EER toe onder voorwaarden. Microsoft Sentinel is een global cloud platform van Microsoft.	A. De aanbestedende dienst bevestigt dit. B. De aanbestedende dienst bevestigt dit en formuleert het als volgt: opdrachtnemer waarborgt dat internationale doorgifte van persoonsgegevens plaatsvindt op basis van de geldende EU Standard Contractual Clauses, aangevuld met het EU-US Data Privacy Framework en passende aanvullende maatregelen. C. De aanbestedende dienst bevestigt dit.
382	conceptovereenkomst		5.1	Is de aanbestedende dienst bereid om: a) De meldtermijn te verlengen naar 72 uur conform AVG artikel 33? b) Te specificeren dat de 24/72-uurs termijn geldt vanaf het moment dat opdrachtnemer redelijkerwijs had moeten weten dat er een datalek is, niet vanaf eerste vermoeden?	Artikel 5.1 van de concept verwerkersovereenkomst vereist melding van een datalek binnen 24 uur. Voor een SOC die zelf security-incidenten onderzoekt is dit zeer kort. Het kan langer duren om te bepalen of er daadwerkelijk een datalek is conform AVG-definitie.	a. Niet akkoord. b. Niet akkoord.
383	Conceptovereenkomst	3	5.2	Wij verzoeken u de laatste zin van artikel 5.2 als volgt te wijzigen: "Tevens komen alle redelijke kosten die opdrachtgever maakt voor herstel van eventuele schade en de redelijke marktconforme meerkosten voor het alsnog uitvoeren van de opdracht door een derde voor vergoeding in aanmerking."	In het geval de opdrachtnemer tekort zou schieten en de opdrachtgever zich daardoor genoodzaakt zou zien de opdracht verder door een derde te laten verrichten, dan impliceert dit dat de opdrachtgever geen verdere kosten verschuldigd is aan de opdrachtnemer, maar in plaats daarvan aan de derde. Het is in dat geval niet redelijk om de totale kostenvergoeding die de opdrachtgever aan de derde betaalt bij de opdrachtnemer in rekening te brengen. Zou de opdrachtnemer immers de opdracht zelf verder hebben uitgevoerd, dan zou de opdrachtgever ook die kosten hebben gemaakt. Alleen indien door de vervanging van de opdrachtnemer door de derde meer kosten zouden zijn verschuldigd door opdrachtgever aan de derde is het redelijk deze bij opdrachtnemer als schade te vorderen, waarbij die te vorderen (meer)kosten bovendien marktconform dienen te zijn.	Akkoord.
384	conceptovereenkomst		5.2 en 5.4	Kan de aanbestedende dienst specificeren: a) Wat de verwachte omvang van ondersteuning is (bijv. verstrekken van technische informatie vs. uitgebreid forensisch onderzoek)? b) Dat uitgebreid forensisch onderzoek, juridische analyse en externe communicatie als meerwerk worden beschouwd? c) Dat kosten voor externe specialisten (forensische experts, juridisch adviseurs) voor rekening van opdrachtgever komen?	Artikel 5.2 en 5.4 concept verwerkersovereenkomst verplichten opdrachtnemer om "alle maatregelen" te nemen en de gemeente te "ondersteunen waar nodig" bij melding. Deze termen zijn vaag en voor meerdere uitleg vatbaar.	a) Zoals beschreven in PvE eis 4.17. De exacte omvang kunnen wij vooraf niet aangeven. Zie ook antwoord op vraag 9. b) Uitgangspunt is dat voor werkzaamheden vallend onder eis 4.17 het uurtarief wordt gehanteerd zoals opgenomen in het prijzenblad. c) De aanbestedende dienst bevestigd dit naar redelijkheid mochten er voor de opdrachtnemer gespecialiseerde externe specialisten ingezet moeten worden die niet binnen de het cybersecurirty / IT vakgebied valt zoals forensische experts en juridisch adviseurs.
385	conceptovereenkomst		10.1	Artikel 10.1 van de conceptovereenkomst (Bijlage 6) stelt dat "de opdrachtnemer aansprakelijk is voor alle schade" zonder enige beperking. Dit lijkt in strijd met de aansprakelijkheidsbeperkingen in GIBIT 2023. Gegadigde is van mening dat het stellen van een onlimiteerde aansprakelijkheid disproportioneel is. Kan de aanbestedende dienst bevestigen dat: a) De aansprakelijkheidsbepalingen van GIBIT 2023 (artikel 16) prevaleren boven artikel 10.1 van de conceptovereenkomst? b) Artikel 10.1 van de conceptovereenkomst zal worden aangepast of geschrapt om consistentie met GIBIT 2023 te waarborgen?	Gegadigde behoort tot een internationale beursgenoteerde onderneming. De corporate governance van beursgenoteerde bedrijven verzet zich tegen de acceptatie van onbeperkte aansprakelijkheden. Daarnaast is het vereisen van een ongelimiteerde aansprakelijkheid in strijd met voorschrift 3.9 van de Gids Propotionaliteit.	Het is de aanbestedende dienst onduidelijk naar welk artikel u verwijst. Er is echter geen sprake van ongelimiteerde aansprakelijkheid. Naast de aansprakelijkheidsbepalingen van de overeenkomst zijn tevens de bepalingen van de GIBIT 2023 van toepassing.
386	conceptovereenkomst		11.2	Kan de aanbestedende dienst bevestigen dat: a) De betalingstermijn 30 dagen na factuurdatum is	Artikel 11.6 GIBIT 2023 stelt een betalingstermijn van 30 dagen. De conceptovereenkomst artikel 11.2 specificeert geen termijn.	Dit kan de aanbestedende dienst niet bevestigen. De betalingstermijn van 30 dagen gaat in na ontvangst van de factuur door aanbestedende dienst.
387	GIBIT		8.1	Kan de aanbestedende dienst bevestigen dat: a) Opdrachtnemer alleen gehouden is aan de normen zoals deze luiden bij contractsluiting (2025)? b) Wijzigingen in de normen tijdens de 10-jarige looptijd niet automatisch van toepassing zijn? c) Implementatie van nieuwe normen als meerwerk wordt beschouwd?	Artikel 8.1 GIBIT 2023 bepaalt dat de ICT Prestatie moet voldoen aan de ten tijde van het sluiten van de overeenkomst in de Gemeentelijke ICT-kwaliteitsnormen voorgeschreven eisen.	Niet akkoord. Nieuwe versies van de Gemeentelijke ICT-kwaliteitsnormen zijn uitdrukkelijk wel van toepassing. In de Gemeentelijke ICT-kwaliteitsnormen is uitgeschreven welke normen opgenomen zijn en worden. Dit betreft normen en standaarden die verplicht zijn. De verplichting kan volgen uit: 1. Een wettelijk kader; en/of 2. Standaarden op de lijst van open standaarden (pas-toe-of-leg-uit); en/of 3. Standaarden die als landelijke gemeentelijke standaard of norm door VNG/KING zijn vastgesteld. Het betreft dus normen waarvoor in alle gevallen procedures zijn waarmee ze vastgesteld worden. Leverancier wordt geacht op de hoogte te zijn van de (door)ontwikkeling van standaarden die voor haar van belang zijn. Leveranciers hebben daarnaast vaak de mogelijkheid te participeren in de vaststellingsprocedures die voor de normen gelden. Tot slot is vaak sprake van invoeringstermijnen, waarmee ook tijd beschikbaar wordt gesteld om aan de verplichting te voldoen.
388	GIBIT		10.12 lid i	Kan de aanbestedende dienst bevestigen dat: a) Compliance-updates binnen de kaders van regulier onderhoud vallen alleen als deze met beperkte inspanning kunnen worden geïmplementeerd? b) Fundamentele wijzigingen in wetgeving die substantiële herontwikkeling vereisen als meerwerk worden beschouwd? c) Er een materiality threshold geldt (bijvoorbeeld wijzigingen >5% jaarvergoeding zijn meerwerk)?	Artikel 10.12 lid i GIBIT 2023 garandeert dat de ICT Prestatie steeds tijdig zal blijven voldoen aan relevante wet- en regelgeving, en artikel 12.1 lid v stelt dezelfde garantie. Nieuwe cybersecurity-wetgeving zoals NIS2, DORA of de AI Act kan substantiële aanpassingen vereisen.	a. Niet akkoord. b. Niet akkoord. c. Niet akkoord.
389	GIBIT		12.1	Is de aanbestedende dienst bereid om te erkennen dat: a) SOC/SIEM-dienstverlening een inspanningsverplichting is en geen resultaatsverbintenis? b) Garanties alleen gelden voor objectief meetbare SLA's (response times, beschikbaarheid, etc.), niet voor security outcomes? c) Opdrachtnemer niet aansprakelijk is voor security-incidenten die ondanks "best practice" maatregelen toch plaatsvinden?	Artikel 12.1 GIBIT 2023 stelt garanties als resultaatsverbintenis met omgekeerde bewijslast (artikel 12.2-12.3). Voor SOC/SIEM-dienstverlening is een absolute garantie op security outcomes onrealistisch: •Been enkele SOC kan 100% van aanvallen detecteren •Nieuwe zero-day exploits kunnen initieel ondetecteerbaar zijn •Geavanceerde persistent threats kunnen maanden onopgemerkt blijven	a. Niet akkoord. b. Niet akkoord. c. Niet akkoord.

390	GBIT		16	Is de aanbestedende dienst bereid om in de overeenkomst expliciet op te nemen dat de opdrachtnemer niet aansprakelijk is voor: • Indirecte schade en gevolgschade • Gederfde winst, omzetverlies en verlies van besparingen • Verlies van goodwill en reputatieschade • Schade door bedrijfsstagnatie • Aanspraken van derden (behalve bij IP-schending) met uitzondering van gevallen van opzet of grove schuld?	De GIBIT 2023 inkoopvoorwaarden bevatten geen expliciete uitsluiting van indirecte schade, gevolgschade, gederfde winst, omzetverlies of reputatieschade. Aansprakelijkheid voor indirecte schade is niet verzekerbaar binnen de IT-branche.	Zie het antwoord op vraag 141.
391	GIBIT		16.5 lid iv	Gegadigde behoort tot een internationale beursgenoteerde onderneming. De corporate governance van beursgenoteerde bedrijven verzet zich tegen de acceptatie van onbeperkte aansprakelijkheden. Artikel 16.5 lid iv van de GIBIT sluit de aansprakelijkheidsbeperking uit voor door de toezichthoudende autoriteit opgelegde boetes. Dit betekent dat de opdrachtnemer onbeperkt aansprakelijk is voor AVG-boetes die aan de gemeente worden opgelegd maar ook aan de leverancier opgelegd hadden kunnen worden. Gegadigde erkent dat betrokkenen die bij van het verwerken van persoonsgegevens materiele of immateriële schade hebben geleden als gevolg van een inbreuk op de AVG door een verwerker dit rechtstreeks (op grond van art 82) bij de verwerker kunnen verhalen. Eveneens erkent Gegadigde de regel dat autoriteiten, op grond van art 83 AVG, rechtstreeks aan de verwerker een boete kunnen opleggen in geval van schending van de AVG door de verwerker. Gegadigde meent echter dat het niet proportioneel is om de contractuele aansprakelijkheid tussen partijen voor schade die kan ontstaan bij verwerken van persoonsgegevens niet te limiteren. Zo acht Gegadigde het niet proportioneel en evenredig dat een verwerkingsverantwoordelijke een boete die zij als verantwoordelijke heeft ontvangen van de Autoriteit Persoonsgegevens (AP) ongelimiteerd kan doorzetten als schade aan de verwerker. Gegadigde overweegt hierbij het volgende: Bij de contractuele aansprakelijkheid gaat het uiteraard om vergoeden van opgetreden schade, terwijl een boete geen schade is vanwege het punitieve aspect. Wanneer de bevoegde toezichthouder zoals de AP een boete oplegt aan de verwerkingsverantwoordelijke is er blijkbaar iets verwijtbaar misgegaan bij de verwerkingsverantwoordelijke. Indien de AP dan een boete oplegt aan de verwerkingsverantwoordelijke, is deze boete tot stand gekomen op basis van diverse aspecten die enkel en alleen gebaseerd zijn op de verwerkingsverantwoordelijke, conform EDPB Guidelines 04/22 on the calculation of administrative fines under the GDPR, en niet op eventuele opdrachtnemers zoals de verwerker. De AP zal alleen een boete aan de betrokken verwerker opleggen, vastgesteld op de factoren van toepassing op de verwerker en de door die partij gemaakte overtreding. Zo kan het voorkomen dat in een boete opgelegd aan de verwerkingsverantwoordelijke eerdere gemaakte fouten bij de verwerkingsverantwoordelijke zijn meegewogen, of andere overtredingen die te maken hebben met het plichten van verwerkingsverantwoordelijke partij, zoals de mate van (niet) meewerken aan het onderzoek van de AP. Deze zaken hebben echter niets van doen met de rol en verantwoordelijkheden van de opdrachtnemer als verwerker.	Vanwege de bestuursrechtelijke aspecten van een boete opgelegd aan de opdrachtgever als verwerkingsverantwoordelijke, is de opdrachtnemer die als verwerker de opgelegde boete doorgeschoven zou krijgen, vaak niet aan te merken als belanghebbende en hierdoor niet ontvankelijk om beroep of bezwaar aan te tekenen tegen een dergelijk besluit.Gelet op het bovenstaande verzoekt Gegadigde u om in geval van schade in verband met het verwerken van persoonsgegevens, de contractuele aansprakelijkheid tussen partijen te beperken op de wijze zoals bedoeld in art 16.4 GIBIT. Is de Aanbestedende Dienst hiertoe bereid? Indien een beperking van aansprakelijkheid bij de verwerking van persoonsgegevens door aanpassing van art 16.5 lid iv voor de Aanbestedende Dienst niet acceptabel wordt geacht, zou Gegadigde de volgende aanpassing willen voorstellen: Art 16.5 lid iv: in geval van aanspraken op schadevergoeding ten gevolge van schending van wet- en regelgeving op het terrein van de bescherming van persoonsgegevens of handelen in strijd met de rechtmatige instructies van de verwerkingsverantwoordelijke. Onder schade wordt mede begrepen een door de toezichthoudende autoriteit opgelegde boete, met in achtneming van: (i) voor zover die boetes ook rechtstreeks aan Leverancier hadden kunnen worden opgelegd, maar niet zijn opgelegd; en (ii) onder de voorwaarde dat Opdrachtgever Leverancier: (a.) onverwijld schriftelijk informeert over een door een toezichthoudende autoriteit gestart onderzoek dat kan leiden tot een boete alsmede over en het bestaan en de inhoud van de opgelegde boete; en (b.) Leverancier volledig betrekt bij het voeren van verweer tegen die boete althans het aan Leverancier toe te rekenen deel van die boete. Artikel 16.5 lid iv van de GIBIT 2023 inkoopvoorwaarden sluit de aansprakelijkheidsbeperking uit voor door de toezichthoudende autoriteit opgelegde boetes. Dit betekent dat de opdrachtnemer onbeperkt aansprakelijk is voor AVG-boetes die aan de gemeente worden opgelegd maar ook aan de leverancier opgelegd hadden kunnen worden.	Niet akkoord, zie de antwoorden op vragen 226 t/m 229.
392	GIBIT		20.4	Artikel 20.4 GIBIT 2023 bepaalt dat alle rechten op Maatwerkprogrammatuur bij opdrachtgever berusten en inclusief broncodes worden overgedragen. Voor SOC/SIEM-dienstverlening gebruikt de opdrachtnemer proprietary tools, methodologieën en componenten zoals: • Threat detection rules, playbooks en runbooks • Security automation scripts en workflows • Threat intelligence databases en correlation rules • Analyse-methodologieën en frameworks • Dashboards, rapportage-templates en visualisaties Deze zijn herbruikbaar en worden ingezet voor meerdere klanten, maar kunnen tijdens de uitvoering worden aangepast/uitgebreid. Is de aanbestedende dienst bereid te erkennen dat: a) Pre-existing IP, achtergrond-IP, tools, methodologieën, frameworks en herbruikbare componenten van opdrachtnemer eigendom blijven van opdrachtnemer? b) Opdrachtgever een niet-exclusieve licentie krijgt voor gebruik van dergelijk IP uitsluitend voor de doeleinden van deze overeenkomst? c) Alleen unieke, klant-specifieke detectie-regels en configuraties die specifiek voor gemeente Steenwijkerland zijn ontwikkeld en niet herbruikbaar zijn, als maatwerk kunnen worden beschouwd? d) Opdrachtnemer gerechtigd is om algemene kennis, ervaring en herbruikbare componenten uit dit project te gebruiken voor andere klanten (zonder vertrouwelijke informatie van opdrachtgever)?	Pre-existing IP, achtergrond-IP, tools, methodologieën, frameworks en herbruikbare componenten van opdrachtnemer behoren tot het bedrijfsdebiet van Gegadigde, Het is redelijk en proportineel dat deze worden uitgezonderde van overdracht naar klanten.	De opdrachtgever gaat akkoord met de volgende verduidelijking van artikel 20.4 GIBIT: a) Eigendom: de eigendomsrechten van pre-existing IP en generieke methodologieën blijven bij de opdrachtnemer. b) Licentie: voor zover dit IP noodzakelijk is voor het gebruik van de dienst, verleent opdrachtnemer aan de opdrachtgever een onvoorwaardelijk, eeuwigdurend en overdraagbaar gebruiksrecht. c) Configuraties in de tenant: alle klantspecifieke inrichting, waaronder maar niet beperkt tot detectieregels, playbooks, scripts en dashboards die binnen de Microsoft Sentinel-tenant van de gemeente zijn gecreëerd of aangepast, worden beschouwd als resultaten waarvan de gebruiksrechten bij de gemeente berusten. De gemeente moet deze na beëindiging van de overeenkomst zelfstandig of met een derde partij kunnen blijven exploiteren. d) Kennis: opdrachtnemer mag algemene kennis en ervaring hergebruiken, mits deze niet herleidbaar is naar de gemeente of haar data. Hiermee wordt geborgd dat de intellectuele eigendommen van de opdrachtnemer beschermd zijn, terwijl de continuïteit van de beveiliging voor de gemeente na contracteinde gewaarborgd blijft.
393	GIBIT		20.4	In het verlengde van de vorige vraag: Artikel 20.4 GIBIT 2023 verplicht tot het ter beschikking stellen van alle broncodes van Maatwerkprogrammatuur. Kan de aanbestedende dienst bevestigen dat deze verplichting niet geldt voor: a) Pre-existing tools en scripts van opdrachtnemer? b) Proprietary detection algorithms en methodologieën? c) Derdenprogrammatuur (zoals Microsoft Sentinel)?	Pre-existing IP, achtergrond-IP, tools, methodologieën, frameworks en herbruikbare componenten van opdrachtnemer behoren tot het bedrijfsdebiet van Gegadigde, Het is redelijk en proportineel dat deze worden uitgezonderde van overdracht naar klanten.	De opdrachtgever bevestigt dat de verplichting tot overdracht van broncode niet geldt voor: a) Pre-existing tools: software en scripts die de opdrachtnemer reeds vóór de overeenkomst in eigendom had en die als 'gereedschap' worden gebruikt. b) Proprietary algorithms: de interne intellectuele methodieken van de opdrachtnemer. c) Derdenprogrammatuur: software van partijen zoals Microsoft (Sentinel/Azure), waarvoor de reguliere licentievoorwaarden van de betreffende fabrikant gelden. Echter, deze uitzondering geldt uitdrukkelijk niet voor de configuraties en scripts die specifiek ten behoeve van de dienstverlening binnen de Microsoft Sentinel-tenant van de gemeente worden ontwikkeld of aangepast. Alle KQL-queries, playbooks (Logic Apps), workbooks en automatiseringsscripts die onderdeel uitmaken van de inrichting voor de gemeente, dienen volledig transparant en beschikbaar te zijn voor de opdrachtgever. De opdrachtgever behoudt het recht om deze configuraties na beëindiging van de overeenkomst te blijven gebruiken.
394	GIBIT		20.5	Kan de aanbestedende dienst bevestigen dat: a) De IP-vrijwaring van artikel 20.5 GIBIT 2023 niet geldt voor claims gerelateerd aan Microsoft Sentinel zelf? b) Opdrachtnemer alleen aansprakelijk is voor eigen toevoegingen aan Sentinel, niet voor het platform zelf?	De gemeente verplicht het gebruik van Microsoft Sentinel als SIEM-oplossing. Opdrachtnemer is afhankelijk van Microsoft's licentievoorwaarden.	A. De aanbestedende dienst bevestigt dit. B. De aanbestedende dienst bevestigt dit.
395	GIBIT		22.3	Is de aanbestedende dienst bereid om: a) Te bevestigen dat opdrachtnemer NIET aansprakelijk is voor gebreken in Microsoft Sentinel zelf? b) Te bevestigen dat opdrachtnemer alleen aansprakelijk is voor eigen configuratie-fouten, niet voor platform-bugs? c) De verplichting uit artikel 22.4 GIBIT om "alle redelijke inspanningen" te betrachten voor het oplossen van Sentinel-bugs te schrappen of te beperken tot rapportage aan Microsoft?	Artikel 22.3 GIBIT 2023 bepaalt dat gebreken in Derdenprogrammatuur niet als gebrek worden beschouwd, tenzij leverancier de fout had behoren te kennen en het effect redelijkerwijs vermeden had kunnen worden. Microsoft Sentinel is een complex cloud-platform met regelmatige updates. Bugs in Sentinel kunnen niet door opdrachtnemer worden voorkomen.	A. De aanbestedende dienst bevestigt dit. B. De aanbestedende dienst bevestigt dit. C. Niet akkoord.
396	GIBIT		24.4 en 24.5	Is de aanbestedende dienst bereid om: a) Bij beëindiging op deze gronden ook een redelijke winstmarge voor de resterende contractperiode te vergoeden (niet alleen gemaakte kosten en gederfde winst zoals in artikel 24.6 staat)? b) Een minimale contractduur te garanderen (bijvoorbeeld 3 jaar) waarin deze beëindigingsrechten niet gelden?	Artikel 24.4 en 24.5 GIBIT 2023 geven opdrachtgever uitgebreide eenzijdige beëindigingsrechten bij gemeentelijke herindeling, uitbesteding aan gemeenschappelijke regeling of overstap op landelijke voorziening. Voor een 10-jarig contract creëert dit aanzienlijke onzekerheid.	Niet akkoord.

397	GIBIT		26.5 en 26.7	Kan de aanbestedende dienst bevestigen dat: a) Exit-verplichtingen beperkt zijn tot wat technisch mogelijk is binnen Microsoft Sentinel's mogelijkheden en API's? b) Kosten voor data-export uit Microsoft Sentinel (bijvoorbeeld naar andere SIEM-platforms) voor rekening van opdrachtgever komen? c) Opdrachtnemer niet aansprakelijk is voor beperkingen of kosten die Microsoft oplegt voor data-export of platformmigratie?	Artikel 26.5-26.7 GIBIT 2023 verplicht opdrachtnemer bij beëindiging om opdrachtgever in staat te stellen over te stappen naar een andere leverancier, inclusief gegevensmigratie en ontvlechting. Microsoft Sentinel is een cloud-platform van Microsoft waar opdrachtnemer geen volledige controle over heeft.	De opdrachtgever reageert als volgt op de gevraagde bevestigingen: a) Technische mogelijkheden: de opdrachtnemer dient binnen de kaders van de op dat moment beschikbare Microsoft-technologie (zoals API's en exporttools) maximale medewerking te verlenen aan de exit. Van de opdrachtnemer wordt verwacht dat zij de benodigde expertise levert om deze middelen effectief in te zetten. b) Kosten data-export: de directe infrastructuurkosten die Microsoft in rekening brengt voor data-export (zgn. 'egress costs') komen voor rekening van de opdrachtgever. De uren die de opdrachtnemer besteedt aan het faciliteren van deze export vallen onder de medewerkingsplicht (zie ook het antwoord op vraag [verwijs naar eerdere vraag over art. 21.2]). c) Aansprakelijkheid derden: de opdrachtnemer is niet aansprakelijk voor prijswijzigingen of technische beperkingen die door Microsoft (als platformleverancier) eenzijdig worden opgelegd, mits de opdrachtnemer de opdrachtgever hierover proactief adviseert en naar redelijkheid alternatieve scenario's onderzoekt.
398	Gibit2040		29	In dit artikel wordt verwezen naar de Gemeentelijke ICT-kwaliteitsnormen ofwel een andere overeengekomen norm voor informatiebeveiliging. Kunt u aangeven welke normen relevant zijn in dit concrete geval en zou u - waar nodig - nader invulling willen geven aan de toepasselijke normen?		Zie het antwoord op vraag 184. Daarnaast wordt onder 'andere overeengekomen norm' de Baseline Informatiebeveiliging Overheid (BIO) verstaan. De BIO is gebaseerd op de ISO 27001/27002-standaarden en is specifiek toegesneden op de Nederlandse overheidscontext. Aanvullend op de BIO zijn de volgende kaders relevant voor de uitvoering van de SIEM/SOC-dienstverlening: NCSC-richtlijnen: voor de inrichting van logging, detectie en incidentrespons. AVG (Algemene Verordening Gegevensbescherming): gezien de verwerking van loggegevens die persoonsgegevens kunnen bevatten. BIO-2 (indien van kracht): gezien de looptijd van het contract dient de opdrachtnemer rekening te houden met de transitie naar de opvolger van de BIO (op basis van NIS2-wetgeving). De opdrachtnemer wordt geacht de dienstverlening gedurende de gehele contractduur in overeenstemming met deze normen uit te voeren en de gemeente proactief te adviseren over noodzakelijke aanpassingen als gevolg van wijzigingen in deze normen.
399	GIBIT		34.3 en 34.4	Kan de aanbestedende dienst bevestigen dat: a) Opdrachtnemer niet aansprakelijk is voor (tijdelijke) verstoringen veroorzaakt door Microsoft-updates? b) Opdrachtnemer redelijke inspanningen levert om gemeente te informeren over geplande Microsoft-updates, maar niet verantwoordelijk is voor onverwachte updates?	Artikel 34.3-34.4 GIBIT 2023 bepaalt dat bij generieke Dienstverlening op Afstand leverancier updates/upgrades installeert en opdrachtgever deze niet kan weigeren. Microsoft Sentinel wordt door Microsoft geüpdatet. Opdrachtnemer heeft hier beperkte controle over.	De aanbestedende dienst bevestigt het volgende: a) Aansprakelijkheid: de opdrachtnemer is niet aansprakelijk voor schade die direct voortvloeit uit (tijdelijke) verstoringen in de Microsoft-infrastructuur zelf, mits de opdrachtnemer kan aantonen dat zij de zorgplicht van een goed opdrachtnemer heeft vervuld. Dit houdt in dat de opdrachtnemer direct na het bekend worden van de verstoring maatregelen neemt om de impact op de dienstverlening te minimaliseren. b) Informatievoorziening: de opdrachtnemer wordt geacht redelijke inspanningen te verrichten om de gemeente te informeren over relevante updates. Voor onverwachte updates geldt een inspanningsverplichting om de impact hiervan achteraf zo snel mogelijk te analyseren en de gemeente hierover te adviseren. De opdrachtnemer blijft echter verantwoordelijk voor het beheer van de configuraties (zoals rules en playbooks) die door updates geraakt kunnen worden. Het onjuist functioneren van de dienst door een gebrek aan onderhoud op deze configuraties na een update valt binnen de risicosfeer van de opdrachtnemer.
400	Bijlage 3 - Prijsinvulformulier en Bijlage 12 - Huidige situatie			Met de nieuwe Bijlage 12 zijn de high level assets niet meer in lijn met de prijs per logbron categorie (A, B, C) in het prijsinvulformulier. Zou u toch nadere informatie willen verschaffen zodat wij onze prijzen daarop kunnen afstemmen?	Momenteel hebben we te weinig informatie voor een goede inschatting van de kosten.	De opdrachtgever heeft in het vertrouwelijke Bijlage 12 detailinformatie een gedetailleerd overzicht gegeven van de aanwezige infrastructuur en de aan te sluiten bronnen. Dit document is uitsluitend beschikbaar voor geïnteresseerde partijen en kan tot uiterlijk de deadline van inschrijvingen worden opgevraagd via TenderNed (berichtenmodule). De geïnteresseerde partij verklaart dat het verstrekte document uitsluitend zal worden gebruikt ten behoeve van het voorbereiden en indienen van een inschrijving in het kader van deze aanbesteding. De partij zal het document niet aan derden verstrekken, noch geheel of gedeeltelijk kopiëren of anderszins gebruiken voor andere doeleinden. Na afronding van de aanbestedingsprocedure, ongeacht de uitkomst daarvan, zal de partij het document onverwijld vernietigen.