Ref. Nr.	Onderwerp	Vraag	Antwoord
1	Vragenronde 1	Verwijzing: GIBIT 2023 Artikel 18.1 In de aanbestedingsdocumenten wordt verwezen naar GIBIT 2023. In artikel 18.1 van GIBIT 2023 wordt vermeld dat openbaarmaking niet is toegestaan, ook niet in het geval van een wettelijke publicatieplicht. Wij maken deel uit van een groep ondernemingen met een beursgenoteerde moedermaatschappij. In dat kader zijn wij onderworpen aan verplichte openbaarmakingsvereisten op grond van beursregelgeving (zoals ESEF, MAR of andere relevante richtlijnen). Wij verzoeken u te bevestigen dat onder “wettelijk voorschrift” ook deze verplichte openbaarmakingsvereisten op grond van beursregelgeving vallen. Uiteraard zullen wij, voor zover mogelijk, de opdrachtgever vooraf informeren over een eventuele openbaarmaking, samen met u alle mogelijkheden verkennen om openbaarmaking te voorkomen en, indien dit niet mogelijk blijkt, de omvang van de openbaarmaking beperken tot het strikt noodzakelijke. Kunt u bevestigen dat openbaarmaking op grond van beursregelgeving wordt beschouwd als een toelaatbare uitzondering op het verbod tot openbaarmaking zoals opgenomen in de overeenkomst?	Artikel 18.1 heeft betrekking op hetgeen bij de uitvoering van de Overeenkomst ter kennis komt en voorziet middels het 'wettelijk voorschrijft' in voldoende ruimte waarmee u aan uw openbaarmakingsvereisten kunt voldoen. Aanbestedende Dienst is van mening dat de openbaarmakingsvereisten op grond van beursregelgeving betrekking hebben op informatie die uw onderneming betreft maar dat deze openbaarmakingsvereisten geen betrekking hebben op hetgeen u bij de uitvoering van de Overeenkomst ter kennis komt.
2	Vragenronde 1	Verwijzing: GIBIT 2023 Artikel 18.4 In de aanbestedingsdocumenten wordt verwezen naar GIBIT 2023. In artikel 18.4 van GIBIT 2023 wordt vermeld dat informatie-uitwisseling tussen gelieerde ondernemingen niet is toegestaan. Wij maken echter deel uit van een groep gelieerde ondernemingen, waarbij de moedermaatschappij en de gelieerde entiteiten interne diensten verlenen op het gebied van onder andere juridische zaken, compliance, gegevensbescherming en financiën. Binnen onze organisatie zijn vertrouwelijkheid en gegevensbescherming geborgd via bestaande schriftelijke raamovereenkomsten. Wij verzoeken u daarom te bevestigen dat overdracht van gegevens aan gelieerde ondernemingen is toegestaan, mits aan de volgende voorwaarden wordt voldaan: a) de overdracht is noodzakelijk voor het leveren van de overeengekomen diensten; b) er bestaan schriftelijke overeenkomsten tussen de gelieerde ondernemingen die vergelijkbaar zijn met de bepalingen uit de GIBIT en de Bijlage B - Concept Overeenkomst MSP en MSSP GGD GHOR Nederland, en die vertrouwelijkheid en gegevensbescherming waarborgen; c) wij als opdrachtnemer blijven volledig aansprakelijk voor de naleving van de vereisten inzake vertrouwelijkheid en gegevensbescherming door onze gelieerde ondernemingen. Kunt u bevestigen dat onder deze voorwaarden informatie-uitwisseling met gelieerde ondernemingen is toegestaan?	Artikel 18.4 heeft betrekking op Opdrachtgever (Gibit is van de gemeenten) en heeft in die zin geen betrekking op Opdrachtnemer.
3	Vragenronde 1	Verwijzing: Bijlage A – Programma van Eisen MSP en MSSP, par. 41 In het Programma van Eisen en de SLA’s zijn geen specificaties opgenomen over het opschalen van virtuele werkplekken in crisissituaties. Kan GGD GHOR Nederland toelichten welke eisen gelden voor opschaling (bijvoorbeeld omvang, tijdspad, beschikbaarheid, performance) en op welke wijze deze opschalingscapaciteit moet worden getest en geborgd, zodat wij dit correct kunnen meenemen in onze inschrijving?	In geval van een crisissituatie, zoals we recent de covid-19 pandemie hebben gezien, kan het gebeuren dat er in korte tijd een groot beroep wordt gedaan op GGD GHOR Nederland. In een dergelijke situatie verwacht Aanbestedende Dienst snel veel extra medewerkers van een virtuele werkplek te moeten voorzien. Omvang is derhalve 100, tijdspad is derhalve binnen 48 uur, beschikbaarheid en performance dienen vergelijkbaar te zijn met de reeds aanwezige virtuele werkplekken. Aanbestedende Dienst is indien nodig bereid bij de implementatie van de MSP testscenario's hiertoe met Opdrachtnemer door te lopen.,
4	Vragenronde 1	Verwijzing: Beschrijvend document EA procedure MSP MSSP v1.0, Par. 3.2 en 3.4.1 Kunt u bevestigen of Gegadigden in een eventuele tweede Nota van Inlichtingen nieuwe vragen mogen indienen?	Zoals u in de planning op TenderNed kunt zien hebben wij voorzien in 2 vragenrondes.
5	Vragenronde 1	Verwijzing: Bijlage B - Concept Overeenkomst MSP en MSSP GGD GHOR Nederland, art. 1.6 In artikel 1.6 van de Conceptovereenkomst wordt bepaald dat alle aanbestedingsdocumenten prevaleren boven de Inschrijving van de Opdrachtnemer. Hierdoor komt de Inschrijving in de huidige rangorde altijd onderaan te staan, terwijl deze Inschrijving op basis van de aanbestedingsuitkomst wel leidend is voor de specifieke aanpak, kwaliteitsuitwerking en service-invulling van de door de Opdrachtnemer aangeboden prestatie. Om te voorkomen dat onderdelen die juist tijdens deze aanbesteding inhoudelijk zijn beoordeeld (zoals onze aanpak, borgingsmaatregelen, werkprocessen en kwaliteitsverbeteringen) buiten toepassing raken zodra zij afwijken van generieke passages in andere aanbestedingsdocumenten, verzoeken wij u te bevestigen dat: a) de Inschrijving als contractdocument een hogere rangorde krijgt dan de generieke aanbestedingsdocumenten, voor zover het gaat om de door de Opdrachtnemer aangeboden werkwijze, kwaliteitsmaatregelen en implementatie-uitwerking; of, indien dit niet de bedoeling is, b) artikel 1.6 wordt aangepast of verduidelijkt, zodat de Inschrijving van de Opdrachtnemer in elk geval voorrang heeft boven de aanbestedingsdocumenten bij tegenstrijdigheden die direct betrekking hebben op door de Opdrachtnemer aangeboden invullingen, methoden of procesuitwerkingen, welke onderdeel zijn van de beoordeling door de Aanbestedende Dienst. Kunt u dit bevestigen of toelichten?	Niet akkoord, de aanbestedingsdocumenten vormen de randvoorwaarden van de dienstverlening. Echter zullen we die dienstverlening ingericht willen zien conform uw voorstel in uw Inschrijving.
6	Vragenronde 1	Kunt u toelichten welke richtlijnen of kaders de overheid hanteert voor de wijze waarop GGD GHOR moet omgaan met calamiteiten, specifiek in de context van IT-dienstverlening?	Aanbestedende Dienst is geen overheidsorganisatie maar een vereniging met de GGD'en en GHOR's als leden. Omdat Aanbestedende Dienst op dit moment wel een aantal gemeenschappelijke taken verzorgt die als overheidsdiensten kunnen worden beschouwd, is zij gehouden aan alle kaders inzake zorg continuïteit, informatiebeveiliging en wettelijke meldplichten. Aanbestedende Dienst zal deze taken op termijn grotendeels overdragen aan een Landelijke Beheer Organisatie (LBO) - zie ook Beschrijvend Document. De kaders die momenteel worden gehanteerd vindt u terug in de geschiktheidseisen: ISO9001, ISO27001, BIO, NIS/2 e.d.
7	Vragenronde 1	Verwijzing: Bijlage A – Programma van Eisen MSP en MSSP, par. 13 Wat is de strategie en/of visie van GGD GHOR op basis van AI?	Aanbestedende Dienst heeft zeer recent haar AI-beleid ontwikkeld en vastgesteld. Aanbestedende Dienst sluit zich aan bij de visie van de Nederlandse overheid. We staan positief tegenover AI als grootste technologische innovatie binnen de digitalisering van dit moment. Digitalisering stelt ons in staat onze dienstverlening te optimaliseren, en het hoofd te bieden aan de druk van arbeidsmarkt. Bij de inzet van AI stellen we de mens centraal, en de impact die AI kan hebben op de mensen die het gebruiken en de mensen die er de gevolgen van ondervinden.
8	Beschrijvend document	Op basis van de aanbestedingsstukken begrijpen wij dat voor de Microsoft-licenties wordt uitgegaan van de contractvorm Cloud Solution Provider (CSP). Kunt u bevestigen of deze interpretatie juist is?	Aanbestedende Dienst maakt op dit moment inderdaad gebruik van de contractvorm CSP. Deze contractvorm maakt verplicht onderdeel uit van de Inbeheername door Opdrachtnemer. Indien hierna vanuit de advisering blijkt dat een andere contractvorm beter/ wenselijker/ goedkoper is, dan staan Aanbestedende Dienst daar voor open.

9	Beschrijvend document2.1-b t/m k	Kunt u nadere toelichting geven op de inrichting en opzet van de ICT-infrastructuur, inclusief de toegepaste vendoren? Deze informatie stelt inschrijvers beter in staat een realistische inschatting te maken van de te verwachten beheerlast en supportmogelijkheden.	Aanbestedende Dienst maakt uitsluitend gebruik van standaard Commercial Of The Shelf componenten.
10	Beschrijvend document2.1-3.e	Kunt u toelichten hoe de cloudhosting momenteel is vormgegeven (fysiek, virtueel, IaaS, PaaS, SaaS en hybride) en daarbij de relevante technische specificaties verstrekken, waaronder CPU, RAM, opslagcapaciteit en de rol van de afzonderlijke serveromgevingen? Deze informatie is noodzakelijk voor een zorgvuldige inschatting van de dienstverlening.	De huidige cloudhosting is multi-cloud ingericht en maakt gebruik van: IaaS-, PaaS- en SaaS-diensten Private, Public en Hybrid Cloud AWS, Azure en Leveranciers-proprietary cloudvoorzieningen. Er worden geen workloads on-premises gehost. De huidige cloudhosting bestaat uit een combinatie van één door GGD GHOR Nederland zelf beheerde Cloud tenant (Azure) en meerdere (15-20) door meerdere leveranciers beheerde cloudomgevingen. Voor workloads die worden gehost op (managed) IaaS- of PaaS-platformen wordt de keuze van het hostingplatform bepaald op basis van classificatie en bestaande contractuele kaders.
11	Beschrijvend document2.1-3.f	Kunt u de huidige omvang van de back-upomgeving specificeren, bij voorkeur uitgedrukt in GB of TB?	De opslag van de (M365) back-up bedraagt op dit moment 10,5 TB
12	Beschrijvend document2.1-3.h	Kunt u toelichten welk concept momenteel wordt gehanteerd voor de virtuele werkplek (bijvoorbeeld VDI, DaaS of een andere inrichting)	De huidige virtuele werkplek is op basis van Azure Virtual Desktop, Windows 365 is momenteel in onderzoek.
13	Beschrijvend document2.1-3.j	Kunt u toelichten wat u verstaat onder 'alle vergadervoorzieningen	Aanbestedende Dienst maakt gebruik van een 10-tal vergaderopstellingen van Barco. Dit betreft Vergaderschermen, webcams, microfoons en de mogelijkheid schermen van de werkplek te delen in de vergaderopstellingen.
14	Beschrijvend document2.	In de aanhef wordt gesproken over '… welke merendeels door … zelf wordt beheerd'. Kunt u nader toelichten wat wordt bedoeld met 'merendeels' en welke onderdelen momenteel intern worden beheerd?	Alle Managed Services worden op dit moment door Aanbestedende Dienst zelf verzorgd, met medewerking van enkele leveranciers die de middelen (mensen, licenties, voorzieningen) aanleveren om dit mogelijk te maken.
15	Beschrijvend document6.8.1-A.b	Ten behoeve van een zorgvuldige calculatie van de licentiekosten verzoeken wij u om gedetailleerd inzicht te verstrekken in de Microsoft Cloud Solution Provider (CSP)-licenties, inclusief type, editie en aantal.	Aanbestedende Dienst heeft hiertoe een aanvullende Bijlage W - Licentieoverzicht op TenderNed in de documentenmap geplaatst.
16	Beschrijvend document6.8.1.A.-	Kunt u aangeven in welke categorie de cloudconsumptie door u verwerkt wenst te zien (bijvoorbeeld C, E of een andere categorie)	Aanbestedende Dienst wil graag van u weten op welk deel van de cloudconsumptie uw vraag betrekking heeft en welke standaard categorisering aan uw vraag ten grondslag ligt. Deze vraag kunt u specifieker herhalen in de tweede vragenronde. Momenteel maakt Aanbestedende Dienst voor haar totaal aan IV/ICT diensten gebruik van IaaS, PaaS en SaaS en zeer beperkt van CaaS (Container as a Service). Van EaaS en XaaS wordt momenteel geen gebruik gemaakt.
17	Beschrijvend document47Periodieke maandkosten	Kunt u toelichten op welke wijze inschrijvers bij het opgeven van tarieven voor de duur van de Overeenkomst rekening dienen te houden met een eventuele jaarlijkse inflatiecorrectie? Is het toegestaan om een jaarlijkse prijscorrectie toe te passen op basis van de CBS CPI-index?	In de concept Overeenkomst en DFA als bijlage staat gespecificeerd hoe met Indexering wordt omgegaan.
18	Beschrijvend documentLicentiekosten	In de aanbestedingsstukken wordt gesproken over 'eeuwigdurend'. Kunt u toelichten wat hiermee wordt bedoeld, met name in de context van het gebruik van een flexibel Microsoft CSP-contract?	Aanbestedende Dienst bedoelt met 'eeuwigdurend' dat deze licenties / gebruiksrechten geen vast bepaalde looptijd hebben. Deze licenties lopen al en blijven lopen ook na aflopen van de Overeenkomst.
19	Beschrijvend documentPeriodieke maandkosten MSS	Wordt met de vermelding van de 6 medewerkers in de SOC-dienst bedoeld dat inschrijvers deze medewerkers overnemen, of gaat het uitsluitend om de te verwachten capaciteit en afschaling? Kunt u tevens aangeven hoe dit financieel verwerkt dient te worden in de aanbieding	Aanbestedende Dienst beoogt met het medewerkersaantal en aantal actieve use-cases een indruk te geven van de huidige SOC/SIEM inspanning en omvang. De huidige SOC/SIEM inspanning en omvang dient as-is in haar geheel door Opdrachtnemer in beheer te worden genomen. Het gaat hier dus primair om capaciteit. In bijlage O - Prijzensheet kunt u onder MSSP dit financieel uitwerken.
20	Beschrijvend document48Periodieke maandkosten MSS	Kunt u aangeven of u instemt met een transitie van de huidige SIEM-oplossing (i) direct naar de oplossing van de inschrijver, of (ii) gefaseerd, overeenkomstig de huidige SIEM-inrichting, zodat de oplossing van de inschrijver als standaard wordt doorgevoerd?	Aanbestedende Dienst hanteert als uitgangspunt dat eerst de as-is situatie door Opdrachtnemer in beheer wordt genomen en dat gezamenlijk een MSSP-Backlog wordt opgesteld waarin wijzigingen t.o.v. de as-is situatie kunnen worden opgenomen.
21	Beschrijvend document527.11	Wij constateren dat de door u voorgestelde geldigheidsduur van de inschrijving afwijkt van de termijn van de Wachtkamerovereenkomst. Kunt u toelichten wat de reden is en hoe dit zich verhoudt tot de uitvoering van de Overeenkomst?	De geldigheidsduur van alle inschrijvingen staat los van de geldigheidsduur die overeengekomen wordt met de nummer twee in ranking in de Wachtkamerovereenkomst.
22	Bijlage A PvE213.1	Microsoft voegt doorlopend, en buiten de invloedsfeer van de inschrijver, AI-functionaliteit toe aan haar oplossingen. Kunt u toelichten hoe deze ontwikkelingen moeten worden meegenomen of beoordeeld in het kader van het betreffende punt?	Aanbestedende dienst is zich bewust van- en maakt reeds gebruik van- de in Microsoftproducten geïntegreerde AI-functionaliteiten. Aanbestedende dienst wenst daarom Eis 13 als volgt aan te passen: Opdrachtnemer garandeert dat voor de levering van managed services en managed security services, geen gebruik gemaakt zal worden van Kunstmatige Intelligentie (AI), Large Language Models e.d. behoudens de reeds in Microsoftproducten aanwezige AI-functionaliteiten, tenzij dit in overleg met Opdrachtgever schriftelijk anders is overeengekomen en vooraf is getoetst aan het GGN AI-beleid en door het CISO-office.
23	Bijlage A PvE328.	In het Programma van Eisen wordt vermeld dat de opdrachtnemer de GGN-eigen voorzieningen voor Kantoor Internettoegang en Internetverbindingen as-is als Managed Services beheert en optimaliseert op basis van de nader overeen te komen Backlog Managed Services. Kunt u toelichten hoe dit zich verhoudt tot de levering van VPN-diensten en verbindingen, en in hoeverre kostenoptimalisaties betrekking kunnen hebben op verbindingen of abonnementen die buiten scope van de Managed Services vallen?	In paragraaf 2.2 vermeldt Aanbestedende Dienst expliciet dat het leveren van VPN-verbindingen en Breedband Internetverbindingen niet tot de opdracht behoort omdat hiervoor nog langlopende overeenkomsten actief zijn. Kostenoptimalisaties hebben hierop geen betrekking.
24	Bijlage A PvE430.	Kunt u aangeven in welke mate de opdrachtnemer bij aanvang van de Overeenkomst de vrijheid heeft om een eigen back-upoplossing te implementeren, met behoud van 100% datasoevereiniteit?	Aanbestedende Dienst is duidelijk dat bij aanvang van de opdracht de bestaande Back-upvoorziening as-is door de MSP in beheer dient te worden genomen. Indien Opdrachtnemer hiervoor een beter alternatief denkt te hebben waarmee de dienstverlening veiliger, efficiënter en/ of effectiever kan worden gerealiseerd dan is dat bespreekbaar en kan dit worden opgenomen in de MSP Backlog.
25	Bijlage A PvE434.	"In eis 34 van het Programma van Eisen wordt vermeld dat de opdrachtnemer kritieke updates, patches en upgrades verzorgt voor diverse componenten, waaronder Kantoorautomatisering, Kantoorinfrastructuur, Netwerkomgeving, Firewalls, Kantoor Internettoegang, Internetverbindingen, Kantoor Cloudhosting en Kantoor Back-up & Recovery, conform de termijnen uit de richtlijnen van het Nationaal Cyber Security Centrum (NCSC) en relevante kaders van de Wet digitale overheid. Kunt u toelichten of met 'upgrades' wordt bedoeld dat de opdrachtnemer ook projectmatige upgrades uitvoert (bijvoorbeeld grote versienummers of migraties), of dat dit beperkt is tot reguliere operationele updates en patching?"	Aanbestedende Dienst is hier van mening dat het woord 'kritiek' belangrijk is: Het betreft kritieke patches en updates die het NCSC communiceert en die daarom doorgaans een groot risico impliceren. Het uitvoeren van de reguliere patches en updates vallen hier niet onder.
26	Bijlage A PvE541.	Voor de inschrijving gaat de opdrachtnemer ervan uit dat incidentele groei van capaciteit niet afzonderlijk ingeprijst hoeft te worden. Kunt u bevestigen of deze interpretatie correct is, zodat inschrijvers geen onbedoelde risico's in hun aanbieding verwerken?	Aanbestedende Dienst gaat er van uit dat de kosten voor het gebruik van een Virtuele Werkplek niet afhankelijk zijn van het tijdstip waarop de Virtuele Werkplek wordt uitgegeven (tijdens kantooruren of in een crisissituatie). Aanbestedende Dienst geeft in Bijlage O - Prijzenblad wel ruimte om de uurtarieven buiten kantooruren (bijvoorbeeld in een crisissituatie) te specificeren.
27	Bijlage A PvE545.	Wat verwacht u van de inschrijver in relatie tot reproductie en printapparatuur/oplossing? Dienen wij hierin een SPOC rol richting de huidige leverancier te vervullen?	Aanbestedende Dienst maakt op dit moment gebruik van print devices van Veenman en Printix voor secure Cloud Print Management. De verwachting ten aanzien van de Inschrijver is dat deze de printvoorzieningen as-is in beheer overneemt waarna wij de overeenkomst met de huidige leverancier kunnen beëindigen en vanaf dat moment zowel de devices als het Cloud Print Management als dienst afnemen van Opdrachtnemer.
28	Bijlage A PvE752.	Kunt u vooraf aangeven op welke technologie en/of bij welke vendor de huidige SIEM-oplossing is gebaseerd?	Aanbestedende Dienst maakt op dit moment gebruik van een eigen SIEM-oplossing op basis van Azure Sentinel.

29	Bijlage A PvE1084.	Veel moderne SIEM-oplossingen integreren met de Microsoft-stack en kunnen logdata uit Microsoft Defender uitlezen, waarbij de inzet van NDR-functionaliteit minder relevant kan zijn. Staat u ervoor open om het gebruik van NDR op een later moment in overleg met de opdrachtnemer te bespreken, afhankelijk van de aanwezige licenties en functionele behoeften?	Aanbestedende Dienst staat open voor verbeteringen aan haar SIEM-oplossing voor zover deze bijdragen aan een veiligere, efficiëntere en effectievere IV/ICT-omgeving. Uitgangspunt is wél dat de voorzieningen as-is in beheer worden genomen en dat verbeteringen/ veranderingen overeen worden gekomen in de MSSP Backlog
30	Bijlage U	Wij merken op dat Bijlage U ontbreekt in de set met aanbestedingsdocumenten. Kunt u deze alsnog beschikbaar stellen?	Aanbestedende Dienst heeft op TenderNed Bijlage U inmiddels beschikbaar gemaakt
31	Algemeen ten aanzien van de opdracht	Kunt u specificeren welke KPI's, boetes en kortingsregelingen van toepassing zijn op de diensten geleverd door de Managed Service Provider / Managed Security Service Provider (MSP/MSSP)?	Aanbestedende Dienst is van mening dat te te overeen te komen Overeenkomst, concept SLA MSP en concept SLA MSSP voldoende duidelijk maken wat de KPI's zijn, welke normen worden gesteld en wat de condities zijn voor boetes en kortingsregelingen.
32	Algemeen ten aanzien van de opdracht	Kunt u toelichten op welke wijze de bandbreedte van de opdrachtwaarde is bepaald en welke aannames hierbij zijn gehanteerd?	Aanbestedende Dienst heeft dit uitgewerkt in paragraaf 2.6 van het Beschrijvend Document. Aanbestedende Dienst heeft hierbij een going concern-situatie van circa 175 medewerkers als uitgangspunt gehanteerd en hierbij de huidige kosten, alsook de kosten op basis van een brede benchmark gehanteerd. De belangrijkste aanname die hierin wordt gedaan is dat Aanbestedende Dienst vanwege het wegvallen van financiering voor Infectieziektebestrijding op zeer korte termijn drastisch zal moeten krimpen.
33	Algemeen ten aanzien van de opdracht	Welke lessons learned uit COVID worden concreet als verplichting opgenomen?	Aanbestedende Dienst ziet als belangrijkste les uit de Covid-19 periode de noodzaak tot structurele financiering van Infectieziektebestrijding. Voor deze aanbestedingsprocedure gelden geen Covid-19 verplichtingen voor de deelnemers
34	Algemeen ten aanzien van de opdracht	Kunt u specificeren welke scenario's binnen de Overeenkomst opgeschaald moeten worden naar 1.000 FTE, en binnen welke termijn dit dient te gebeuren?	Aanbestedende Dienst heeft in paragraaf 1.1.3 van het beschrijvend document getracht te schetsen dat de gewenste situatie een going concern betreft van circa 175 FTE maar dat in geval van een crisissituatie de mogelijkheid moet bestaan om snel op te schalen in FTE-aantal. Bijvoorbeeld bij een nieuwe pandemie of andere crisis in de Publieke Gezondheid. In. een dergelijke situatie zal naar verwachting met name het aantal virtuele werkplekken voor deze medewerkers in korte tijd aanzienlijk moeten kunnen toenemen.
35	Algemeen ten aanzien van de opdracht	Wij verzoeken u te verduidelijken welk deel van het gebruikersvolume structureel (vast) is en welk deel variabel, zodat inschrijvers een correcte inschatting kunnen maken van de benodigde capaciteit en kosten.	Zie hiervoor Beschrijvend Document en Prijzenblad. Op dit moment zijn er circa 300 structurele gebruikers, maar op termijn wordt verwacht dat dit zal teruglopen naar gemiddeld structureel 175. Incidenteel kan het gebeuren, bijvoorbeeld bij een crisissituatie, dat het aantal gebruikers in korte tijd moet stijgen.
36	Algemeen ten aanzien van de opdracht	Kunt u aangeven of er lopende contracten zijn die tijdens de transitieperiode door de opdrachtnemer moeten worden overgenomen?	Aanbestedende Dienst wil met deze procedure juist een groot aantal aflopende contracten rechtsgeldig laten opvolgen door bij voorkeur één nieuw contract. Er hoeven derhalve geen bestaande contracten te worden overgenomen.
37	Algemeen ten aanzien van de opdracht	Kunt u specificeren welke data-overdrachtsvereisten gelden voor de verschillende omgevingen, zoals productie, acceptatie en test?	Aanbestedende Dienst is van mening dat er niet/ nauwelijks sprake zal zijn van data-overdracht omdat de bestaande voorzieningen as-is in beheer dienen te worden overgenomen. De data blijft derhalve logisch en fysiek op dezelfde locatie. Wel stelt Aanbestedende Dienst eisen ten aanzien van het (sub)verwerkerschap. Dit is onder andere uitgewerkt in Bijlage C - (sub)Verwerkersovereenkomst. Waar het specifiek de data-overdracht binnen een OTAP (evt. met staging) betreft, geldt dat er nooit mag worden getest met productiedata, tenzij dat onontbeerlijk / kritiek is voor de volledigheid van de test. In dat soort gevallen dient te allen tijd schriftelijk toestemming te worden gevraagd en dienen de data dusdanig te worden geanonimiseerd dat deze niet naar natuurlijk personen te herleiden zijn.
38	Algemeen ten aanzien van de opdracht	Zijn er kritische afhankelijkheden van externe leveranciers? Zo ja, welke?	Aanbestedende Dienst ziet als kritische afhankelijkheden het zorgvuldig en volledig overnemen van haar CSP-account (huidige leverancier) en de afstemming met de huidige ISP (Signet).
39	Algemeen ten aanzien van de opdracht	Wat is het volledige transitie-tijdpad en vindt de migratie plaats via een 'big bang' of gefaseerde aanpak?	Aanbestedende Dienst is van mening dat dit voldoende in het Beschrijvend Document is uitgewerkt: Vanaf de ingang van de Overeenkomst dient de due diligence plaats te vinden alsook het definitief afronden van het gezamenlijk implementatieplan op basis van het door u aangereikte (G1) Implementatieplan. Aanbestedende Dienst verwacht dat 1 a enkele sprints vóór einde 2026 gereed kunnen zijn maar dat de totale transitie nog in 2027 zal doorlopen.
40	Algemeen ten aanzien van de opdracht	Wat zijn de compliance-audits waaraan de leverancier jaarlijks moet voldoen (BIO, PURA, GIBIT-proeven, DPIA's, etc.)?	De Compliance Audits zullen uitsluitend betrekking hebben op de onder Geschiktheidseisen (tabel paragraaf 4.4.4) vastgestelde kwaliteit- en veiligheidscertificaten.
41	Algemeen ten aanzien van de opdracht	Zijn Tier 1–3 IR-processen reeds gedefinieerd of verwacht u dat de MSP/MSSP deze opstelt?	Aanbestedende Dienst beschikt reeds over Tier 1-3 Incident Respons processen welke as-is door de MSSP dienen te worden genomen, waarna aan de hand van de MSSP Backlog verbeteringen kunnen worden doorgevoerd dan wel IR-processen kunnen worden toegevoegd.
42	Algemeen ten aanzien van de opdracht	Wat zijn de logging requirements (EPS, datavolume, retentie)?	Aanbestedende Dienst is voor EPS en Volume gehouden aan de Logging requirements van de BIO. Voor retentie geldt artikel 5, tweede lid, van het Besluit elektronische gegevensverwerking door zorgaanbieders: De logging als bedoeld in het Besluit elektronische gegevensverwerking door zorgaanbieders, wordt ten minste 5 jaar bewaard vanaf het moment dat de logregel wordt geschreven.
43	Microsoft pricing	Gezien het feit dat Microsoft prijsaanpassingen kan doorvoeren buiten de invloedsfeer van de inschrijver, verzoeken wij u te verduidelijken hoe dergelijke verhogingen worden behandeld binnen de Overeenkomst en welke impact dit heeft op de tariefstelling door inschrijvers	Aanbestedende dienst betrekt momenteel haar Microsoft Licenties via de CSP van de huidige leverancier, welke de kosten voor de licenties van Microsoft Producten aan Aanbestedende dienst doorberekent. Prijsverhogingen van Licenties die door Microsoft worden doorgevoerd worden 1 op 1 doorberekend.
44	Juridische interpretatie	Bijlage K: Uit de verschillende documenten blijkt dat Service Now niet volledig is ingericht voor alle processen. Is de implementatie nog bezig? Is uw Service Now omgeving op dit moment 100% operationeel? Zijn er nog onderdelen te ontwikkelen/implementeren en zo ja, welke?	Aanbestedende Dienst heeft haar ServiceNow-implementatie gereed (het MVP) - waar op dit moment nog aan gewerkt wordt is de backlog. Dit zal doorlopend het geval zijn.
45	Juridische interpretatie	Bijlage H: Gegevens mogen uitsluitend binnen de beveiligde omgeving van GGD GHOR Nederland verwerkt worden; Vraag: Kan een SIEM buiten de beveiligde omgeving van GGD GHOR worden toegevoegd als zijnde onderdeel van genoemde beveiligde omgeving?	Bijlage H bevat de gedragscode voor telewerken. Indien een medewerker inlogt bevindt deze zich binnen de beveiligde omgeving. Het SIEM van Aanbestedende Dienst bevindt zich binnen de beveiligde omgeving en dient as-is door de MSSP in beheer te worden genomen en blijft daarmee binnen de beveiligde omgeving.
46	Juridische interpretatie	Worden eventuele tegenstrijdigheden tussen het Beschrijvend document en het Programma van Eisen geïnterpreteerd in het voordeel van het Beschrijvend document?	Aanbestedende Dienst is van mening dat BD en PvE niet strijdig met elkaar zijn en kan daarom als zodanig niet aangeven welke documenten prevaleren. Indien u van mening bent dat deze documenten strijdig zijn dan verzoeken wij u in de volgende vragenronde eventuele tegenstijdigheden expliciet te maken en hierover vragen te stellen
47	Referenties & Financiële drempels	Moeten zowel voor MSP als voor MSSP afzonderlijke referenties worden aangeleverd?	Aanbestedende Dienst heeft dit beschreven in het Beschrijvend Document: De Inschrijver toont de gevraagde bekwaamheid aan met maximaal één referentieopdracht per kerncompetentie. Het is toegestaan om dezelfde referentieopdracht ter aantoning van meerdere kerncompetenties te gebruiken. Uit de referenties moet de gevraagde bekwaamheid blijken.
48	Referenties & Financiële drempels	Geldt de referentie-eis van €300.000 per jaar uitsluitend voor MSSP, uitsluitend voor MSP, of voor MSP en MSSP tezamen?	De omvang van de referentie-eis heeft betrekking op de referenties waaruit de gevraagde bekwaamheid blijkt.

49	Exit & Continuïteit	Wordt verwacht dat capaciteit vooraf contractueel wordt gereserveerd (bijvoorbeeld via een wachtkamerregeling) in het kader van pandemische opschaling?	Aanbestedende Dienst hanteert voor deze procedure een standaard going concern scenario van circa 175 FTE waarvoor de basis IV/ICT voorzieningen moeten worden verzorgd door de MSP + MSSP. Aanbestedende Dienst stelt de Eis dat het aantal virtuele werkplekken in geval van een crisissituatie snel moet kunnen worden opgeschaald. Deze eis staat los van wat u Pandemische Opschaling noemt. De door Aanbestedende Dienst aangeduide crisissituatie is generiek en staat los van Pandemische (specifieke crisis) opschaling. U hoeft derhalve gaan capaciteit vooraf te reserveren. Wel wordt u geacht in geval van een crisissituatie het aantal virtuele werkplekken binnen enkele dagen te kunnen opschalen.
50	Exit & Continuïteit	Hoe wordt patch-classificatie en de bijbehorende implementatietermijn contractueel vastgelegd?	Beide worden vastgelegd in de combinatie van de Overeenkomst en de bijbehorende SLA's en DAP's MSP en MSSP.
51	SLA & Governance	-	-
52	SLA & Governance	Wordt van de MSSP verwacht dat containment maatregelen zelfstandig mogen worden uitgevoerd bij kritieke incidenten?	Aanbestedende Dienst is van mening dat hierover bij het definitief maken van het SLA MSSP en het DAP afspraken over moeten worden vastgelegd in onder andere een autorisatiematrix
53	SLA & Governance	Hoe wordt patch-classificatie en de bijbehorende implementatietermijn contractueel vastgelegd?	Beide worden vastgelegd in de combinatie van de Overeenkomst en de bijbehorende SLA's en DAP's MSP en MSSP.
54	SLA & Governance	In de Concept SLA MSSP wordt gesproken over het Governance Security Operations Center (G-SOC). Kunt u toelichten of het G-SOC primair een regierol of een uitvoerende rol vervult?	Het G-SOC of Governance-SOC is naar verwachting de uitwerking van de Functionele Regie Organisatie in relatie tot het SOC/SIEM. Dit houdt in dat het G-SOC een regierol zal vervullen in de situatie dat de MSSP het SOC/SIEM volledig in beheer heeft overgenomen.
55	Implementatie en transitie	"Wordt een parallelle beheerperiode (overdracht huidige leverancier naar nieuwe leverancier) verwacht? Zo ja, wat is de beoogde duur?"	Aanbestedende dienst heeft gepland dat de nieuwe Overeenkomst in gaat per 01-07-2026 en dat eerst de Due Diligence wordt uitgevoerd alvorens de implementatie (inbeheername) kan worden gestart. Verwacht wordt dan ook dat er een periode is waarin zowel huidige als nieuwe Opdrachtnemer tegelijkertijd voor Aanbestedende Dienst werken en er daarom sprake zal zijn van een parallelle beheerperiode van 6 maanden tot ultimo 2026. Deze parallelle beheerperiode betekent overigens niet dat er tegelijkertijd twee beheerders op dezelfde diensten actief zijn. Oude leverancier blijft beheerder totdat de formele acceptatie per dienstverleningsonderwerp heeft plaatsgevonden, waarna de nieuwe leverancier beheerder wordt.
56	Implementatie en transitie	Kunt u specificeren welke resources en beschikbaarheid vanuit GGD GHOR worden voorzien tijdens de implementatiefase?	Aanbestedende Dienst werkt op dit moment aan haar eigen Implementatie- en uitrolplan voor de In beheer te geven dienstverlening. Aanbestedende Dienst zal voorzien in alle noodzakelijke rollen (resources) die volgens haar eigen plan en die volgens Inschrijver (G1) noodzakelijk zijn. Dit betreft tenminste 1 projectmanager, 1 product Owner KA, 1 diensteneigenaar SOC/SIEM. het voltallige SOC/SIEM-team, 1 Contractmanager, 2 service level managers en 1 architect MSP en 1 architect MSSP. Inschrijver wordt gevraagd de door Aanbestedende Dienst beschikbaar te maken capaciteit op te nemen in haar Implementatieplan (G1)
57	ServiceNow & Security Servicemanagement	Welke integraties bestaan er momenteel tussen ServiceNow en de huidige SIEM/SOC-omgeving?	Aanbestedende dienst heeft op dit moment geen (technische) integraties actief tussen de huidige SOC/SIEM-voorzieningen en de ServiceNow-omgeving.
58	ServiceNow & Security Servicemanagement	Kunt u inzicht geven in de huidige security servicemanagement-processen zoals ingericht binnen de GGN-eigen ServiceNow-omgeving?	Alle meldingen (Problemen (intern) Issues (extern), gebruikersvragen, Changes en alle Tier 1 tot 3 meldingen dienen te allen tijde tenmínste in ServiceNow te zijn/ worden ondergebracht.
59	AI-beperking	Indien AI uitsluitend wordt toegepast als ondersteunend analyse-instrument zonder autonome besluitvorming, valt dit onder het verbod?	"Aanbestedende dienst is zich bewust van- en maakt reeds gebruik van- de in Microsoftproducten geïntegreerde AI-functionaliteiten. Aanbestedende dienst wenst daarom Eis 13 als volgt aan te passen: Opdrachtnemer garandeert dat voor de levering van managed services en managed security services, geen gebruik gemaakt zal worden van Kunstmatige Intelligentie (AI), Large Language Models e.d. behoudens de reeds in Microsoftproducten aanwezige AI-functionaliteiten, tenzij dit in overleg met Opdrachtgever schriftelijk anders is overeengekomen en vooraf is getoetst aan het GGN AI-beleid en door het CISO-office." Indien u buiten dit kader om AI ándere AI wenst toe te passen als ondersteunend analyse-instrument dan is Aanbestedende Dienst bereid hierover afspraken te maken.
60	AI-beperking	Hoe wordt onderscheid gemaakt tussen rule-based detectie en AI-ondersteunde detectie?	Aanbestedende Dienst hanteert hierin het onderscheid dat Rule based detectie te allen tijde detectieregels betreft die het SOC zelf heeft geïdentificeerd /geformuleerd en dat AI based detectie in de data kijkt naar afwijkende/ opvallende patronen die (nog) niet onder Rule based detectie zijn opgenomen.
61	AI-beperking	"In het Programma van Eisen wordt gesteld dat geen gebruik mag worden gemaakt van AI of LLM's tenzij vooraf schriftelijk overeengekomen. Kunt u verduidelijken of standaard AI-functionaliteiten binnen Microsoft security tooling (zoals Defender AI-detectie) hieronder vallen?"	"Aanbestedende dienst is zich bewust van- en maakt reeds gebruik van- de in Microsoftproducten geïntegreerde AI-functionaliteiten. Aanbestedende dienst wenst daarom Eis 13 als volgt aan te passen: Opdrachtnemer garandeert dat voor de levering van managed services en managed security services, geen gebruik gemaakt zal worden van Kunstmatige Intelligentie (AI), Large Language Models e.d. behoudens de reeds in Microsoftproducten aanwezige AI-functionaliteiten, tenzij dit in overleg met Opdrachtgever schriftelijk anders is overeengekomen en vooraf is getoetst aan het GGN AI-beleid en door het CISO-office." Indien u buiten dit kader om AI ándere AI wenst toe te passen als ondersteunend analyse-instrument dan is Aanbestedende Dienst bereid hierover afspraken te maken."
62	SIEM, tooling en Microsoft-oriëntatie	Mag de Opdrachtnemer een eigen SIEM-oplossing inzetten, mits deze aantoonbaar voldoet aan de gestelde eisen?	Aanbestedende Dienst hanteert het principe dat het eigen (MS) SIEM as-is in beheer wordt genomen. Indien u mogelijkheden ziet om daarná middels uw eigen SIEM-oplossing de veiligheid , efficiency en effectiviteit van de IV/ICT voorzieningen te vergroten dan staat Aanbestedende Dienst daar voor open en kan dit bij akkoord worden opgenomen in de MSSP Backlog.

63	SIEM, tooling en Microsoft-oriëntatie	"GGD GHOR geeft aan gebruik te maken van Microsoft-"compatibele" producten. Kunt u een overzicht verstrekken van deze producten?"	MS Windows 11 MS Office 365 MS SharePoint MS Power BI MS Azure Virtual Desktop MS Sentinel: MS Defender for Threat Intelligence MS Office 365 MS Defender for Endpoint Azure Services Entra ID MS Entra ID Protection MS Defender for Business MS Defender for Cloud Apps MS Defender for Office 365 (o.a. Purview alerting DLP) MS Defender for Vulnerability Management
64	SIEM, tooling en Microsoft-oriëntatie	"Indien gebruik wordt gemaakt van Microsoft Sentinel: o Is GGD GHOR reeds licentiehouder? o Of wordt verwacht dat de licenties via de Opdrachtnemer worden geleverd/overgenomen?"	Aanbestedende Dienst maakt voor haar Microsoft licenties gebruik van het CSP-programma dat door de huidige leverancier wordt verzorgd. GGD GHOR Nederland is dus inderdaad al licentiehouder via het CSP-programma. Zoals u in het PvE kunt lezen hoort de overname van de CSP en daarmee de uitlevering en facturatie van licenties tot de opdracht.
65	SIEM, tooling en Microsoft-oriëntatie	Is het verplicht deze SIEM-oplossing over te nemen, of is het toegestaan dat de Opdrachtnemer een eigen SIEM inzet?	Aanbestedende Dienst hanteert het principe dat het eigen (MS) SIEM as-is in beheer wordt genomen. Indien u mogelijkheden ziet om daarná middels uw eigen SIEM-oplossing de veiligheid , efficiency en effectiviteit van de IV/ICT voorzieningen te vergroten dan staat Aanbestedende Dienst daar voor open en kan dit bij akkoord worden opgenomen in de MSSP Backlog.
66	SIEM, tooling en Microsoft-oriëntatie	Welke SIEM-oplossing wordt momenteel gebruikt?	MS Sentinel: MS Defender for Threat Intelligence MS Office 365 MS Defender for Endpoint Azure Services Entra ID MS Entra ID Protection MS Defender for Business MS Defender for Cloud Apps MS Defender for Office 365 (o.a. Purview alerting DLP) MS Defender for Vulnerability Management
67	Data Intelligence	Wordt verwacht dat security governance binnen de Data Intelligence-omgeving integraal onderdeel is van de MSSP-dienstverlening?	De huidige (extern betrokken) Data Intelligence-omgeving valt momenteel inderdaad onder de security governance van het SOC/SIEM. Voor de nieuwe MSSP zal gelden dat dit inderdaad zo zal blijven. Ook in het geval dat de extern betrokken Data Intelligence-omgeving in haar geheel of gedeeltelijk wordt vervangen op basis van uw kansendossier.
68	Data Intelligence	Wordt Azure beschouwd als het verplichte platform voor Data Intelligence?	Managed Data Intelligence Services vormen geen onderdeel van het Programma van Eisen maar worden als Kansendossier uitgevraagd. Indien blijkt dat er rendabele kansen die voor uitvoering/ implementatie in aanmerking komen, dan zal dit inderdaad bij voorkeur op basis van Azure Managed Cloudhosting moeten plaatsvinden. Aanbestedende Dienst staat ook open voor Hybrid of Private Cloudmogelijkheden.
69	Data Intelligence	Is de veronderstelling correct dat het Kansendossier Managed Data Intelligence Services uitsluitend betrekking heeft op de MSP-dienstverlening?	Zoals u kunt lezen in het Beschrijvend Document - G4 ziet Aanbestedende Dienst de Managed Data Intelligence Services als aanvulling op de managed services (MSP en MSSP)
70	Is de veronderstelling correct dat het Kansendossier Managed Data Intelligence Services uitsluitend betrekking heeft op de MSP-dienstverlening?	Is de veronderstelling correct dat het Kansendossier Managed Data Intelligence Services uitsluitend betrekking heeft op de MSP-dienstverlening?	Zoals u kunt lezen in het Beschrijvend Document - G4 ziet Aanbestedende Dienst de Managed Data Intelligence Services als aanvulling op de managed services (MSP en MSSP)
71	Data Intelligence	"Kunt u een nadere toelichting geven op de volledig geoutsourcete Data Intelligence-voorzieningen? Graag inzicht in: o De huidige architectuur; o De betrokken leveranciers; o De gebruikte platformen; o De (technische) rol die de MSSP hierin dient te vervullen."	Voor de huidige Managed Data Intelligence Services maakt Aanbestedende Dienst gebruik van 2 contractpartijen die uit oogpunt van vertrouwelijkheid hier niet bij naam genoemd worden. Voor de voorzieningen geldt dat er gebruik wordt gemaakt van: - Dataportaal, webapplicatie voor toegangsbeheer tot dashboards, rapportages en content - Power BI voor het samenstellen van dashboards en rapportages - Datakubussen & DeltaGateway voor de OTAP-omgeving, Operational Data Store en Data warehouse-laag - Het geheel wordt gehost op een private cloudomgeving van leverancier. De rol die het huidige SOC/SIEM hierin vervult is dat de Data Intelligence-voorzieningen worden gelogd en gemonitored. De rol die de MSSP hier in dient te vervullen is de inbeheername van deze SOC/SIEM-rol.
72	Toekomstige regieorganisatie	Welke applicaties of onderdelen worden op termijn overgedragen aan een landelijke beheerorganisatie en welke blijven onder verantwoordelijkheid van de MSSP?	Of, wanneer en in hoeverre applicaties worden overgedragen is op dit moment nog onderwerp voor besluitvorming. De demarcatie zal liggen bij applicaties die van overheidswege gecontinueerd moeten worden en binnen overheidskaders in beheer moeten blijven. Aanbestedende Dienst GGD GHOR Nederland is géén Overheidsorganisatie in die zin. Wat zeker is is dat de bedrijfsbrede toepassingen zoals Kantoorautomatisering e.d. te allen tijde onder de verantwoordelijkheid van SOC/SIEM en MSSP blijven vallen.
73	Toekomstige regieorganisatie	"In de aanbestedingsstukken wordt aangegeven dat binnen twee jaar wordt toegewerkt naar een regieorganisatie. Kunt u toelichten hoe u de verschuiving van de huidige MSSP-werkzaamheden naar deze toekomstige inrichting voor zich ziet?"	Op dit moment beschikt Aanbestedende Dienst over een eigen SOC met een SIEM (Sentinel) en een in eigen beheer ontwikkeld Logbuffet (Log verzamelaar) welke de loggingdata aanlevert bij een tweede SIEM (Splunk). De activiteiten van het SOC en de SIEM-voorzieningen dienen as-is door de MSSP in beheer te worden genomen en aan de hand van de backlog MSSP verder te worden geoptimaliseerd in de breedste zin van het woord. Aansturing van de MSSP zal in eerste instantie door het eigen SOC van aanbestedende dienst geschieden, echter het ligt in de lijn der verwachting dat het eigen SOC op termijn wordt veranderd naar een G-SOC of Governance SOC met uitsluitend een regiefunctie naar de MSSP.
74	Huidig MSSP-landschap & situatie	Van welke specifieke Publieke Gezondheidsmaat-applicaties is sprake en dienen deze te worden aangesloten op SIEM/SOC?	Er zijn circa maatwerkapplicaties en bedrijfsbrede toepassingen die reeds actief worden gelogd en gemonitored door het eigen SOC in de eigen SIEM-voorziening. Er hoeven derhalve geen specifieke Publieke Gezondheidsmaatwerkapplicaties opnieuw te worden aangesloten. De MSSP wordt geachte de huidige SOC/SIEM-voorzieningen as-is in beheer te nemen.

75	Huidig MSSP-landschap & situatie	data	-
76	Huidig MSSP-landschap & situatie	Kunt u toelichten hoe Incident Response momenteel is ingericht en welke afspraken (SLA's, escalatieprocedures, verantwoordelijkheden) hierbij gelden?	Aanbestedende Dienst heeft de huidige Service Levels, procedures en verantwoordelijkheden als Bijlage J concept SLA MSP en Bijlage K concept SLA MSSP uitgewerkt. De daarin vermelde service levels, procedures en verantwoordelijkheden zijn momenteel bij Aanbestedende Dienst actief en geldig.
77	Huidig MSSP-landschap & situatie	"Er wordt vermeld dat delen van het SOC worden uitbesteed. Kunt u toelichten: o Welke onderdelen momenteel zijn uitbesteed; o Welke onderdelen bij GGD GHOR blijven; o Welke contractuele afspraken hierbij gelden?"	Op dit moment beschikt Aanbestedende Dienst over een eigen SOC met een SIEM (Sentinel) en een in eigen beheer ontwikkeld Logbuffet (Log verzamelaar) welke de loggingdata aanlevert bij een tweede SIEM (Splunk). De activiteiten van het SOC en de SIEM-voorzieningen dienen as-is door de MSSP in beheer te worden genomen en aan de hand van de backlog MSSP verder te worden geoptimaliseerd in de breedste zin van het woord. Aansturing van de MSSP zal in eerste instantie door het eigen SOC van aanbestedende dienst geschieden, echter het ligt in de lijn der verwachting dat het eigen SOC op termijn wordt veranderd naar een G-SOC of Governance SOC met uitsluitend een regiefunctie naar de MSSP. De momenteel uitbestede delen zijn: - managed cloudhosting van de SOC/SIEMvoorzieningen - levering van de onderliggende licenties via de CSP
78	Huidig MSSP-landschap & situatie	"Er wordt aangegeven dat de GGN-eigen SOC/SIEM-voorzieningen gedurende het eerste jaar “as is” worden overgenomen. Kunt u zeer concreet inzicht geven in wat hieronder exact wordt verstaan? Graag specificatie van: o Medewerkers en functies; o Applicaties en tooling; o Netwerk- en infrastructuurcomponenten; o Bestaande contractuele verplichtingen; o Documentatie en configuraties."	- Het huidige SOC bestaat uit 6 teamleden van SOC Data analisten en SOC technisch analisten en 1 SOC architect. - Applicaties: Ms-Sentinel, Ms-Defender, Splunk, Topdesk / ServiceNow De levering van de softwarelicenties loopt via de CSP, deze overeenkomst eindigt in december 2026 en wordt geacht door de MSP te worden overgenomen.
79	Huidig MSSP-landschap & situatie	"In de stukken wordt verwezen naar een gedeeld domein met regionale GGD'en en GHOR-organisaties. Kunt u bevestigen of deze omgevingen integraal onderdeel zijn van het MSSP-landschap en derhalve binnen scope vallen?"	Aanbestedende Dienst verzorgt een groot aantal maatwerkapplicaties voor GGD'en en GHOR, deze verzameling wordt hier het 'gedeelde domein' genoemd, intern ook wel het Verenigingsdomein. Betreffende applicaties in dit gedeelde domein leveren logfiles welke door het eigen SOC/SIEM worden gemonitored. In die zin is het 'gedeelde domein' dus inderdaad onderdeel van het MSSP-landschap en derhalve binnen de scope. Nota bene dat de MSSP wordt gevraagd de monitoring en verwerking van de loginformatie te verzorgen. MSSP heeft geen rol in de applicatiestrategie van betreffende applicaties in het gedeelde domein.
80	Huidige MSP situatie	"Kunt u nader inzicht bieden in het huidige MSP-landschap? o de huidige Werkplek oplossing (fysiek & virtueel) o de architectuur van het volledige werkplekdomein o gebruikte applicaties lokaal o gebruikte applicaties cloud o Mate van beveiliging / toegepast beveiligingsbeleid"	Aanbestedende Dienst maakt uitsluitend gebruik van mainstream Commercial Of The Shelf producten/ devices. Zie ook de overige antwoorden in deze Nota van Inlichtingen. MS Windows 11 MS Office 365 MS SharePoint MS Power BI MS Azure Virtual Desktop MS Sentinel: MS Defender for Threat Intelligence MS Office 365 MS Defender for Endpoint Azure Services Entra ID MS Entra ID Protection MS Defender for Business MS Defender for Cloud Apps MS Defender for Office 365 (o.a. Purview alerting DLP) MS Defender for Vulnerability Management Splunk Aanbestedende Dienst heeft de Non Profitstatus conform de voorwaarden van Microsoft. Firewall: Fortigate Switches: Fortigate en Unifi AP's: Unifi Alle niet-Microsoft licenties lopen te allen tijde via de Softwarebroker SoftwareOne.
81	Huidig MSSP-landschap & situatie	"Kunt u een volledige beschrijving geven van het huidige MSSP-landschap? Graag ontvangen wij inzicht in: o de huidige SIEM-oplossing; o gekoppelde logbronnen (applicaties, firewalls, EDR, cloudomgevingen, etc.); o bestaande use cases / detectieregels; o het huidige SOC-team (omvang, rolverdeling en eventuele uitbesteding); o de architectuur van het volledige securitydomein."	- Het huidige SOC bestaat uit 6 teamleden van SOC Data analisten en SOC technisch analisten en 1 SOC architect. - Applicaties: Ms-Sentinel, Ms-Defender, Splunk, Topdesk / ServiceNow - Logbronnen: Maatwerkapllicaties voor de GGD'en en Bedrijfsbrede toepassingen van Aanbestedende Dienst De levering van de softwarelicenties loopt via de CSP, deze overeenkomst eindigt in december 2026 en wordt geacht door de MSP te worden overgenomen.
82	7.5 Gegevens aan te leveren door opdrachtnemer	"De opdrachtnemer levert alle relevante configuratie- en assetgegevens aan, zodat deze volledig en correct kunnen worden opgenomen in het Asset Register van GGD GHOR Nederland." "In de aanbestedingsdocumentatie wordt gesteld dat “de opdrachtnemer alle relevante configuratie- en assetgegevens aanlevert, zodat deze volledig en correct kunnen worden opgenomen in het Asset Register van GGD GHOR Nederland.” Kunnen wij ervan uitgaan dat GGD GHOR Nederland verantwoordelijk is voor het verwerken en beheren van deze door de opdrachtnemer aangeleverde informatie in het Asset Register van GGD GHOR Nederland, en dat de rol van de opdrachtnemer zich beperkt tot het aanleveren van juiste en volledige gegevens?"	Dat is correct.
83	2.2 Beschikbaarheidsniveaus	Beschikbaarheid fysieke werkplekken "In de aanbestedingsdocumentatie wordt een beschikbaarheidspercentage gehanteerd voor Werkplekken. Wij constateren dat het hier (mede) fysieke werkplekken betreft. Kunt u toelichten op welke objectieve en verifieerbare wijze de beschikbaarheid van fysieke werkplekken wordt gedefinieerd en gemeten, en hoe hierbij onderscheid wordt gemaakt tussen fysieke componenten (zoals bureau, monitor, dockingstation) en digitale diensten? Indien een betrouwbare en eenduidige meetmethodiek voor fysieke werkplekken niet kan worden vastgesteld, verzoekt u dan te bevestigen dat: * beschikbaarheidspercentages uitsluitend van toepassing zijn op digitale werkplekdiensten en applicaties, en * fysieke werkplekken worden geborgd via responstijden en hersteltijden na melding, in plaats van via beschikbaarheids-KPI’s."	Aanbestedende Dienst bedoelt hier de softwarematige beschikbaarheid van de werkplekken (diensten, applicaties).

84	2.2 Beschikbaarheidsniveaus	Werkplekken ≥99,5% en Applicaties ≥99,5% "In de concept SLA wordt gesteld dat: de beschikbaarheid van Werkplekken ≥ 99,5% per kwartaal bedraagt, gebaseerd op een beschikbaarheidsvenster van maandag t/m vrijdag van 08:00–18:00 uur; de beschikbaarheid van Applicaties (Office 365 en standaardapplicaties) ≥ 99,5% per kwartaal bedraagt, gebaseerd op een 24/7 beschikbaarheidsvenster; voor beide geldt een maximale downtime van ≤ 10,92 uur per kwartaal. In de bijbehorende toelichting wordt echter aangegeven dat het beschikbaarheidsvenster voor de Werkplekken eveneens 24/7 van toepassing is. Kunt u bevestigen welk beschikbaarheidsvenster leidend is voor de Werkplekken: ma–vr 08:00–18:00 uur of 24/7?"	Voor de Werkplekken is het beschikbaarheidsvenster van ma-vr 08:00 - 18:00 van toepassing.
85	2.2 Beschikbaarheidsniveaus	Disaster Recovery Test Wat verwacht de Opdrachtgever concreet van de jaarlijkse Disaster Recovery Test?	De jaarlijkse Disaster Recovery Test is een test waarbij de noodplannen in de praktijk worden getoetst.
86	Managed Services 48.	"Opdrachtnemer werkt initieel samen met de GGN-eigen Servicedesk en neemt op aangeven van Opdrachtgever de servicedeskwerkzaamheden op termijn deels of in haar geheel als Managed Service over." Aanvullend op Nr 5. Verschuiving verantwoordelijkheden Servicedesken tussen Opdrachtgever en Opdrachtnemer gedurende contractperiode. Kan aangegeven worden wat vanaf start contractperiode verwacht wordt van de Servicedesk samenwerking en kan de term 'op termijn' nader toegelicht worden in kader van tijd?	Ten tijde van de Inbeheername zal de eigen Servicedesk van Aanbestedende Dienst nog volledig de eerste lijns support verzorgen. De verwachting is dat dit na Inbeheername (na 1 jaar) per managed service onderdeel aan de MSP zal worden uitgefaseerd.
87	Managed Services 42.	alle Fysieke en Virtuele werkplekken te allen tijde middels Microsoft Intune (of gelijkwaardig) als Unified Endpoint Management (UEM)-oplossing centraal worden beheerd. Zijn alle huidige werkplekken, zowel virtueel als fysiek, momenteel ook beheerd via Microsoft oplossingen (Intune, Azure)? En geldt dit ook voor de Applicaties die op de Werkplekken actief zijn?	Ja
88	Managed Services 31. & 32.	Elke 24 uur een back-up van specifieke data Hoe lang dient iedere type back-up bewaard te blijven, of wenst Opdrachtgever hier anders mee om te gaan?	Aanbestedende Dienst hanteert een duidelijk onderscheid tussen haar verplichtingen op basis van de Archiefwet en haar verplichtingen op basis van haar ISO27001 en BIO compliance. De back-up valt onder ISO27001, BIO en AVG die stellen dat de beschikbaarheid van informatie wordt geborgd (1 jaar) maar dat de persoonlijke data van medewerkers na 6 maanden dient te worden verwijderd. Kantoorautomatisering & Kantoor-back-up (MSP): 30 tot 90 dagen, Logbestanden (MSSP): 6 maanden tot 1 jaar.
89	Algemene Eisen	"hetzij met gebruikmaking van de GGN-eigen ServiceNow-omgeving hetzij met een koppeling tussen de servicemanagement omgeving van Opdrachtnemer en de GGN-eigen ServiceNow-om" Zijn er minimale vereisten aan een interface tussen GGN-ServiceNow en ITSM-systeem van Opdrachtnemer, zo ja welke?	Uitgangspunt bij een koppeling tussen ITSM van Opdrachtnemer en ServiceNow van Aanbestedende Dienst is dat deze koppeling ISO27001 en specifiek BIO-compliant zijn. Hiermee wordt bedoeld de authenticatie- (oAuth) autorisatie- (Least Privilege) versleuteling- (TLS 1.3) en logging (Elke API call moet gelogd worden) eisen uit de BIO.
90	G4 Kansendossier	Managed Data Intelligence "Kunt u nader inzicht bieden in het huidige Data Intelligence Voorziening? o De huidige architectuur o Gebruikte platform(en) o Betrokken afnemers en leveranciers o De technische rol van de MSP"	Voor de huidige Managed Data Intelligence Services maakt Aanbestedende Dienst gebruik van 2 contractpartijen die uit oogpunt van vertrouwelijkheid hier niet bij naam genoemd worden. Voor de voorzieningen geldt dat er gebruik wordt gemaakt van: - Dataportaal, webapplicatie voor toegangsbeheer tot dashboards, rapportages en content - Power BI voor het samenstellen van dashboards en rapportages - Datakubussen & DeltaGateway voor de OTAP-omgeving, Operational Data Store en Data warehouse-laag - Cloud Hosting op basis van Private Cliud vand e leverancier. G4 vraagt juist aan Inschrijver welke rol deze voor zichzelf ziet (welke kansen deze biedt aan Aanbestedende Dienst) en als MSP en/ of MSSP kan vervullen in Managed Data Intelligence Services.
91	2.6 Omvang van Opdracht	Boven- en ondergrens "In de aanbestedingsdocumenten wordt een ondergrens en bovengrens genoemd, waarbij is aangegeven dat de uiteindelijke omvang van de opdracht niet vooraf is vastgesteld. Gezien het feit dat GGD GHOR Nederland een marktconsultatie heeft uitgevoerd en hieruit een indicatieve bandbreedte is bepaald, verzoeken wij om verduidelijking inzake de beoordeling van inschrijvingen die (significant) onder de ondergrens dan wel boven de bovengrens worden aangeboden. Kunt u bevestigen hoe om te gaan met inschrijvingen waarvan de prijsstelling mogelijk als niet-marktconform of als manipulatief wordt beschouwd? Wordt een inschrijving die duidelijk buiten de vastgestelde bandbreedte valt — zowel aan de onder- als aan de bovenzijde — terzijde gelegd, of wordt deze op een andere wijze beoordeeld binnen het kader van marktconformiteit en proportionaliteit?"	De marktconsultatie en benchmark en de analyse van de kosten van de afgelopen jaren hebben gediend als basis voor de berekening van de Opdrachtwaarde. Tegelijkertijd is Aanbestedende Dienst zich bewust van het feit dat deze berekening (significant) kan afwijken van de daadwerkelijke offertes en heeft daarom het prijscriterium dusdanig uitgewerkt dat een goede beoordeling kan plaats vinden op basis van Implementatiekosten, kosten managed services en kosten van de uren voor alles wat niet standaard onder de kosten van de managed services valt. De ruwe berekening van de Opdrachtwaarde geeft een redelijke verwachting aan maar is geen dwingende bandbreedte.
92	2.6 Omvang van Opdracht	Aantal Netwerkcomponenten 10 Gaat het hier alleen om vast netwerk, of ook draadloos (Wi-Fi) en zijn de geschatte aantallen daarmee realistisch?	Het gaat om bedraad en draadloos (WiFi). 2 firewalls, 4 switches en ongeveer 25 AP's
93	2.2 Buiten scope van Opdracht	het fysieke kantoor van GGD GHOR Nederland Klopt het dat alle statische componenten (servers, netwerkcomponenten, firewalls, printers en vergadervoorzieningen) op 1 locatie actief zijn, of zijn deze verdeeld over meerdere locaties? Zo ja, welke?	Het is correct dat al deze voorzieningen op 1 locatie aanwezig zijn op het kantoor van Aanbestedende Dienst in Utrecht. Op deze locatie bevinden zich overigens geen services e.d. alle voorzieningen worden als cloudservices afgenomen.
94	2.6 Omvang van Opdracht	Aantal Mobiele toestellen 150 "- Corporate, BYOD of mix van toestellen? -Worden deze toestellen beheerd, zo ja hoe? "	Het is een mix van BYOD en corporate mobiele devices. Corporate devices worden volledig beheerd middels Mobile Device Management
95	2.1.3l Binnen Scope van Opdracht	Beheer Servicedesk in samenwerking met de eigen GGD GHOR Nederland-servicedesk Wat is de rol van de Opdrachtnemer in de samenwerking met GGD Servicedesk? Neemt de Opdrachtnemer de volledige Servicedesk over voor de MSP & MSSP dienstverlening (1e lijn Support), of vervult 2e lijn Support, of anders?	Ten tijde van de Inbeheername zal de eigen Servicedesk van Aanbestedende Dienst nog volledig de eerste lijns support verzorgen. De verwachting is dat dit na Inbeheername (na 1 jaar) per servicemanagement domein aan de MSP zal worden uitgefaseerd.
96	1.4 Doelstellingen (Continuïteit)	"De huidige contracten zijn reeds verlengd en lopen einde 2026 af. Het is daarom noodzakelijk deze contracten tijdig te vervangen." Is dit de verantwoordelijkheid van de Opdrachtnemer of adviseert de Opdrachtgever hierin? Aanvullend op de SPOC vraag (nr 1).	De lopende contracten (>12) met huidige leveranciers lopen af. Dit zijn allemaal losse contracten die tezamen de supply chain vormen voor de interne/ eigen Managed Services en Managed Security Services. In plaats van al deze contracten individueel te laten opvolgen en zodoende het versnipperde leverancierlandschap in stand te houden, is het doel van deze aanbesteding om 1 opdrachtnemer te selecteren die middels 1 Overeenkomst voorziet in alle elementen van de interne/ eigen Managed Services en Managed Security Services en die deze as a service (als dienst) beschikbaar maakt.

97	1.1.2 Applicaties, Infra & Cloud	Aanzienlijk aantal verschillende leveranciers tbv dienstovername is inzicht benodigd in het aantal leveranciers en wordt daarbij geacht dat Opdrachtnemer deze leveranciers gaat aansturen? In welke vorm wordt dit verwacht? (SPOC vs Service-integrator (SIAM))?	De lopende contracten (>12) met huidige leveranciers lopen af. Dit zijn allemaal losse contracten die tezamen de supply chain vormen voor de interne/ eigen Managed Services en Managed Security Services. In plaats van al deze contracten individueel te laten opvolgen en zodoende het versnipperde leverancierlandschap in stand te houden, is het doel van deze aanbesteding om 1 opdrachtnemer te selecteren die middels 1 Overeenkomst voorziet in alle elementen van de interne/ eigen Managed Services en Managed Security Services en die deze as a service (als dienst) beschikbaar maakt.
98	1.1.1. Aanleiding	"Uitgangspunt hierbij is dat een groot deel van het momenteel door GGD GHOR Nederland beheerde landschap van applicaties voor de GGD'en en GHOR-bureaus zal worden afgebakend (carve-out) en in beheer zal worden gegeven aan een Landelijke Beheer Organisatie (LBO)" Welke applicaties of onderdelen worden op termijn overgedragen aan een landelijke beheerorganisatie en welke blijven onder verantwoordelijkheid van de MSP?	Of, wanneer en in hoeverre applicaties worden overgedragen is op dit moment nog onderwerp voor besluitvorming. De demarcatie zal liggen bij applicaties die van overheidswege gecontinueerd moeten worden en binnen overheidskaders in beheer moeten blijven. Aanbestedende Dienst GGD GHOR Nederland is géén Overheidsorganisatie in die zin. Wat zeker is is dat de bedrijfsbrede toepassingen zoals AFAS, Kantoorautomatisering, ServiceNow e.d. te allen tijde onder de verantwoordelijkheid van SOC/SIEM en MSSP blijven vallen. Technisch betreft het de logstromen van de systemen HPZone en CoronIT (t.b.v. infectieziektebestrijding) en de BI omgeving daaromtrent (DeltaGateway) aangevuld met de daar aanwezige datacollecties omtrent HPV18+ en ImPex. De vervangende systemen hiervoor zullen worden ondergebracht bij de LBO.
99	1.4 Doelstellingen (Continuïteit)	"De huidige contracten zijn reeds verlengd en lopen einde 2026 af. Het is daarom noodzakelijk deze contracten tijdig te vervangen." Is dit de verantwoordelijkheid van de Opdrachtnemer of adviseert de Opdrachtgever hierin? Aanvullend op de SPOC vraag (nr 1).	De lopende contracten (>12) met huidige leveranciers lopen af. Dit zijn allemaal losse contracten die tezamen de supply chain vormen voor de interne/ eigen Managed Services en Managed Security Services. In plaats van al deze contracten individueel te laten opvolgen en zodoende het versnipperde leverancierlandschap in stand te houden, is het doel van deze aanbesteding om 1 opdrachtnemer te selecteren die middels 1 Overeenkomst voorziet in alle elementen van de interne/ eigen Managed Services en Managed Security Services en die deze as a service (als dienst) beschikbaar maakt.
100	1.1.4.1e Managed Services	Kantoor Cloudhosting Wat wordt concreet verstaand onder 'Kantoor Cloudhosting, betreft dit de 60x virtuele werkplekken zoals genoemd op Prijzenblad, of anders?	Aanbestedende Dienst verstaat onder Kantoor Cloudhosting: Het geheel van managed Cloudhosting voor de volgende domeinen: Productiviteit en samenwerking: Exchange online, Ms Office 365, Teams, Teams Manager, SharePoint Bestandsopslag: Persoonlijke en gedeelde OneDrives, SharePoint Bibliotheken en Azure Files, Back-up en Archivering Werkplekbeheer en Beveiliging: Ms Entra ID, Intune (Endpoint Manager) en security tools (Defender e.d.) Virtual Desktop Infrastructuur (VDI) voor Azure Virtual Desktop (AVD) en Windows 365
101	Beschrijvend document, Paragraaf 2.2	Voor een realistische prijsvorming en het minimaliseren van risico-opslagen verzoeken wij om meer detailinformatie over de huidige (IST) infrastructuur. Kunt u een overzicht verstrekken van de merken en typen van de 10 genoemde netwerkcomponenten en de 2 firewalls? Tevens vernemen wij graag de aard van de 10 servers voor kantoorautomatisering (bijv. Windows/Linux mix en gemiddelde resource-omvang), zodat wij de beheer- en licentielast nauwkeurig kunnen dimensioneren.	Aanbestedende Dienst maakt uitsluitend gebruik van mainstream Commercial Of The Shelf producten/ devices. Zie ook de overige antwoorden in deze Nota van Inlichtingen. MS Windows 11 MS Office 365 MS SharePoint MS Power BI MS Azure Virtual Desktop MS Sentinel: MS Defender for Threat Intelligence MS Office 365 MS Defender for Endpoint Azure Services Entra ID MS Entra ID Protection MS Defender for Business MS Defender for Cloud Apps MS Defender for Office 365 (o.a. Purview alerting DLP) MS Defender for Vulnerability Management Splunk Aanbestedende Dienst heeft de Non Profitstatus conform de voorwaarden van Microsoft. Firewall: Fortigate Switches: Fortigate en Unifi AP's: Unifi Alle niet-Microsoft licenties lopen te allen tijde via de Softwarebroker SoftwareOne.
102	PVE33: Internet, routers en firewalls	Kunt u verduidelijken waar de grens van het beheer op de internetverbindingen ligt? Gaat de aanbestedende dienst ervan uit dat de MSP uitsluitend de randapparatuur (zoals firewalls en routers) beheert en configureert, terwijl het contractmanagement en de tweedelijns ondersteuning vanuit de ISP (lijnleverancier) bij de eigen regie-organisatie van de GGD GHOR blijven?	Dat is correct.
103	PVE30	Eigen backup en recovery die in beheer moet worden genomen. Welke oplossing gebruikt u en welke RTO en RPO eisen zijn hierin ingericht. Hoeveel jaar wordt de backup bewaard?	Zie hiervoor het antwoord op vergelijkbare vragen in deze Nota van Inlichtingen
104	G3 - blz. 42 en G4 - blz. 44	Met betrekking tot de subgunningscriteria G3 en G4 wordt een financieel maximum van € 216.000,- genoemd. Dient dit bedrag te worden beschouwd als een hard prijsplafond voor de volledige mini-businesscase over 4 jaar, of is dit een indicatieve waarde ten behoeve van de prijsvergelijking? Daarnaast verzoeken wij om een nadere functionele duiding van de 'wens-scope' voor deze kansen, zodat inschrijvers een realistische en vergelijkbare businesscase kunnen opstellen die aansluit bij uw ambities voor data-gedreven werken.	Aanbestedende Dienst is gehouden aan de Aanbestedingswetgeving en de daaraan verbonden aanbestedingsbedragen en drempels. Derhalve hanteert Aanbestedende Dienst een prijsplafond van 216.000,- voor de volledige mini-businesscase over 4 jaar. Indien de businesscase het plafond overschrijdt dan is Aanbestedende Dienst verplicht dit in een aparte procedure aan te besteden. Aanbestedende Dienst heeft met zorg de doelstellingen per Kansendossier geformuleerd en hierover heldere vragen gesteld. Onduidelijk is derhalve wat u bedoelt met functionele duiding van de wens-scope

105	Blz. 18 eis NEN7510 of gelijkwaardig	Kunt u nader specificeren wat de aanbestedende dienst verstaat onder 'gelijkwaardige bewijzen' voor de NEN 7510?	De Aanbestedingswet verbiedt het om in een specificatie te verwijzen naar een specifiek merk, octrooi of een specifieke herkomst. Aanbestedende Dienst heeft derhalve ' of vergelijkbaar' toegevoegd op basis van juridische noodzaak binnen het Aanbestedingsrecht.
106	Beschrijvend document, Paragraaf 2.2	Hoewel de levering van hardware buiten de scope van de opdracht valt, heeft de technische specificatie van deze hardware directe impact op de beheersbaarheid (o.a. via Hello-ID en ServiceNow) en de security-compliancy (o.a. MFA-ondersteuning en Intune-beheer). Is de aanbestedende dienst bereid om in de implementatiefase (fase G1) gezamenlijk een 'Preferred Hardware List' of een set technische minimumeisen vast te stellen waaraan nieuwe hardware moet voldoen, zodat de MSP de gegarandeerde servicelevels en beveiligingsstandaarden kan blijven borgen?	Zolang dit betrekking heeft op alle nieuw aan te schaffen hardware na de inbeheername is dit akkoord voor Aanbestedende Dienst.
107	Beschrijvend document, Paragraaf 2.6	"Voor het correct dimensioneren van de gevraagde geïntegreerde oplossing voor Network Detection & Response (NDR), inclusief IDS/IPS, is de huidige informatie over het logvolume (EPS/GB per dag) onvoldoende. NDR-oplossingen worden primair gecalculeerd op basis van netwerkdoorvoer, het aantal inspectiepunten en de aard van het verkeer. Kan de aanbestedende dienst ten behoeve van een realistische prijsvorming en technisch ontwerp de volgende aanvullende informatie verstrekken: 1.Netwerkdoorvoer (Throughput): Wat is de gemiddelde en de piekdruk van het netwerkverkeer (in Mbps of Gbps) dat geïnspecteerd moet worden op de centrale knooppunten (zoals de firewalls en core-switches)? 2.Verdeling On-premise vs. Cloud: Hoeveel van het te monitoren netwerkverkeer bevindt zich binnen de fysieke kantooromgeving in Utrecht en hoeveel betreft 'oost-west' verkeer binnen de Azure Cloud-omgeving (Landing Zones)? 3.Inspectiepunten: De parameters noemen 2 firewalls en 10 netwerkcomponenten. Kan worden bevestigd of dit ook de beoogde locaties zijn voor NDR-sensoren (bijv. via TAP/SPAN-poorten), of dat er ook inspectie van virtueel netwerkverkeer in Azure wordt verwacht? 4.Versleuteld verkeer: Welk percentage van het interne netwerkverkeer is momenteel versleuteld (SSL/TLS) en heeft de aanbestedende dienst een eis of wens ten aanzien van SSL-decryptie voor diepe pakketinspectie (DPI) door de NDR-oplossing? 5.Samenhang met Managed Services: Aangezien de opdrachtnemer de netwerkinfrastructuur ""as-is"" in beheer neemt, is er ruimte om tijdens de implementatiefase (G1) de netwerksegmentatie aan te passen om de effectiviteit van NDR te vergroten?"	Aanbestedende Dienst is van menig dat met de functionele uitvraag (i.t.t. technisch) en de gegeven parameters voldoende is gespecificeerd. Indien deze vragen bepalend zijn voor uw inschrijving dan verzoeken wij u de vragen opnieuw en afzonderlijk te formuleren met de door u gehanteerde definities in de volgende vragenronde.
108	Eis 84	De opdrachtnemer is verantwoordelijk voor een geïntegreerde oplossing voor Network Detection & Response (NDR). Om de juiste hoeveelheid en locaties van sensoren te bepalen (bijv. voor oost-west verkeer in Azure vs. kantoorlocaties), is inzicht in de huidige netwerktopologie essentieel. Is de aanbestedende dienst bereid om een (geanonimiseerd) overzicht van de centrale netwerkinfrastructuur en de koppelingen tussen de Cloud Landing Zones en de fysieke locaties beschikbaar te stellen?	Ja, Dit wordt uitgezocht voor de volgende vragenronde.
109	Bijlage A - Programma van Eisen, eis 5	"De aanbestedende dienst stelt in eis 5 dat rechten voor beheeraccounts te allen tijde via Privileged Identity Management (PIM) moeten worden uitgegeven. De opdrachtnemer onderschrijft dit principe volledig als middel om de 'attack surface' te verkleinen. Voor een robuust en conform de Marktpraktijk ingericht Identity & Access Management (IAM) ontwerp, vragen wij om een nadere duiding van de reikwijdte in specifieke scenario's. Kan de aanbestedende dienst bevestigen of de verplichting tot het gebruik van PIM onverkort van toepassing is op de volgende drie categorieën, of dat hiervoor (onder voorwaarden) uitzonderingen zijn toegestaan: 1.Nood- en Break-glass accounts: Conform internationale standaarden (zoals NCSC-richtlijnen en Microsoft Best Practices) wordt geadviseerd om een beperkt aantal 'emergency access' accounts te hebben die geen afhankelijkheid hebben van de reguliere PIM-infrastructuur of MFA-oplossingen, om uitsluiting bij grote verstoringen te voorkomen. Is de aanbestedende dienst bereid deze specifieke uitzondering toe te staan? 2.SOC-tooling buiten het Microsoft-platform: De scope omvat ook tools zoals Splunk. Geldt de PIM-eis hier specifiek voor de integratie met Microsoft Entra ID PIM, of volstaat een vergelijkbaar mechanisme voor Just-In-Time (JIT) access dat eigen is aan de betreffende applicatie? 3.Accounts van onderaannemers: Indien de opdrachtnemer gebruikmaakt van gespecialiseerde onderaannemers, dienen zij dan verplicht te worden gefedereerd/onboarded in de PIM-omgeving van de GGD-tenant, of is het toegestaan dat zij hun beheertaken uitvoeren vanuit een eigen, aantoonbaar gelijkwaardig beveiligde PIM-omgeving? Indien uitzonderingen zijn toegestaan, aan welke aanvullende compenserende maatregelen (bijv. verscherpte logging of fysieke kluisprocedures) dient de opdrachtnemer dan minimaal te voldoen?"	Ad 1: Onder voorwaarden zijn uitzonderingen toegestaan Ad 2: De PIM eis geldt hier vor de integratie met.. Ad 3: Zij dienen verplicht te worden gefedereerd Noodzakelijke / Gewenste Uitzonderingen op eis 5 dienen bij de Due Diligence te worden geidentificeerd aan de hand waarvan compenserende maatregelen worden overeengekomen.
110	Beschrijvend document, Paragraaf 2.4	Voor een effectieve ketenbeveiliging is de aansluiting tussen het ISMS van de opdrachtnemer en het managementsysteem van de GGD cruciaal. Kan de aanbestedende dienst verduidelijken welke specifieke onderdelen van het ISMS (zoals de risico-registraties, auditrapportages of de Baseline Informatiebeveiliging Overheid (BIO) compliance-matrix) integraal gedeeld of gekoppeld moeten worden met de GGD-organisatie, aanvullend op de maandelijkse rapportages?	Er is in het Beschrijvend Document door Aanbestedende Dienst niets vermeld over koppellingen tussen uw ISMS en dat van Aanbestedende Dienst.
111	Hoofdstuk 6, Subgunningscriterium G1 & Bijlage A, Eis 80	"Ten behoeve van een vlekkeloze transitie en een reëel 'Implementatie- en Uitrolplan' (Subgunningscriterium G1), verzoeken wij de aanbestedende dienst om meer inzicht in de huidige SOC/SIEM-volwassenheid. Kunt u aanvullende informatie verstrekken over: • Het huidige aantal en de aard van de actieve Use Cases; • De mate waarin SOAR-automatisering reeds is doorgevoerd; • De huidige verdeling van logbronnen tussen Microsoft Sentinel en Splunk?"	Het aantal Use Cases is 300 - zie documentatie en Prijzenblad SOAR automatisering is niet toegepast. Sentinel: MS Defender for Threat Intelligence MS Office 365 MS Defender for Endpoint Azure Services Entra ID MS Entra ID Protection MS Defender for Business MS Defender for Cloud Apps MS Defender for Office 365 (o.a. Purview alerting DLP) MS Defender for Vulnerability Management Firewall syslog van HPZone omgeving Keeper SPLUNK: Delta Gateway (iMPeX en HPV18+) TOPdesk SOC SPLUNK via Logbuffet: HPZone GraphQL CoronIT iTBC iTBC IMS EVS Cluster TBC EVS Cluster SG (25 keer) PGA Registratieschil
112	Bijlage A - Programma van Eisen, Eis 4	In eis 4 van het Programma van Eisen wordt een 'strikte scheiding' gevraagd tussen de teams voor Managed Services en Managed Security Services. Om een integraal beheer- en veiligheidsmodel te ontwerpen dat voldoet aan uw administratieve organisatie-eisen, vragen wij om een nadere precisering van deze scheiding. Dient deze scheiding uitsluitend personeel te zijn (geen overlap in uitvoerende medewerkers), of strekt dit zich ook uit tot de governance (gescheiden rapportagelijnen), de gebruikte tooling (gescheiden backend-systemen) en/of de juridische entiteit?	Deze scheiding is vereist vanuit administratief organisatorisch oogpunt: Aanbestedende Dienst wil hiermee bereiken dat 'de slager niet zijn eigen vlees keurt' - met andere woorden: tenminste een scheiding van personeel en rapportagelijnen. Dit betreft niet een scheiding van juridische entiteiten.
113	PvE 31	Kunnen jullie specificeren welk back-up-product en API-bandbreedte acceptabel is, de RPO/RTO doelen, objectniveau-herstel en of Entra-ID herstel tenant-breed of granulair (config-items) moet zijn?	Aanbestedende Dienst maakt gebruik van AvePoint als Back-up voorziening. Aanbestedende Dienst hanteert een duidelijk onderscheid tussen haar verplichtingen op basis van de Archiefwet en haar verplichtingen op basis van haar ISO27001 en BIO compliance. De back-up valt onder ISO27001, BIO en AVG die stellen dat de beschikbaarheid van informatie wordt geborgd (1 jaar) maar dat de persoonlijke data van medewerkers na 6 maanden dient te worden verwijderd. Kantoorautomatisering & Kantoor-back-up (MSP): 30 tot 90 dagen, Logbestanden (MSSP): 6 maanden tot 1 jaar. De zaken waar u naar vraagt betreffen technische configuratie, welke bij de Due Diligence overeen wordt gekomen. Indien dit bepland is voor uw inzending dan verzoeken wij u de vraag ind e tweede vragenronde te verduidelijken.
114	PvE 25	Welke governance- en controlemomenten eist Opdrachtgever bij de CSP-rolovername en wat is de strategie om licentie-continuïteit te borgen?	Inschrijver wordt verwacht dit te adresseren in het G1 implementatieplan. U kunt er van uitgaan dat Aanbestedende Dienst een projectteam hiervoor beschikbaar heeft.

115	PvE 6	Opdrachtgever eist dat alle data die gepaard gaan met MSP/MSSP binnen de EER worden bewaard. Hoe moet dit worden toegepast bij support-vendors? Is data-lokalisatie vereist voor alle log- en case-data inclusief hot/cold storage en back-ups van SIEM? Hoe verhoudt e.e.a. zich tot de CLOUD-Act?	Het feit dat enige verwerking aantoonbaar buiten de EER geschiedt is voldoende aanleiding voor Aanbestedende Dienst om verwerking buiten de EER te beoordelen. Opdrachtnemer dient verwerking buiten de EER te allen tijde vooraf te melden aan Aanbestende Dienst. De criteria die Aanbestedende Dienst hierbij hanteert zijn afhankelijk waar buiten de EER die verwerking zal plaatsvinden en welke risico's dat met zich meebrengt. Zo zal verwerking in bijvoorbeeld de VK of Zwitserland (naar verwachting) minder risicovol zijn dan verwerking in bijvoorbeeld Wit-Rusland of Oekraine.
116	PvE 13	Het PvE verbiedt inzet van AI/LLM's tenzij vooraf getoetst door CISO-office. Kunnen jullie definiëren of dit verbod alle AI-toepassingen raakt en zo ja, welke whitelist of beoordelingskaders (risicoklassen, datastromen, model-hosting binnen EER) gelden voor toestemming?	Aanbestedende dienst is zich bewust van- en maakt reeds gebruik van- de in Microsoftproducten geïntegreerde AI-functionaliteiten. Aanbestedende dienst wenst daarom Eis 13 als volgt aan te passen: Opdrachtnemer garandeert dat voor de levering van managed services en managed security services, geen gebruik gemaakt zal worden van Kunstmatige Intelligentie (AI), Large Language Models e.d. behoudens de reeds in Microsoftproducten aanwezige AI-functionaliteiten, tenzij dit in overleg met Opdrachtgever schriftelijk anders is overeengekomen en vooraf is getoetst aan het GGN AI-beleid en door het CISO-office. Het beleidsdocument kan in deze fase (nog) niet gedeeld worden.
117	PvE 4	Jullie vragen een strikte scheiding tussen MSP- en MSSP-teams, maar contracteren ze in één perceel bij één contractant. Kunnen jullie toelichten welke organisatorische, technische en juridische controles (bijv. Chinese walls, gescheiden SOC tooling/tenancy, gescheiden rollen in ServiceNow, onafhankelijke managementrapportage) minimaal vereist zijn om belangenconflicten te voorkomen?	Aanbestedende Dienst heeft de verdeling in percelen onderzocht en inhoudelijk gemotiveerd waarom is gekozen voor het NIET onderverdelen in percelen. Aanbestedende Dienst heeft gedurende de Covid-19 pandemie een groot aantal taken en voorzieningen verzorgd die op dat moment kritiek en nodig waren. Nu de Covid-19 pandemie ten einde is, stopt eveneens de financiering van overheidswege, hetgeen Aanbestedende Dienst noopt tot grote reducties van externe en interne medewerkers en het (verantwoord) afstoten/ overdragen/ uitfaseren van vrijwel al haar niet essentiële taken. Aanbestedende Dienst keert daarom in vorm en volume terug naar haar oorspronkelijke taken van voor de Covid-19 pandemie en behoudt uitsluitend een regierol voor de voorzieningen van haar leden (GGD'en en GHOR's). Zij gaat in feite terug naar een min of meer standaard mkb-organisatie. Door de aanbesteding niet in percelen te verdelen verwacht Aanbestedende Dienst ondanks haar geringe omvang toch voldoende interessant te zin voor MSP's en MSSP's Aanbestedende Dienst heeft tijdens de marktconsultatie vastgesteld dat er een aanzienlijk aantal partijen juist hebben geadviseerd de MSP en MSSP gezamenlijk aan te besteden zonder percelen. Aanbestedende dienst heeft ten aanzien van objectiviteit, controleerbaarheid en risicobeheersing eisen gesteld in het PvE
118	PvE 58	Er worden 'proven" en "mainstream" producten verlangd. Welke objectieve bronnen gelden als toets; en hoe gaan we om met innovaties die (nog) niet in een MQ voorkomen maar wel aantoonbaar geschikt zijn?	Proven en Mainstream verwijzen onder meer naar of het gangbare producten zijn, of ze vrij en breed verkrijgbaar zijn en bijvoorbeeld marktaandeel en gebruikersbase. Als een product nog niet in een Magic Quadrant staat betekent dit niet dat het niet Proven of Mainstream is.
119	PvE 49	Willen jullie 'hoofdversie' definiëren voor client-applicaties (b.v. browser/Teams) en beheerapplicaties?	Hoofdversie verwijst naar een major version, het eerste digit in een versienummer.
120	PvE 44	Kunnen jullie de koppelspecificaties delen voor toegang/uitgifte via Hello-ID of gelijkwaardig, inclusief het ownership van identity-workflows (GGN vs MSP)?	Aanbestedende Dienst begrijpt deze vraag niet. Gelieve deze vraag in de volgende vraag te verduidelijken. Aanbestedende Dienst is van mening dat de Functioneel gespecificeerde eis voldoende duidelijk is.
121	PvE 41	Is er een capaciteitsplanning en sizing-referentiebeeld beschikbaar waarop de 100 extra VDI's binnen 48 uur gebaseerd zijn? Hoe worden licenties (bijv. M365) en netwerk-egress tijdens nood-opschaling gegarandeerd, en wie draagt het financiële risico bij stand-by capaciteit?	Aanbestedende Dienst heeft deze Eis functioneel beschreven. Aangezien ook de CSP onderdeel uitmaakt van de MSP-dienstverlenign gaat Aanbestedende Dienst er van uit dat de licenties geen probleem zouden moeten zijn.
122	PvE 34	Jullie refereren aan NCSC-termijnen voor kritieke updates. Willen jullie het x-aantal dagen na vendor-release expliciet vastleggen per risicoklasse (bijv. 7/14/30 dagen), inclusief uitzonderingsprocedure?	Ja.
123	GIBIT 2023 - Artikel 11.5	GIBIT 2023 - Artikel 11.5 Gegadigde acht de laatste zin niet realistisch en stelt voor deze zin te verwijderen.	Niet akkoord. Er staat immers al "tenzij anders overeengekomen".
124	GIBIT 2023 - Artikel 10.14	GIBIT 2023 - Artikel 10.14 Gegadigde wenst aan het artikel het volgende toe te voegen: "iii) er geen sprake is van een tekortkoming van Leverancier in het kader van Onderhoud indien een Update en/of Upgrade benodigd is om security en/of continuïteit te borgen en Opdrachtgever de ingebruikname van die Update of Upgrade weigert."	Niet akkoord. Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd.
125	GIBIT 2023 - Artikel 4.2 i.	GIBIT 2023 - Artikel 4.2 i. Gegadigde is van oordeel dat het niet in alle gevallen redelijk is om de einddatum voor de Implementatie als fatale termijn te laten gelden. Gegadigde stelt voor om hierover in de Overeenkomst dan wel in het Implementatieplan nadere afspraken te maken en artikel 4.2 in zoverre buiten toepassing te verklaren.	Niet akkoord. In het Implementatieplan kunt u de planning uitwerken waarbij er voldoende evaluatie en tussentijdse oplevermomenten zijn om de planning tijdig bij te stellen indien dit noodzakelijk is.
126	GIBIT 2023 - Artikel 3.3	GIBIT 2023 - Artikel 3.3 Wij verzoeken u de volgende zin tussen de eerste en derde te voegen in artikel 3.3: "Opdrachtgever zal proactief de Leverancier tijdig van adequate informatie voorzien indien en voor zover zij in redelijkheid geacht kan worden te begrijpen dat de informatie voor Leverancier van belang is."	Niet akkoord. Aanbestedende Dienst hanteert hier de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd.
127	GIBIT 2023 - Artikel 18.5 en 24.14	GIBIT 2023 - Artikel 18.5 en 24.14 Gegadigde verzoekt 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 bewaarverplichtingen."	Niet akkoord. Aanbestedende Dienst hanteert hier de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd.
128	GIBIT 2023 - Artikel 17.2	GIBIT 2023 - Artikel 17.2 Gegadigde maakt deel uit van een concern waarvan de moedermaatschappij jaarlijks verzekeringen sluit/verlengt voor alle wereldwijde opererende entiteiten. Het is daarbij niet mogelijk klantspecifieke en opdrachtspecifieke afspraken te maken over de verzekeringspolis en de te verzekeren bedragen zoals die worden verlangd in artikel 17.2. Gegadigde verzoekt u dit lid te schrappen en te volstaan met lid 1.	Niet akkoord. Aanbestedende Dienst hanteert hier de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd.
129	GIBIT 2023 - Artikel 16.4	GIBIT 2023 - Artikel 16.4 Gegadigde verzoekt aan het artikel het volgende toe te voegen: "De in dit lid bedoelde aansprakelijkheid is beperkt tot vergoeding van directe schade. Aansprakelijkheid van partijen voor indirecte en/of gevolgschade is uitgesloten. Onder indirecte en/of gevolgschade wordt onder andere verstaan gederfde winst, gemiste besparingen, geleden verlies, verminderde goodwill en schade door bedrijfsstagnatie."	Niet akkoord. Aanbestedende Dienst hanteert hier de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd.
130	GIBIT 2023 - Artikel 16.3	GIBIT 2023 - Artikel 16.3 Gegadigde verzoekt het artikel als volgt aan te passen: "De in lid 1 bedoelde aansprakelijkheid voor persoons- en zaakschade is beperkt tot vergoeding van directe schade en tot een bedrag van € 1.250.000,– per gebeurtenis en € 2.500.000,- per jaar. Samenhangende gebeurtenissen worden daarbij aangemerkt als één gebeurtenis. De aansprakelijkheid van partijen voor indirecte en/of gevolgschade is uitgesloten. Onder indirecte en/of gevolgschade wordt onder andere verstaan gederfde winst, gemiste besparingen, geleden verlies, verminderde goodwill en schade door bedrijfsstagnatie."	Niet akkoord. Aanbestedende Dienst hanteert hier de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd.
131	GIBIT 2023 - Artikel 26.11	GIBIT 2023 - Artikel 26.11 Gegadigde verzoekt het volgende aan het artikel toe te voegen: "Partijen zullen alle relevante factoren laten meewegen bij het bepalen van de verlengingsperiode die in het betreffende geval redelijk is, waaronder, doch niet uitsluitend, de omvang van de voort te zetten werkzaamheden, de mate waarin Leverancier mensen en middelen beschikbaar kan houden gelet op de contractuele verplichtingen die hij heeft jegens andere opdrachtgevers, de partij aan wie toerekenbaar is dat een verlenging noodzakelijk is."	Niet akkoord omwille van de continuiteit van GGD GHOR.
132	GIBIT 2023 - Artikel 25	GIBIT 2023 - Artikel 25 Gegadigde verzoekt 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.	Zie het antwoord op vraag 141. Aanbestedende Dienst heeft zelf een Team Audit & Compliance en Audits worden te allen tijde uitgevoerd door daartoe geaccrediteerde functionarissen of organisaties.
133	GIBIT 2023 - Artikel 24.2	GIBIT 2023 - Artikel 24.2 Gegadigde verzoekt u om in afwijking van artikel 24.2 van de GIBIT een opzegtermijn voor Leverancier op te nemen van 6 maanden, onder uitsluiting van artikel 7:408 lid 1 en 2 van het Burgerlijk Wetboek.	Niet akkoord. Aanbestedende Dienst hanteert hier de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd.
134	GIBIT 2023 - Artikel 23.1	GIBIT 2023 - Artikel 23.1 Gegadigde verzoekt het artikel enigszins te objectiveren door dit als volgt te wijzigen: "Opdrachtgever kan vervanging verlangen van Personeel, indien hij daartoe gegronde redenen heeft en deze redenen redelijkerwijs de wens tot vervanging rechtvaardigen."	Niet akkoord. Aanbestedende Dienst hanteert hier de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd.
135	Concept Overeenkomst art. 17.5–17.7	Kan u bevestigen dat eventuele audits niet door een concurrent worden uitgevoerd en met een redelijke termijn vantevoren (bijvoorbeeld 30 dagen) worden aangekondigd?	Zie het antwoord op vraag 141 en 132.

136	Concept Overeenkomst art. 17.5–17.7	Kan u bevestigen dat gecoördineerde pentest-vensters en respons-SLA's worden afgesproken, en dat pentests/audits die buiten scope van de MSP/MSSP-omgeving vallen (bijv. vendor cloud of Microsoft tenant) risicogestuurd worden ingeregeld met shared responsibility? Hoe worden kostenverdeling en remediatie-deadlines vastgelegd?	Pentesten worden op initiatief van Aanbestedende Dienst uitgevoerd en altijd in overleg met Opdrachtnemer.
137	Beschrijvend document 2.9.2	De optionele Managed Cloudhosting en Managed Data Intelligence Services kunnen later geactiveerd worden. Kunnen jullie de toetsingscriteria voor 'geen wezenlijke wijziging' concretiseren (omvang, prijsplafond, scope-afbakening) en de beslisgovernance (wie beslist, binnen welke doorlooptijd)?	Dit is de juridische formulering waarmee Aanbestedende Dienst aangeeft dat de Kansendossiers optioneel zijn. Indien gebruik wordt gemaakt van 1 of beide Kansendossiers dan zal dat te allen tijd conform de beschreven Kansen zijn en daar niet vanaf wijken. Aanbestedende Dienst beoogt als eerste de MSP en MSSP te implementeren. Aanvullend daarop zal Aanbestedende Dienst in overleg met Opdrachtnemer kijken naar de noodzaak/ wens/ mogelijkheid om de kansen uit het Kansendossier MDISP en Managed Cloudhosting gedurende de geldigheid van de overeenkomst te realiseren.
138	Artikel 21.2 van de conceptovereenkomst.	Opdrachtgever mag bij crisis SLA-KPI's eenzijdig verhogen en opschaling eisen. Kunnen jullie verduidelijken hoe dit qua kosten in zijn werk gaat?	Aanbestedende Dienst zal in een dergelijke situatie altijd overleg plegen met Opdrachtnemer. Mits Opdrachtnemer de additioneel overeengekomen kosten transparant inzichtelijk maakt, komen deze kosten voor rekening van Opdrachtgever.
139	PvE 60-61	Jullie eisen conformiteit met verplichte standaarden Forum Standaardisatie en 'ruim voldoende versleuteling'. Kunnen jullie de minimale eisen nader specificeren?	Zie Forum Standaardisate: Minimaal TLS 1.2, bij voorkeur 1.3 met sterke cipher suites
140	Concept Overeenkomst art. 3.6.	De boete is 5% van de jaarlijkse fee. Kunt u verduidelijken: (a) geldt dit per mijlpaal of alleen bij totale oplevering; (b) is er een cumulatief plafond; (c) hoe wordt toerekenbaarheid vastgesteld bij afhankelijkheden?	Het Implementatieplan (G1) en de daarin benoemde planning en mijlpalen worden geacht behaald te worden. De boete betreft het (niet) realiseren van het Implementatieplan zoals dat is ingediend.
141	Concept overeenkomst art. 3.5	Kunt u specificeren welke objectieve criteria bepalen dat Opdrachtnemer "structureel niet voldoet", en bevestigen dat inschakeling van derden alleen plaatsvindt na aantoonbare toerekenbaarheid, voorafgaande hersteltermijn en transparante, marktconforme kosten, conform de procedure voor verzuim in art. 16.2 GIBIT?	Aanbestedende Dienst doet de aanname dat de ICT-prestatie professioneel wordt geleverd en dat voorafgaand en tijdens de dienstverlening solide overlegstructuren worden ingeregeld via welke eventuele tekortkomingen worden gemeld (ITIL) en indien nodig worden geëscaleerd. Het structureel niet voldoen zal blijken uit de administratie van deze meldingen, zoals het DAP
142	Beschrijvend document 6.3/6.4	Kunnen jullie toelichten hoe consistentie tussen reviewers wordt geborgd (kalibratie/scorecards) en of er een nabespreking of presentatie toegestaan is om inherente ambiguïteiten in een 10-pagina's document (G1/G2) te verhelderen vóór definitieve scoring?	Aanbestedende Dienst heeft gekozen voor de Gewogenfactormethode. Beoordeling vindt eerst individueel plaats door een beoordelingsteam van 9 materie-deskundigen, waarna middels een consensusmeeting de definitieve kwalitatieve uitslag wordt bepaald. Er is geen mogelijkheid tot het mondeling toelichten van uw inzending
143	PvE 79	Jullie eisen dat alle functionaliteiten blijvend beschikbaar zijn gedurende de looptijd van de overeenkomst maar ook daarna. Kunnen jullie duiding geven hoe hoermee om te gaan bij exit als het een derde-leverancier betreft? bevestigen dat IP-rechten op door opdrachtnemer ontwikkelde use-cases en content bij de opdrachtnemer liggen, inclusief recht op hergebruik door de opvolger?	Alle bestaande functionaliteiten die ten tijde van de afroep van het exitscenario actief zijn, dienen zorgvuldig en volledig te worden overgedragen aan de opvolgende partij.
144	Beschrijvend document 2.6	De parameters noemen o.a. 350 EPS en 10 GB/dag. Kunnen jullie bevestigen dat de parameters plafonds zijn voor de prijsinschatting en dat meer-verbruik (bij incident pieken) tegen staffels mag worden afgerekend?	De parameters zijn gekozen op basis van actuele waarden. De tarieven die U invult worden gehanteerd voor de definitieve Overeenkomst. De verwachting is (zie Beschrijvend Document) dat de aantallen/ volumes op termijn zullen afnemen.
145	Beschrijvend document 7.10	Welke objectieve toets wordt gehanteerd voor 'manipulatief inschrijven'? Wordt bv. een abnormaal lage inschrijving-onderzoek (ALI) procedure toegepast met kostprijs-opening en zekerheidsstelling bij acceptatie?	Het Prijzenblad is tot stand gekomen op basis van onder andere de Marktconsultatie en analyse van de huidige kostenstructuren. Aanbestedende dienst verwacht op basis van het Prijzenblad daarom tarieven en bedragen die binnen een bandbreedte vallen en die onderling niet meer afwijken dat 2 x de standaarddeviatie. Indien buiten deze bandbreedten wordt geoffreerd volgt een onderzoek.
146	Beschrijvend document 6.8 (P1)	Kunnen jullie de exacte formule voor P1 bevestigen (Implementatie + Jaarsom MSP + Implementatie + Jaarsom MSSP) incl. aannames over volume-parameters (FTE, EPS/GB/dag) en looptijd voor de jaarsommen binnen de beoordelingsprijs?	De Beoordelingsprijs omvat de Implementatie + Jaarsom MSP + Implementatie + Jaarsom MSSP. De parameters waarmee wordt gerekend zijn terug te vinden in het Prijzenblad en de Jaarsommen worden alleen berekend voor het eerste jaar.
147	Concept Overeenkomst art. 14.6	In de Overeenkomst staat dat ontbrekende exit-werkzaamheden kosteloos zijn, tenzij onvoorzien. Kunnen jullie hierbij accepteren dat ontbrekende exit-activiteiten gefactureerd mogen worden, mits op voorhand voor akkoord voorgelegd aan opdrachtgever?	Aanbestedende Dienst verwacht dat er bij aanvang een Exitplan conform Bijlage Q wordt opgesteld waarin de kosten voor een exit-scenario worden begroot. Dit exitplan dient tenminste jaarlijks te worden bijgewerkt en door Aanbestedende Dienst te worden goedgekeurd.
148	Indexering	In het DFA wordt gesproken over indexering per 1-1-2028 o.b.v. CBS J62/J6202 én elders over CPI en tussentijdse aanpassingen. Kunnen jullie de leidende index eenduidig vastleggen?	Ja er wordt een relevante index overeengekomen.
149	Beschrijvend document 3.9	Jullie plannen vier verificatiegesprekken (account, CISO, privacy, operations). Kunnen jullie de objectieve afwijzingsgronden publiceren (checklist) en aangeven of er een hersteltermijn is bij kleinere onvolkomenheden in bewijsvoering?	De verificatiegesprekken account, CISO, Privacy en Operations zijn ingesteld op basis van het 4-ogen principe waarin zij het werk van de materiedeskundigen uit de beoordelingscommissie controleren. Dit proces wordt zorgvuldig genotuleerd in een Verificatieverslag. Indien er bezwaren naar boven komen dan worden deze bezwaren te allen tijde volledigschriftelijk en juridisch onderbouwd kenbaar gemaakt in het Verificatieverslag.
150	Eis 84	Kan GGN inzicht geven in de Firewall oplossingen die op dit moment toegepast worden. Merken/Typen/Contracten?	Firewall: Fortigate Switches: Fortigate en Unifi AP's: Unifi
151	Eis 47	Kan GGN aangeven welke zakelijke telecommunicatievoorzieningen in gebruik zijn inclusief aantallen?	De huidige provider van Zakelijke Telecom is Odido, er wordt gebruik gemaakt van Odido Hosted Voice en Odido Virtuele Telefooncentrale. Odido levert tevens circa 100 mobiele abonnementen.
152	Eis 46	Kan GGN aangeven hoeveel vergadervoorzieningen in gebruik zijn. Welke merken en types en welke oplossing.	Aanbestedende Dienst maakt gebruik van een 10-tal vergaderopstellingen van Barco. Dit betreft Vergaderschermen, webcams, microfoons en de mogelijkheid schermen van de werkplek te delen in de vergaderopstellingen.
153	Eis 45	Kan GGN aangeven hoeveel printen en reproductie apparaten in gebruik zijn. Welke merken en types en welke printoplossing.	Aanbestedende Dienst maakt op dit moment gebruik van print devices van Veenman en Printix voor secure Cloud Print Management. De verwachting ten aanzien van de Inschrijver is dat deze de printvoorzieningen as-is in beheer overneemt waarna wij de overeenkomst met de huidige leverancier kunnen beëindigen en vanaf dat moment zowel de devices als het Cloud Print Management als dienst afnemen van Opdrachtnemer.
154	Eis 42	Kunnen jullie aangeven hoe dit op dit moment is ingeregeld en of de werkplekken al met Intune zijn ingericht en als er al een Unified Endpoint Management (UEM) in gebruik is welk dit dan is.	De werkplekken zijn al met InTune ingericht, dit wordt ook gebruikt voor UEM
155	Eis 37	Dezelfde omgeving is een rekbaar begrip. Kunnen jullie gedetailleerd beschrijven wat jullie hiermee precies bedoelen?	Hiermee wordt bedoeld dat behoudens de hardware (bijvoorbeeld laptop) alle medewerkers dezelfde gebruikerservaring hebben, ongeacht of ze een fysieke werkplek (laptop) of een virtuele werkplek ter beschikking hebben gekregen.
156	Eis 37	Is wat hier als eis wordt gesteld ook al in de huidige omgeving ingeregeld of is dit een nieuwe eis?	Het betreft hier de huidige situatie.
157	Eis 36	Welke oplossing gebruikt GGN nu voor virtuele werkplekken.?	Azur Virtual desktop en W365
158	Eis 35	Kan GGN duiden welke fysieke werkplekken het betreft? PC, Laptop, Tablet, OS versie, docking, wifi, bedraad, hoeveel externe monitoren, etc.	U kunt hierbij uitgaan (zie ook Parameters en Prijzenblad) van 200 fysieke werkplekkken. Dit zijn Laptops. Docking stations en Monitoren vallen onder de Hardwaremantel en zijn geen onderdeel van deze aanbesteding.
159	Eis 33	Welke besturingssystemen zijn in gebruik? Kan GGN een overzicht geven van alle workloads en de specificaties ervan?	Zie specificatie van de Kantoorautomatsiering elders in deze Nota van Inlichtingen

160	Eis 31	Is een dergelijke oplossing op dit moment al in gebruik? Zo ja, welke oplossing is dit?	Aanbestedende Dienst maakt gebruik van AvePoint als Back-up voorziening. Aanbestedende Dienst hanteert een duidelijk onderscheid tussen haar verplichtingen op basis van de Archiefwet en haar verplichtingen op basis van haar ISO27001 en BIO compliance. De back-up valt onder ISO27001, BIO en AVG die stellen dat de beschikbaarheid van informatie wordt geborgd (1 jaar) maar dat de persoonlijke data van medewerkers na 6 maanden dient te worden verwijderd. Kantoorautomatisering & Kantoor-back-up (MSP): 30 tot 90 dagen, Logbestanden (MSSP): 6 maanden tot 1 jaar. De zaken waar u naar vraagt betreffen technische configuratie, welke bij de Due Diligence overeen wordt gekomen. Indien dit bepland is voor uw inzending dan verzoeken wij u de vraag ind e tweede vragenronde te verduidelijken.
161	Eis 30	Eis is dat de opdrachtnemer de GGN-eigen voorzieningen voor Kantoor Back-up & Recovery as-is als Managed Services in beheer neemt. Kan GGN informatie geven over de in gebruik zijnde oplossing, hoeveelheid entitieten die gebackupt worden, de hoeveelheid data per back-upcyclus. De hoeveelheid data van een volledige back-up, retentietijden, jobtypes en back-upperioden.	Aanbestedende Dienst maakt gebruik van AvePoint als Back-up voorziening. Aanbestedende Dienst hanteert een duidelijk onderscheid tussen haar verplichtingen op basis van de Archiefwet en haar verplichtingen op basis van haar ISO27001 en BIO compliance. De back-up valt onder ISO27001, BIO en AVG die stellen dat de beschikbaarheid van informatie wordt geborgd (1 jaar) maar dat de persoonlijke data van medewerkers na 6 maanden dient te worden verwijderd. Kantoorautomatisering & Kantoor-back-up (MSP): 30 tot 90 dagen, Logbestanden (MSSP): 6 maanden tot 1 jaar. De zaken waar u naar vraagt betreffen technische configuratie, welke bij de Due Diligence overeen wordt gekomen. Indien dit bepland is voor uw inzending dan verzoeken wij u de vraag ind e tweede vragenronde te verduidelijken.
162	Eis 29	Kan GGN informatie verschaffen over het type cloudhosting, het aantal en type workloads, de hoeveelheid opslagcapaciteit en in gebruikzijnde opslagcapaciteit. Getroffen maatregelen op het gebied van veiligheid, beschikbaarheid en continuiteit. Kunnen wij ervanuit gaan dat wij volledige toegang krijgen tot de cloudhostingomgeving t.b.v. beeldvorming, inventarisatie, beheer en eventuele migraties?	Zie voor de specifieke zaken de specificaties in de andere vragen van deze Nota van Inlichtingen. Aanbestedende Dienst draagt zorg voor aanlevering iinformatie en toegang tot de omgevingen bij aanvang van de Due Diligence.
163	Eis 28	Kan GGN informatie verschaffen over het type internetverbindingen, bandbreedtes, SLA, etc.	Het leveren van de breedbandverbinding zelf hoort niet tot de opdracht. Momenteel maakt Aanbestedende Dienst gebruik van een bandbreedte van 1 Gbit
164	Eis 25	Mogen wij ervan uitgaan dat, indien er sprake is van overdracht vanuit een huidige partner, er volledige medewerking is door die partner.	Ja
165	Prijstabel	Voor de volgende onderdelen wordt een prijs per user gevraagd. •Kantoor Infrastructuur, Netwerkomgeving & Firewalls als managed service •Kantoor Internettoegang en Internetverbindingenals managed service •Kantoor Cloudhosting als managed service •Kantoor Back-up & Recovery als managed service •Beheer Fysieke Werkplekken van de medewerkers als managed service •Beheer Virtuele Werkplekken van de medewerkers als managed service •Beheer Printen & Reproductie als managed service •Beheer Vergadervoorzieningen als managed service Al deze onderdelen zijn echter niet user afhankelijk maar device, component of capaciteit afhankelijk. Bij een gelijkblijvend en stabiel aantal users is dit niet een grote uitdaging maar jullie geven zelf aan dat dit aantal flexibel zal en moet zijn. Om een prijs te kunnen invullen die transparant en conform gebruik is willen we vragen om de prijstabel hierop aan te passen?	Het Prijzenblad is tot stand gekomen op basis van onder andere de Marktconsultatie en analyse van de huidige kostenstructuren. Aanbestedende dienst verwacht op basis van het Prijzenblad daarom dat tarieven en bedragen door Inschrijver worden omgerekend naar de gevraagde posten.
166	Soll situatie	Voor de Soll situatie. In hoeverre wil GGD GHOR dat de backend data in een souvereine cloudomgeving staat? Dus in hoeverre moet er in de oplossing rekening gehouden worden met data-soevereiniteit waarbij de opgeslagen backend/server data alleen mag vallen onder de wetgeving van het land waar ze zich bevindt of waar ze is verzameld wat in dit geval Nederland is?	Aanbestedende Dienst is zich bewust van het feit dat het vrijwel onmogelijk is garanties voor Data Soevereiniteit te krijgen. Daarom is Eis10 opgenomen omdat Aanbestedende Dienst het belangrijk vind dat Opdrachtnemer in een situatie waarbij de Data Soevereiniteit in het geding komt, alles wat technisch, juridisch en/ of organisatorisch mogelijk is in het werk stelt om schending te voorkomen / vertragen/ aan te vechten.
167	Exit plan huidige MSP	Is er een exit clausule opgenomen met de huidige leverancier? Zo ja, kunnen jullie de afspraken beschrijven die met hun gemaakt zijn als de diensten overgenomen worden door een nieuwe MSP-er?	Voor iedere contractovereenkomst geldt dat de Exit-procedure wordt overeengekomen, dat geldt ook voor de huidige leveranciers. Samenvattend zijn deze gelijk aan de Exit-voorwaarden in de Concept Overeenkomst, Beschrijvend Document en Programma van Eisen van deze Aanbesteding. Leveranciers worden conform die bepalingen geacht mee te werken aan een professionele overdracht naar de nieuwe Leveranciers.
168	GIBIT 2023, artikel 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. 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 vi. 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?	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn. Aanbestedende Dienst heeft de noodzaak tot deze aanbesteding voldoende gemotiveerd, op basis waarvan u mag aannemen dat Aanbestedende Dienst alles in het werk zal stellen om de uitvoering van de te sluiten Overeenkomst te laten slagen.
169	GIBIT 2023, artikel 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?	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn. Aanbestedende Dienst heeft de noodzaak tot deze aanbesteding voldoende gemotiveerd, op basis waarvan u mag aannemen dat Aanbestedende Dienst alles in het werk zal stellen om de uitvoering van de te sluiten Overeenkomst te laten slagen.
170	GIBIT 2023, artikel 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…'?	Aanbestedende Dienst is van mening dat de gevraagde dienstverlening breed verkrijgbaar en in hoge mate gestandaardiseerd worden aangeboden. Met Garanties worden derhalve resultaatverplichtingen aangegaan, een inspanningsverplichting is hierbij onvoldoende.
171	GIBIT 2023 artikel 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 niet, bent u dan bereid akkoord te gaan met een ander plafondbedrag (anders dan de beperking per jaar)?	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn.
172	GIBIT 2023 artikel 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?	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn. Op basis van de eerdere Marktconsultatie heeft Aanbestedende Dienst begrepen dat de Gibit 2023 voorwaarden redelijk zijn, het schadebedrag is voor Aanbestedende Dienst bespreekbaar.
173	GIBIT 2023 artikel 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?	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn.

174	GIBIT 2023 artikel 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 10,000 EURO (ongeacht het aantal gebeurtenissen)?	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn.
175	GIBIT 2023 artikel 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)?	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn.
176	GIBIT 2023 artikel 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.	Niet akkoord.
177	GIBIT 2023 artikel 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.	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn.
178	MSP- en MSSP-diensten in één perceel	Geachte heer/mevrouw, In paragraaf 2.5 van het Beschrijvend Document geeft u aan waarom GGD GHOR Nederland ervoor kiest om MSP- en MSSP-diensten in één perceel onder te brengen. Graag verzoeken wij u om te verduidelijken of u bereid bent dit besluit te heroverwegen en de opdracht (gedeeltelijk) te verkavelen, of anders toe te lichten waarom dit niet wenselijk wordt geacht. Onze vraag is ingegeven door de internationaal erkende best practice dat beheertaken (MSP) en detectie-, monitoring- en securitytaken (MSSP/SOC/SIEM) functioneel gescheiden behoren te zijn. Deze scheiding draagt direct bij aan objectiviteit, controleerbaarheid en risicobeheersing. Kunt u aangeven of u openstaat voor het opdelen van de opdracht in twee afzonderlijke percelen, of anders kunt toelichten waarom dit binnen deze aanbesteding niet kan worden overwogen? Onderbouwing • Scheiding van functies Kaders zoals de BIO, NIS2 en ISO27001 benadrukken het belang van functiescheiding. Wanneer dezelfde leverancier zowel beheerwijzigingen uitvoert als incidentdetectie verzorgt, ontstaat een belangenconflict. • Objectieve monitoring en auditing Een SOC moet onafhankelijk kunnen beoordelen of wijzigingen en beheertaken correct en veilig zijn uitgevoerd. Bij één geïntegreerde leverancier vervalt deze onafhankelijke controlefunctie. • Risicobeheersing en incidentrespons Bij security-incidenten moet het SOC onderzoek kunnen doen naar beheeractiviteiten. Dit wordt aantoonbaar complexer wanneer dezelfde partij beide rollen vervult. • Vendor lock-in Het combineren van MSP en MSSP binnen één perceel vergroot het risico op lock-in. Voor overheidsaanbestedingen zijn marktwerking, transparantie en een werkbare exit-strategie essentieel. • Best practices binnen de publieke sector Bij organisaties in zorg, overheid en vitale infrastructuur wordt doorgaans een duidelijke organisatorische scheiding aangebracht tussen beheerpartijen en SOC-/monitoringtaken. Deze lijn wordt versterkt door de implementatie van NIS2. • Transparantie richting opdrachtgever Een gescheiden verantwoordingsstructuur zorgt voor meer inzicht in prestaties, incidenten en compliance, en versterkt de governance. Concrete vragen: Graag ontvangen wij uw reactie op de volgende punten:	Aanbestedende Dienst heeft de verdeling in percelen onderzocht en inhoudelijk gemotiveerd waarom is gekozen voor het NIET onderverdelen in percelen. Aanbestedende Dienst heeft gedurende de Covid-19 pandemie een groot aantal taken en voorzieningen verzorgd die op dat moment kritiek en nodig waren. Nu de Covid-19 pandemie ten einde is, stopt eveneens de financiering van overheidswege, hetgeen Aanbestedende Dienst noopt tot grote reducties van externe en interne medewerkers en het (verantwoord) afstoten/ overdragen/ uitfaseren van vrijwel al haar niet essentiële taken. Aanbestedende Dienst keert daarom in vorm en volume terug naar haar oorspronkelijke taken van voor de Covid-19 pandemie en behoudt uitsluitend een regierol voor de voorzieningen van haar leden (GGD'en en GHOR's). Zij gaat in feite terug naar een min of meer standaard mkb-organisatie. Door de aanbesteding niet in percelen te verdelen verwacht Aanbestedende Dienst ondanks haar geringe omvang toch voldoende interessant te zin voor MSP's en MSSP's Aanbestedende Dienst heeft tijdens de marktconsultatie vastgesteld dat er een aanzienlijk aantal partijen juist hebben geadviseerd de MSP en MSSP gezamenlijk aan te besteden zonder percelen. Aanbestedende dienst heeft ten aanzien van objectiviteit, controleerbaarheid en risicobeheersing eisen gesteld in het PvE
179	Beschrijvend document: Licenties	Kunt u specificeren welke Microsoft- en/of overige security-licenties momenteel aanwezig zijn binnen de bestaande SOC-dienstverlening, inclusief eventuele non-profit licentieconstructies?	MS Windows 11 MS Office 365 MS SharePoint MS Power BI MS Azure Virtual Desktop MS Sentinel: MS Defender for Threat Intelligence MS Office 365 MS Defender for Endpoint Azure Services Entra ID MS Entra ID Protection MS Defender for Business MS Defender for Cloud Apps MS Defender for Office 365 (o.a. Purview alerting DLP) MS Defender for Vulnerability Management Aanbestedende Dienst heeft de Non Profitstatus conform de voorwaarden van Microsoft.
180	Beschrijvend document: SOLL	Is het de expliciete wens dat de SOC-dienstverlening in de SOLL-situatie gebaseerd wordt op Microsoft-technologie? Of staat de MSSP vrij om, binnen de gestelde functionele vereisten, een best-of-breed oplossing aan te bieden?	Aanbestedende Dienst is volstrekt duidelijk dat op dit moment uitsluitend Microsoft-technologie wordt gehanteerd.
181	Beschrijvend document: IST	Kunt u een actuele architectuurplaat of -documentatie delen van de huidige SOC- en IT-omgeving, zodat duidelijk wordt welke componenten en verantwoordelijkheden door de MSSP moeten worden overgenomen?	Aanbestedende Dienst heeft bij de marktconsultatie een Bijlage Praatplaat gepubliceerd. Vanwege het vertrouwelijke karakter van de huidige SOC en IT-omgeving worden géén gedetailleerde architectuurplaten verstrekt en wordt het SOC SIEM uitsluitend functioneel gespecificeerd.
182	Beschrijvend document: G-SOC	Kunt u een uitgebreide beschrijving verstrekken van de taken, verantwoordelijkheden en positionering van het G-SOC, zodat helder wordt hoe de samenwerking en taakverdeling met de toekomstige MSSP vormgegeven moet worden?	Het G-SOC of Governance-SOC is naar verwachting de uitwerking van de Functionele Regie Organisatie in relatie tot het SOC/SIEM. Dit houdt in dat het G-SOC een regierol zal vervullen in de situatie dat de MSSP het SOC/SIEM volledig in beheer heeft overgenomen. In het G-SOC kunt u de rollen Product Owner, Service Level Manager, Privacy Officer, CISO Officer, Compliance & Audit Officer verwachten. Onderdeel van de implementatie zal zijn dat Aanbestedende Dienst in samenwerking met Opdrachtnemer een RASCI-matrix zal overeenkomen.
183	SLA MSP 3.1	Welke objectieve criteria worden gebruikt voor een 'Major Incident' (hoofdstuk 3.1) en hoe bepaalt GGD toerekenbaarheid bij ketenafhankelijkheden (GGD-netwerk of externe leveranciers)?	Zie hiervoor paragraaf 3.1: Prioriteitsniveaus P1 (hoog - werk ligt stil) t/m P4 (laag - geen hinder). Aanbestedende Dienst kent geen situaties waarbij er sprake zou zijn van genoemde ketenafhankelijkheid omdat de Managed Services bij 1 Opdrachtnemer worden ondergebracht middels deze aanbesteding en uitsluitend betrekking hebben op Aanbestedende Dienst en niet op haar leden.
184	SLA MSP 2.2	Kunt u bevestigen dat beschikbaarheidseisen alleen gelden voor componenten binnen MSP-scope, en dat downtime door GGD-services, externe SaaS-componenten of GGD-netwerk expliciet wordt uitgesloten van SLA-berekening?	Zie ook vraag 183 - Beachikbaarheidseisen MSOP hebben alleen betrekking op de MSP-scope.

185	Verwerkersovereenkomst art. 4.5	Kunt u bevestigen dat bij bezwaar tegen een nieuwe subverwerker GGD GHOR Nederland een alternatief scenario biedt zodat continuïteit en contractverplichtingen niet worden geraakt?	Bij het aangaan van de Overeenkomst tussen Aanbestedende Dienst en Opdrachtnemer wordt eveneens de (Sub)Verwerkersovereenkomst gezamenlijk ingevuld en ondertekend. Hierin is in Bijlage 3 ruimte om vooraf eventueel in te schakelen subverwerkers op te nemen. Indien Opdrachtnemer een subverwerker inschakelt die niet in Bijlage 3 is vermeld, dan behoudt Aanbestedende Dienst het recht hiertegen bezwaar te maken. Aanbestedende Dienst zal in dergelijke gevallen te allen tijde het bezwaar tegen deze subverwerker motiveren en Opdrachtnemer de gelegenheid geven een subverwerker in te schakelen op wie dit bezwaar niet van toepassing is.
186	Verwerkersovereenkomst art. 4.3	Kunt u aangeven welke objectieve criteria GGD GHOR hanteert om verwerking buiten de EER te beoordelen, en of SCC's of andere waarborgen onder voorwaarden wel/niet worden aanvaard?	Het feit dat enige verwerking aantoonbaar buiten de EER geschiedt is voldoende aanleiding voor Aanbestedende Dienst om verwerking buiten de EER te beoordelen. Opdrachtnemer dient verwerking buiten de EER te allen tijde vooraf te melden aan Aanbestende Dienst. De criteria die Aanbestedende Dienst hierbij hanteert zijn afhankelijk waar buiten de EER die verwerking zal plaatsvinden en welke risico's dat met zich meebrengt. Zo zal verwerking in bijvoorbeeld de VK of Zwitserland (naar verwachting) minder risicovol zijn dan verwerking in bijvoorbeeld Wit-Rsuland of Oekraine.
187	Verwerkersovereenkomst 4.1	Kunt u bevestigen dat de invulling van 'passende technische en organisatorische maatregelen' uit Bijlage C, art. 4.1 gezamenlijk wordt vastgesteld en dat GGD GHOR Nederland vooraf instemming geeft op de door Opdrachtnemer voorgestelde maatregelen, inclusief wijzigingsproces?	Bij het aangaan van de Overeenkomst tussen Aanbestedende Dienst en Opdrachtnemer wordt eveneens de (Sub)Verwerkersovereenkomst gezamenlijk ingevuld en ondertekend. Hierin is in Bijlage 2 ruimte om vooraf de passende technische en organisatorische maatregelen vast te leggen en overeen te komen, inclusief wijzigingsproces.
188	Beschrijvend document par,. 2.1. blz 15 en kostenoverzicht	U vraagt om een fee per gebruiker per maand voor beheer in samenwerking met ServiceDesk GGN. Kunt u specifieker aangeven waar deze samenwerking uit dient te bestaan. Bijvoorbeeld leveren personeel, verwerken van bepaald aantal tickets, urenbesteding hiervoor per maand ?	Ten tijde van de Inbeheername zal de eigen Servicedesk van Aanbestedende Dienst nog volledig de eerste lijns support verzorgen. De verwachting is dat dit na Inbeheername (na 1 jaar) per managed service onderdeel aan de MSP zal worden uitgefaseerd.
189	Beschrijvend document par,. 2.1. blz 15 en kostenoverzicht Het opstellen van een backlog voor managed services.	A) Hoeveel uur verwacht u dat er nodig is om deze backlog uit te werken? B) Hoeveel backlog items verwacht u?	Zowel voor de MSP alsook de MSSP geldt dat de Implementatie (Inbeheername) een gezamenlijke inspanning zal zijn tussen Aanbestedende Dienst en Opdrachtnemer conform het Implementatieplan (G1) van Opdrachtnemer. Aanbestedende Dienst gaat er van uit dat bij de Implementatie / Inbeheername van zowel MSP alsook de MSSP punten worden geidentificeerd die betrekking hebben op de (door)ontwikkeling en/ of verbetering van de voorzieningen en diensten teneinde de doelstellingen van Aanbestedende Dienst te behalen, dan wel de ICT-prestaties / managed services van Opdrachtnemer efficienter, effectiever of makkelijker uitvoerbaar te maken. Deze punten worden doorlopend geregistreerd in de Backlog MSP en Backlog MSSP, besproken en na wederzijdse beoordeling en begroting doorgevoerd. Aanbestedende dienst beschouwt het gezamenlijk opstellen van de Backlog als onderdeel van de dienstverlening (implementatie/ inbeheername) en kan geen concrete uitspraken doen over het aantal backlog items. Wel is het zo dat de realisatie van de backlog-items waar het changes betreft ten opzichte van de bestaande situatie, altijd vooraf wordt gegaan door een begroting door Opdrachtnemer tegen de tarieven die u in het Prijzenblad opneemt.
190	Beschrijvend document par,. 2.1. blz 15 en kostenoverzicht Beheer Kantoor Infrastructuur, Netwerkomgeving & Firewalls	A) Welke netwerk throughput is nodig voor deze firewall(s) op basis van IDS verkeerinspectie? B) Kunt u een beschrijving geven van de huidige kantoor infrastructuur en netwerkomgeving en modellen/ typen, beschrijvingen van de netwerkdevices die beheerd moeten worden?	E-mail, tekstverwerking e.d. - 5 Mbps Web-browsing, SaaS-applicaties)5 - 10 Mbps Videobellen, grote bestanden, VDI)15 - 25 Mbps. Voor de specificaties zie antwoorden in deze Nota van Inlichtingen.
191	Beschrijvend document par,. 2.1. blz 17	U meldt dat de levering van VPN verbindingen buiten scope zijn. A) Betekent dit dat de firewall dienst die geleverd wordt niet gebruikt gaat worden om de VPN verbindingen op te termineren? B) Kunt u toelichten hoe u de VPN verbindingen wilt gaan ondersteunen qua netwerkinfrastructuur?	A. Correct B. De VPN verbindingen worden uitsluitend gebruikt door medewerkers die zich niet op de kantoorlocatie van Aanbestedende Dienst bevinden
192	Beschrijvend document blz 50 Beoordelingskader prijs	In het rekenvoorbeeld berekent u dat de afstand tussen de onder en bovengrens 1.470.000 is. Inschrijver komt uit op (3.300.000 – 1.850.000) 1.450.000. Kunt u het verschil verklaren?	Aanbestedende Dienst heeft hier een rekenfout gemaakt, het afstandsbedrag is inderdaad 1.450.000
193	Beschrijvend document, blz 48 Licentiekosten (kosten programmatuur en/ of applicatiesoftware) Managed Security Services	U geeft aan dat de licenties eeuwigdurend moeten zijn. In het programma van eisen meldt u dat alle gebruikte software van Microsoft afkomstig moet zijn. A) Mag Inschrijver voor SOC SIEM diensten gebruik maken van software die niet van Microsoft afkomstig is? B) Kunt u de eis dat de licenties eeuwigdurend zijn laten vervallen? In het geval van Microsoft SOC SIEM maar ook van andere SOC SIEM applicaties is een eeuwigdurende licentie niet mogelijk.	A. Zie voor de SOC SIEM specificaties de antwoorden in deze Nota van Inlichtingen. het enige niet-Microsoft product voor SOC/SIEM is Splunk. B. Aanbestedende Dienst bedoelt met 'eeuwigdurend' dat deze licenties / gebruiksrechten geen vast bepaalde looptijd hebben. Deze licenties lopen al en blijven lopen ook na aflopen van de Overeenkomst.
194	Programma van eisen punt 12	Wat bedoelt u met Microsoft compatibele producten?	Dit betreft producten die door Microsoft zelf worden geleverd alsook producten die door derden worden geleverd en die aantoonbaar technisch, functioneel en soms ook formeel gecertificeerd zijn om zonder problemen binnen een Microsoft-omgeving te functioneren. Concreet betekent dit dat ze tenminste werken met het Windows besturingssysteem en Micrososft protocollen (bijv. Active Directury, Azure AD, SMB) en API's (Ms Exchange, Azure API's., .NET) ondersteunen. De producten mogen voorts geen conflicten veroorzaken en Updates van Microsoft niet verstoren of blokkeren.
195	Programma van eisen punt 28	Kunt u specifiek beschrijven welke netwerkverbindingen en internetverbindingen u op dit moment gebruikt en met welke bandbreedtes?	Het leveren van de breedbandverbinding zelf hoort niet tot de opdracht. Momenteel maakt Aanbestedende Dienst gebruik van een bandbreedte van 1 Gbit
196	Programma van eisen punt 29	A) Wat verstaat u onder kantoor Cloud hosting? B) Van welke technologie maakt u gebruik voor uw virtuele werkplekken?	Aanbestedende Dienst verstaat onder Kantoor Cloudhosting: Het geheel van managed Cloudhosting voor de volgende domeinen: Productiviteit en samenwerking: Exchange online, Ms Office 365, Teams, Teams Manager, SharePoint Bestandsopslag: Persoonlijke en gedeelde OneDrives, SharePoint Bibliotheken en Azure Files, Back-up en Archivering Werkplekbeheer en Beveiliging: Ms Entra ID, Intune (Endpoint Manager) en security tools (Defender e.d.) Virtual Desktop Infrastructuur (VDI) voor Azure Virtual Desktop (AVD) en Windows 365
197	Programma van eisen punt 30 en prijzenblad	Moet Inschrijver de kosten per medewerker aangeven voor het beheer van de huidige oplossing die u zelf inkoopt of moet de inschrijver hiervoor ook een dienst leveren en de kosten van deze dienst opnemen in het prijzenblad?	Aanbestedende Dienst maakt gebruik van AvePoint en heeft deze eerder zelf ingekocht. Deze Back-up-voorziening moet in beheer worden genomen door Inschrijver en daarom opgegeven worden in het Prijzenblad

198	Prijzenblad Licentiekosten managed services, CSP management, beheer en optimalisatie	A) Kunt u aangeven welke Microsoft licenties en de hoeveelheden die u op dit moment afneemt? B) Moet inschrijver de kosten van de Microsoft licenties ingeven in het prijzenblad of alleen het beheer van deze licenties ten behoeve van GGN? C) Kunt u bevestigen dat in deze post geen Azure licenties dienen te worden vermeld?	A. Exchange Online Plan 1 - 18 licenties Ms-365 Audio Conferencing - 9 licenties Ms-365 E3 - 325 licenties Ms-365 E5 - 1 licentie Office 365 E1 - 30 licenties Ms-Defender Suite - 325 licenties Power BI - Pr - 22 licenties Visio Plan 2 - 40 licenties Windows 365 Enterprise 4 vCPU, 16 Gb, 128 Gb - 2 licenties B: Beide - daartoe is voorzien in het prijzenblad C: De Azure licenties (bijvoorbeeld voor Kantoor Cloudhosting) dient u om te rekenen naar de gevraagde posten.
199	SLA MSSP 9.3	Indien kritieke patches niet binnen 24 uur beschikbaar zijn of incompatibel blijken, kan de MSSP deze termijnen dan opschuiven mits goed onderbouwd en afgestemd?	Ja.
200	SLA MSSP 2.1 / 2.2	Gelden de 24/7-responsnormen ook wanneer incidenten veroorzaakt worden door externe SaaS-providers of het GGD-netwerk, en hoe wordt dit meegenomen in SLA-rapportages?	Ja, de oorzaak van een incident is doorgaans niet bij voorbaat duidelijk. Ook deze incidenten waarvan wordt vastgesteld dat deze bij externe leveranciers of het netwerk worden veroorzaakt moeten in de SLA / Incident-rapportages worden meegenomen.
201	SLA MSP 5.5	Hoe wordt omgegaan met patches die volgens vendor urgent zijn, maar functioneel risicovol zijn volgens MSP (hoofdstuk 5.5)? Is uitstel mogelijk mits gemotiveerd en akkoord van Opdrachtgever?	Ja.
202	SLA MSP 5 / 5.1	Waar worden wijzigingen geregistreerd? Alleen in ServiceNow of ook ergens anders?	In ServiceNow van Aanbestedende Dienst en/ of in het ITSM van Opdrachtnemer dat met ServiceNow van Aanbestedende Dienst is gekoppeld
203	Programma van eisen 24 tm 50	Opdrachtgever vereist bij start van de opdracht een 'as is'-overname van de bestaande dienstverlening, en stelt daar vanaf de start performance/SLA-eisen (bijlage J Concept SLA-MSP) aan. Is opdrachtgever akkoord met een 'best effort' benadering gedurende de due dilligence en implementatiefase, waarbij wordt gestreefd naar voldoen aan de SLA?	Het spreekt voor zich bij Aanbestedende Dienst dat de Service Levels pas geldig zijn nadat Due Diligence en Implementatie hebben plaatsgevonden en de Implementatie formeel is geaccepteerd. Zie ook Concept Overeenkomst.
204	Programma van eisen 13	GGN heeft (terecht) een strak AI-beleid. Om vast te stellen of gecontroleerde toepassing van AI, binnen de services van aanbieder, binnen dat beleid valt ontvangen wij graag het betreffende beleidsdocument. Dit is een factor die een rol speelt in de te hanteren pricing.	Aanbestedende dienst is zich bewust van- en maakt reeds gebruik van- de in Microsoftproducten geïntegreerde AI-functionaliteiten. Aanbestedende dienst wenst daarom Eis 13 als volgt aan te passen: Opdrachtnemer garandeert dat voor de levering van managed services en managed security services, geen gebruik gemaakt zal worden van Kunstmatige Intelligentie (AI), Large Language Models e.d. behoudens de reeds in Microsoftproducten aanwezige AI-functionaliteiten, tenzij dit in overleg met Opdrachtgever schriftelijk anders is overeengekomen en vooraf is getoetst aan het GGN AI-beleid en door het CISO-office. Het beleidsdocument kan in deze fase (nog) niet gedeeld worden.
205	Beschrijvend document EA Par 6.8, pag 43 en 45	Bij de vormvereisten in het kader van Kansendossiers G3 en G4 worden twee getallen genoemd voor het maximale aantal pagina's voor de beantwoording. Welke is leidend?	Het maximum aantal pagina's bedraagt 10 (tien)
206	Beschrijvend document EA 1.1.2 Huidige Situatie, pag 9	De IST situatie is vrij compact beschreven. Voor een goede inschatting van de benodigde transformatie-werkzaamheden en bijbehorende kosten is meer gedetailleerde informatie nodig over de huidige inrichting. Het gaat hierbij om zowel de huidige inrichting van de basis IV / ICT-voorzieningen als die van de SOC-SIEM inrichting. Een lijst van gebruikte producten/services met korte aanduiding van de toepassing daarvan is van belang om tot een betere beeldvorming te komen.	Zie voor het antwoord vergelijkbare vragen in deze Nota van Inlichtingen.
207	GIBIT	Zijn gewenste afwijkingen op de GIBIT 2023 bespreekbaar in de verificatiefase?	Indien er gewenste afwijkingen zijn ten aanzien van de GIBIT dan kunt u hierover vragen stellen in deze of de volgende vragenronde - Nota van Inlichtingen. Tijdens de Verificatiefase worden de Geschiktheidseisen gecontroleerd, er is dan geen onderhandelingsruimte over de GIBIT-voorwaarden. Indien er op basis van deze en volgende vragenronde - Nota van Inlichtingen ruimte wordt geboden voor afwijkingen aan de GIBIT dan worden deze afwijkingen ná definitieve gunning in de 'contractfase' (overleg en ondertekening) besproken en vastgelegd. Nota bene dat in de Markstconsultatie het merendeel van de deelnemers heeft aangegeven geen probleem te hebben bij de toepassing van de GIBIT-voorwaarden
208	PvE (Service management)	Is er een actuele en betrouwbare CMDB beschikbaar die gebruikt kan worden bij de transitie?	Ja
209	PvE (Service management)	Dient opdrachtnemer volledig in de ServiceNow-omgeving van opdrachtgever te werken, of is een integratie met een eigen ITSM-tool toegestaan mits volledig gekoppeld?	Conform de Eis zijn beide toegestaan.
210	Gunningscriteria (G3 en G4)	Worden de kansendossiers (Cloudhosting en Data Intelligence) op verzoek gerealiseerd gedurende de overeenkomst of wordt dit vastgesteld in de verificatiefase?	Aanbestedende Dienst beoogt als eerste de MSP en MSSP te implementeren. Aanvullend daarop zal Aanbestedende Dienst in overleg met Opdrachtnemer kijken naar de noodzaak/ wens/ mogelijkheid om de kansen uit het Kansendossier MDISP en Managed Cloudhosting gedurende de geldigheid van de overeenkomst te realiseren. Dit staat los van de Verificatiefase. De Verificatiefase dient uitsluitend om de bewijsvoering van de geschiktheidseisen te bespreken.
211	Beschrijvend Document EA procedure MSP MSSP v1.0	Zijn er onderdelen binnen de huidige dienstverlening waarvan reeds is besloten dat deze binnen de eerste contractperiode zullen worden uitgefaseerd?	Nee, het Programma van Eisen is gebaseerd op de huidige dienstverlening die door een groot aantal losse leveranciers wordt geleverd en waarvan Aanbestedende Dienst beoogt deze bij één Opdrachtnemer onder te brengen. De huidige dienstverlening wordt door Aanbestedende Dienst beschouwd als ' Basis IV/ICT-voorzieningen' zonder welke zij niet kan functioneren. Er is in die zin geen sprake van uitfasering. Wel zal het zo zijn dat de volumes van de dienstverlening zullen afnemen.
212	PVE Bijlage A	Wat wordt exact bedoeld met “as-is” overname bij de MSSP-dienstverlening: betreft dit uitsluitend tooling/licenties of ook bestaande use cases, playbooks, detectieregels en SOC-processen?	Dit betreft zowel de tooling/ licenties alsook de bestaande use cases, playbooks, detectieregels en gelidelijk ook de SOC-processen.

213	Hoofdstuk 1.4 / Opdrachtomschrijving	Kan opdrachtgever een actueel overzicht van de huidige MSP- en MSSP-architectuur (tooling, versies, integraties) delen, zodat de implementatie- en beheerinspanning correct kan worden ingeschat?	Aanbestedende Dienst maakt uitsluitend gebruik van mainstream Commercial Of The Shelf producten/ devices. Zie ook de overige antwoorden in deze Nota van Inlichtingen. MS Windows 11 MS Office 365 MS SharePoint MS Power BI MS Azure Virtual Desktop MS Sentinel: MS Defender for Threat Intelligence MS Office 365 MS Defender for Endpoint Azure Services Entra ID MS Entra ID Protection MS Defender for Business MS Defender for Cloud Apps MS Defender for Office 365 (o.a. Purview alerting DLP) MS Defender for Vulnerability Management Splunk Aanbestedende Dienst heeft de Non Profitstatus conform de voorwaarden van Microsoft. Firewall: Fortigate Switches: Fortigate en Unifi AP's: Unifi Alle niet-Microsoft licenties lopen te allen tijde via de Softwarebroker SoftwareOne.
214	Bijlage A - Programma van Eisen MSP en MSSP Eis 84	Kunt u aangeven of deze eis betekent dat sprake moet zijn van continue 24/7 actieve monitoring (“eyes-on-screen”), of dat ook een 24/7 beschikbaarheidsmodel met standby/on-call dienstverlening wordt geaccepteerd, mits de overeengekomen responstijden en SLA’s worden geborgd?	De overeengekomen responstijden en SLA's dienen te allen tijden te worden gehaald, de methodiek is bespreekbaar.
215	Beschrijvend document EA procedure MSP MSSP v1.0	Ten behoeve van een realistische inschatting van de omvang van de Managed Security Services / MDR-dienstverlening, verzoekt Inschrijver Opdrachtgever aan te geven of er een indicatief beeld kan worden gegeven van het historische of verwachte aantal security-incidenten, uitgesplitst naar prioriteit (P1, P2, P3, P4).	Nee, historische data zijn vertrouwelijk en gezien de grote veranderopgave (BD) waar Aanbestedende Dienst voor staat kan geen betrouwbare prognose worden gegeven voor toekomstoge incidenten.
216	Beschrijvend document EA procedure MSP MSSP v1.0	Kunt u een beeld geven van de huidige licentiekosten in de IST situatie?	Uit concurrentie-oogpunt worden geen tarieven verstrekt die door de huidige leveranciers in rekening worden gebracht.
217	Bijlage A - Programma van Eisen MSP en MSSP Eis 13	Kan Opdrachtgever verduidelijken hoe deze eis moet worden geïnterpreteerd in situaties waarin onderliggende (SaaS-)diensten of platformen van derde leveranciers, zoals bijvoorbeeld Microsoft, standaard gebruikmaken van AI-functionaliteit (bijvoorbeeld binnen security-, cloud- of productivity-diensten), zonder dat Opdrachtnemer hier directe invloed op heeft of deze expliciet activeert?	Aanbestedende dienst is zich bewust van- en maakt reeds gebruik van- de in Microsoftproducten geïntegreerde AI-functionaliteiten. Aanbestedende dienst wenst daarom Eis 13 als volgt aan te passen: Opdrachtnemer garandeert dat voor de levering van managed services en managed security services, geen gebruik gemaakt zal worden van Kunstmatige Intelligentie (AI), Large Language Models e.d. behoudens de reeds in Microsoftproducten aanwezige AI-functionaliteiten, tenzij dit in overleg met Opdrachtgever schriftelijk anders is overeengekomen en vooraf is getoetst aan het GGN AI-beleid en door het CISO-office.
218	Bijlage O, Prijzenblad	Kan Opdrachtgever verduidelijken of het is toegestaan (of gewenst) om aanvullende security-specialistische rollen, zoals bijvoorbeeld pentesters of andere specialistische security consultants, op te nemen in het prijzenblad, zodat deze – indien benodigd binnen de scope van de dienstverlening – transparant en vooraf geprijsd kunnen worden aangeboden?	De indeling van het Prijzenblad mag niet worden gewijzigd, er mogen geen rijen aan worden toegevoegd. Inschrijver wordt geacht tarieven in te vullen op basis van junior - medior - senior. Indien er buiten de scope van de MSSP-dienstverlening aanvullende expertises nodig zijn dan worden deze via een andere procedure ingehuurd.
219	Bijlage A - Programma van Eisen MSP en MSSP Eis 45	Kunt u voor de dienst "GGN-eigen voorzieningen voor Printen en Reproductie" details worden aangeleverd? Wat zijn de producten en beheertooling die hiervoor gebruikt worden?	Aanbestedende Dienst maakt op dit moment gebruik van print devices van Veenman en Printix voor secure Cloud Print Management. De verwachting ten aanzien van de Inschrijver is dat deze de printvoorzieningen as-is in beheer overneemt waarna wij de overeenkomst met de huidige leverancier kunnen beëindigen en vanaf dat moment zowel de devices als het Cloud Print Management als dienst afnemen van Opdrachtnemer.
220	Bijlage A - Programma van Eisen MSP en MSSP Eis 40	Voor het binnen 48 uur opschalen van de virtuele werkplekomgeving is de vraag of voor deze eis al een configuratie aanwezig is, of moeten we deze configuratie na het in beheer nemen van de omgeving zelf realiseren?	Het uitleveren van virtuele werkplekken staat in Eis 41 niet in 40 en betreft extra virtuele werkplekken die identiek zij aan de configuratie van de reguliere virtuele werkplekken.
221	Bijlage A - Programma van Eisen MSP en MSSP Eis 26 t/m 30	Kunnen er voor de in beheer te nemen diensten details worden aangeleverd? welke producten worden er gebruikt voor de diensten benoemd in de PVE?	Zeker, zie de antwoorden op vergelijkbare vragen in deze Nota van Inlichtingen.
222	Verlenging Overeenkomst	In artikel 2.3 van de Overeenkomst krijgt de Opdrachtgever de mogelijkheid de Overeenkomst maximaal twaalf jaar te laten doorlopen onder ongewijzigde voorwaarden. Voor de Opdrachtnemer kan dit bezwaarlijk zijn, omdat technologische ontwikkelingen, markt- en prijsontwikkelingen en overige ontwikkelingen over een termijn van twaalf jaar niet te overzien zijn. Een verplichting om een verlenging altijd onder gelijke voorwaarden te accepteren kan daardoor tot disproportionele risico’s leiden. Wij verzoeken daarom om opname van de volgende aanvullende bepaling: “Indien Opdrachtnemer van mening is dat een (verdere) verlenging onder ongewijzigde voorwaarden voor hem ernstige nadelige gevolgen heeft, kan hij dit - voor het eerst na verloop van 6 jaren - tot uiterlijk twaalf (12) maanden vóór afloop van de in artikel 2.3 bedoelde (verlengde) contractperiode schriftelijk en gemotiveerd kenbaar maken, in welk geval geen (verdere) verlenging zal plaatsvinden.”	Gevraagd wordt naar een serie van standaard diensten door een MSP en MSSP. Ongewijzigde voorwaarden hebben met name betrekking op de GIBIT2023. Technologische ontwikkelingen die binnen de Overeenkomst vallen kunnen worden geagendeerd in de MSP Backlog en/ of de MSSP Backlog. Prijsontwikkelingen zullen veelal via de CSP verlopen voor de Microsoftproducten en worden door MSP doorberekend aan Aanbestedende Dienst. Aanbestedende Dienst heeft de theoretische mogelijkheden tot verlenging opgenomen met dien verstande dat er een goede werkrelatie wordt ontwikkeld met Opdrachtnemer. Er ligt een verantwoordelijkheid bij zowel Aanbestedende Dienst alsook bij Opdrachtnemer om binnen de overeengekomen kaders en Overeenkomst tijdig aan te geven wanneer de samenwerking voor 1 of beide partijen nadelige gevolgen heeft.

223	Beschrijvend document EA procedure MSP MSSP v1.0 par 2.6	Ten behoeve van een realistische inschatting van de omvang van de Managed Security Services / SOC-dienstverlening, verzoekt Inschrijver Opdrachtgever aan te geven of er een indicatief overzicht kan worden gegeven van het aantal logbronnen dat momenteel is aangesloten op het SOC/SIEM. Hierbij kan bijvoorbeeld worden gedacht aan een globale verdeling naar type bron (bijv. werkplekken, servers, netwerkcomponenten, cloud- en/of SaaS-applicaties).	Sentinel: MS Defender for Threat Intelligence MS Office 365 MS Defender for Endpoint Azure Services Entra ID MS Entra ID Protection MS Defender for Business MS Defender for Cloud Apps MS Defender for Office 365 (o.a. Purview alerting DLP) MS Defender for Vulnerability Management Firewall syslog van HPZone omgeving Keeper SPLUNK: Delta Gateway (iMPeX en HPV18+) TOPdesk SOC SPLUNK via Logbuffet: HPZone GraphQL CoronIT iTBC iTBC IMS EVS Cluster TBC EVS Cluster SG (25 keer) PGA Registratieschil
224	Bijlage G. Geheimhoudingsverklaring	Aanbieder werkt met een geheimhoudingsverklaring die op organisatieniveau met Opdrachtgever wordt aangegaan. Deze overeenkomst is door aanbieder richting medewerkers afgedekt als onderdeel van de arbeidsvoorwaarden. Is dat voor Opdrachtgever acceptabel en vervalt deze bijlage daarmee?	U dient er vanuit te gaan dat de Geheimhoudingsverklaring van Aanbestedende Dienst leidend is.
225	Bijlage A - Programma van Eisen MSP en MSSP Eis 83	Ten behoeve van een goed begrip van de huidige situatie (IST) rondom Managed Security Services, verzoekt Inschrijver Opdrachtgever toe te lichten hoe vulnerability management momenteel is ingericht. Kan Opdrachtgever aangeven: welke tooling momenteel wordt gebruikt voor vulnerability scanning; welke onderdelen in scope zijn (bijv. werkplekken, servers, netwerk, cloud/SaaS); en in welke mate opvolging en prioritering van kwetsbaarheden momenteel plaatsvindt?	Sentinel: MS Defender for Threat Intelligence MS Office 365 MS Defender for Endpoint Azure Services Entra ID MS Entra ID Protection MS Defender for Business MS Defender for Cloud Apps MS Defender for Office 365 (o.a. Purview alerting DLP) MS Defender for Vulnerability Management Firewall syslog van HPZone omgeving Keeper SPLUNK: Delta Gateway (iMPeX en HPV18+) TOPdesk SOC SPLUNK via Logbuffet: HPZone GraphQL CoronIT iTBC iTBC IMS EVS Cluster TBC EVS Cluster SG (25 keer) PGA Registratieschil
226	Bijlage A PVE eis 45	Wij lezen hier het volgende: Opdrachtnemer neemt de GGN-eigen voorzieningen voor Printen en Reproductie as-is als Managed Service in beheer en verzorgt gedurende de overeenkomst de verdere optimalisatie van de Print- en Reproductievoorzieningen in termen van gebruik, kosten, veiligheid, beschikbaarheid en continuïteit op basis van de nader overeen te komen Backlog Managed Services. Vraag: kan een overzicht worden gegeven (CMDB) van de Print- en Reproductie apparatuur?	Aanbestedende Dienst maakt op dit moment gebruik van print devices van Veenman en Printix voor secure Cloud Print Management. De verwachting ten aanzien van de Inschrijver is dat deze de printvoorzieningen as-is in beheer overneemt waarna wij de overeenkomst met de huidige leverancier kunnen beëindigen en vanaf dat moment zowel de devices als het Cloud Print Management als dienst afnemen van Opdrachtnemer.
227	Bijlage A PVE eis 27	Wij lezen hier het volgende: Opdrachtnemer neemt de GGN-eigen voorzieningen voor Kantoorinfrastructuur, Netwerkomgeving en Firewalls as-is als Managed Services in beheer en verzorgt gedurende de overeenkomst de verdere optimalisatie van de Kantoorinfrastructuur, Netwerkomgeving en Firewalls in termen van gebruik, kosten, veiligheid, beschikbaarheid en continuïteit op basis van de nader overeen te komen Backlog Managed Services. Vraag: kan een CMDB lijst worden aangeleverd van alle netwerkapparatuur welke as-is in beheer genomen moet worden?	Ja, bij de Due Diligence - zie voor de specificaties de antwooden in deze Notra van Inlichtingen
228	Bijlage A PVE eis 47	U geeft aan dat Opdrachtnemer de GGN-eigen Zakelijke Telecommunicatievoorzieningen as-is als Managed Service in beheer neemt, en gedurende de overeenkomst de verdere optimalisatie verzorgt van de Zakelijke telecommunicatievoorzieningen in termen van gebruik, kosten, veiligheid, beschikbaarheid en continuïteit op basis van de nader overeen te komen Backlog Managed Services. Om hier goed invulling aan te kunnen geven hebben we wat meer informatie nodig over uw huidige Telecommunicatievoorzieningen wilt u ons hierin voorzien: - welke provider levert u momenteel telefonie diensten? - van welke telefonie oplossingen maakt u gebruik waar wij rekening mee moeten houden?	De huidige provider van Zakelijke Telecom is Odido, er wordt gebruik gemaakt van Odido Hosted Voice en Odiudo Virtuele Telefooncentrale. Odido levert tevens circa 100 mobiele abonnementen.

229	BD algemeen / Bijlage 0 - Prijzenblad	Geïnteresseerde ervaart wat betreft alle as is in beheer te nemen onderdelen een gebrek aan informatie. Behalve de specificatie van aantallen worden er in de stukken hoegenaamd geen details gedeeld. Gaat de aanbestedende dienst er van uit dat alle onderdelen van de gevraagde Managed Services door Geïnteresseerden beprijsd kunnen worden, zowel voor het as is in beheer nemen als het als managed service beheren, zonder specifieke informatie over de zaken die in gebruik zijn? Zo niet, welke aannames heeft u dan over hoe Geïnteresseerden hun prijsopgave bepalen?	Aanbestedende Dienst maakt uitsluitend gebruik van mainstream Commercial Of The Shelf producten/ devices. Zie ook de overige antwoorden in deze Nota van Inlichtingen. MS Windows 11 MS Office 365 MS SharePoint MS Power BI MS Azure Virtual Desktop MS Sentinel: MS Defender for Threat Intelligence MS Office 365 MS Defender for Endpoint Azure Services Entra ID MS Entra ID Protection MS Defender for Business MS Defender for Cloud Apps MS Defender for Office 365 (o.a. Purview alerting DLP) MS Defender for Vulnerability Management Splunk Aanbestedende Dienst heeft de Non Profitstatus conform de voorwaarden van Microsoft. Firewall: Fortigate Switches: Fortigate en Unifi AP's: Unifi
230	BD 2.1	Kunt u aangeven welke oplossing in gebruik is wat betreft Zakelijke Telefonie?	De huidige provider van Zakelijke Telecom is Odido, er wordt gebruik gemaakt van Odido Hosted Voice en Odiudo Virtuele Telefooncentrale. Odido levert tevens circa 100 mobiele abonnementen.
231	BD 2.1	Kunt u de fabrikant benoemen van de in gebruik zijnde netwerkapparatuur, specifiek wat betreft de Switches, de Firewall en de Wifi componenten?	Aanbestedende Dienst maakt uitsluitend gebruik van mainstream Commercial Of The Shelf producten/ devices. Zie ook de overige antwoorden in deze Nota van Inlichtingen. MS Windows 11 MS Office 365 MS SharePoint MS Power BI MS Azure Virtual Desktop MS Sentinel: MS Defender for Threat Intelligence MS Office 365 MS Defender for Endpoint Azure Services Entra ID MS Entra ID Protection MS Defender for Business MS Defender for Cloud Apps MS Defender for Office 365 (o.a. Purview alerting DLP) MS Defender for Vulnerability Management Splunk Aanbestedende Dienst heeft de Non Profitstatus conform de voorwaarden van Microsoft. Firewall: Fortigate Switches: Fortigate en Unifi AP's: Unifi
232	BD 2.1	Kunt u aangeven welke printer oplossing(en) op dit moment bij u in gebruik zijn cq welke partij de leverancier is van de apparatuur ?	Aanbestedende Dienst maakt op dit moment gebruik van print devices van Veenman en Printix voor secure Cloud Print Management. De verwachting ten aanzien van de Inschrijver is dat deze de printvoorzieningen as-is in beheer overneemt waarna wij de overeenkomst met de huidige leverancier kunnen beëindigen en vanaf dat moment zowel de devices als het Cloud Print Management als dienst afnemen van Opdrachtnemer.
233	BD 2.9.1	Er wordt verwezen naar beschrijvingen van de optionele dienstverlening in paragraaf 1.1 en 2.1. Geïnteresseerde ziet deze beschrijvingen daar niet terug. Kunt u aangeven waar hier precies naar wordt verwezen?	Dit betreft optionele dienstverlening Managed Data Intelligence Services en Managed Cloudhosting. Onder Applicaties, Infra en Cloud vindt u de IST en SOLL
234	BD 2.11	Dit onderdeel geeft aan dat de bijagen J en K de SLA concepten zijn die als basis "dienen te worden gebruikt" voor de uiteindelijk te ondertekenen SLA's. Tegelijkertijd wordt Geïnteresseerde onder Gunningscriterium G2 gevraagd om twee (eigen) concept SLA's bij te voegen. Kunt u aangeven hoe beide zaken zich tot elkaar verhouden en daarbij specifiek aangeven op welke wijze de eigen SLA van geïnteresseerde nog een basis kan zin voor de uiteindelijk te ondertekenen SLA's?	U dient gebruik te maken van de concept documenten zoals deze zijn begevoegd bij de aanbestedingsdocumenten. Deze documenten kunt u verder uitwerken met uw eigen input.
235	BD 3.9	Deze paragraaf beschrijft dat in de verificatiefase op functioneel niveau een viertal verificatiegesprekken gevoerd zal worden waarbij elke materiedeskundige (GGD GHOR) functionaris die voorlopige gunning dient te onderschrijven. Geïnteresseerde verwacht, gezien de mogelijke consequentie van terzijde legging, dat het eventueel niet onderschrijven van de voolopige gunning door een functionaris is op een juridisch heldere, houdbare, objectieve en daardoor aanvechtbare wijze onderbouwd wordt. Dit lezen we in de aangehaalde tekst niet terug. Verder in deze paragraaf wordt ingegaan op de mogelijke uitsluitingsgronden die uit de verificatiegesprekken kunnen voortkomen. Naar de inschatting van geïnteresseerde betreffen de eerste vier bullets objectief vast te stellen gronden. Alleen de onderste bullet, het "niet gaan voldoen aan het PvE" is als mogelijke uitsluitingsgrond niet bijvoorbaat te objectiveren. Kunt u aangeven of u begrijpt dat geinteresseerde het voorgaande aanhaalt omdat de basis voor het eventueel intrekken van een voorlopige gunning als gevolg van de gevoerde verificatiegesprekken onvoldoende objectief is gespecificeerd, en daarbij aangeven dat alleen objectief houdbare en verifieerbare bezwaren van de betreffende materiedeskundigen een reden kunnen zijn voor het alsnog ongeldig verklaren van een voorlopig gegunde opdracht?	Aanbestedende Dienst begrijpt dat. In het geval dat tijdens de verificatiefase een materiedeskundige bezwaar maakt tegen de definitieve gunning zal dat altijd zijn op objectief houdbare bezwaren en te allen tijde volledig schriftelijk en juridisch onderbouwd kenbaar worden gemaakt.
236	BD 4.4.2	De vier aan te tonen kerncompetenties zijn in zwaarte, omvang van het gevraagde, niet gelijk maar de jaarlijks gefactureerde waarde voor de referentieopdrachten die de kerncompetenties moeten aantonen is voor alle vier de op te leveren opdrachten wel gelijk. Een waarde van 300.000 euro is daarbij erg hoog, zeker voor wat betreft 'losse' referentieopdrachten voor kerncompetenties B, C en D, waar onder andere expliciet wordt gevraagd naar ervaring bij kleine of middelgrote organisaties. Heeft de aanbestedende dienst een voorkeur voor Geïnteresseerden die alle vier de kerncompetenties met één referentieopdracht kunnen aantonen (wat het een stuk eenvoudiger maakt om de gevraagde waarde te realiseren)? Zo niet, waarom kiest u dan voor alle vier de aan de te tonen competenties voor dit hoge bedrag?	Het is voor de Aanbestedende Dienst belangrijk dat de referentieopdrachten voldoende groot zijn. Er is geen specifieke voorkeur maar de kerncompetenties mogen ook aangetoond worden in een referentieopdracht waarin alle kerncompetenties voorkomen indien duidelijk is dat aan alle kerncompetenties invulling is gegeven.
237	BD 5.2	Het ondertekenen van de UEA is bij inschrijving voldoende voor een aantal zaken. De laatste bullet noemt expliciet ook de bevestiging van geen Russische betrokkenheid. Daarbij wordt ook verwezen naar Bijlage F. Geïnteresseerde gaat ervan uit dat deze verklaring bij inschrijving niet (ondertekend) hoeft te worden ingediend. Kunt u dit bevestigen?	Correct, u dient deze verklaring uiteraard wel bij de bewijsmiddelen in te leveren, na voorlopige gunning.
238	BD 6.8	Wat betreft de Gunningscriteria G3 (p.43) en G4 (p. 45) zou er verwarring kunnen bestaan over het aantal toegestane pagina's, tien of (15). Kunt u hier helderheid verschaffen?	Het betreft 10 (tien) pagina's.

239	BD 6.8	De Gunningscriteria G3 en G4 betreffen kansendossiers. Geïnteresseerde legt dit in eerste instantie uit als twee keer een beschrijving van een separate kans, nl G3 en G4. De beschrijvingen onder de kopjes Kansencomponent en de verschillen daarbij tussen G3 en G4: (G3): "Inschrijver wordt gevraagd per Kans aan te geven" en (G4): Inschrijver wordt gevraagd aan te geven welke kansen zij aanbiedt en aan te geven in welke mate deze kansen bijdragen aan bovenstaande doelstelling. Per kans wordt gevraagd:") maken dat het voor Geïnteresseerde niet duidelijk is of onder deze Gunningscriteria beide keren één samenhangende kans moet worden beschreven of dat onder beide Kansendossiers meerdere aparte kansen mogen worden ingediend. Kunt u bevestigen dat u per Gunningscriterium G3 en G4 één samenhangende kans bescheven wilt zien?	De gunningscriteria G3 en G4 zijn aparte kansendossier waarbij u aparte businesscases dient in te dienen die dan ook onafhankelijk van elkaar worden beoordeeld. Na gunning kunnen deze kansen dan ook onafhankelijk van elkaar worden afgenomen indien daartoe wordt besloten.
240	Bijlage O - Prijzenblad	Kolom M biedt de mogelijkheid een toelichting te geven op gevraagde prijselementen. Kunt u aangeven of en in welke gevallen u ook expliciet een toelichting verwacht en daarbij welke rol eventueel gegeven toelichtingen spelen of kunnen spelen in het verdere proces?	U wordt verzocht uitsluitend de cellen in het Rood in te vullen. Eventuele opmerkingen worden niet in de prijsbeoordeling meegenomen.
241	BD 6.8(.1) Prijs, beoordelingskader prijs en Bijlage O - Prijzenblad	Zowel in de tabel op p.38 als bij de getotaliseerde waarde in cel L168 van het Prijzenblad wordt de beoordelingsprijs / vergelijkingswaarde gebaseerd op de kosten van 2x implementatie en 2x een jaar dienstverlening. Maar het beoordelingskader (p.50) spreekt over Totale Kosten Inschrijving. Dit roept verwarring op over welke formule precies de inschrijfprijs bepaalt en welke formule precies bepaalt of geïnteresseerde inschrijft binnen de grensbedragen. Kunt u beide zaken verduidelijken?	Als u de tarieven invult in de cellen in het Rood dan sommeert het Prijzenblad deze naar Implementatiekosten MSP, Jaarkosten MSP, Implementatiekosten MSSP en Jaarkosten MSSP. Deze 4 elementen vormen tesamen de Beoordelingsprijs aam de hand waarvan uw prijscriterium wordt beoordeeld.
242	BD 6.8.1 - Licentiekosten Managed Services, Bijlage O - Prijzenblad	Het Beschrijvend Document vraagd in de toelichting om "een prijs per gebruiker per maand op te geven voor het totaal aan gebruikerslicentiekosten voor de managed services" In het Prijzenblad wordt een prijs per gebruiker gevraagd voor elk onderdeel van de in beheer te nemen dienstverlening welke, zo begrijpt Geïntereseerde, nu via de huidige CSP wordt verstrekt en welke als onderdeel van de dienstverlening van deze CSP wordt overgenomen. Geïnteresseerde meent onvoldoende informatie te hebben over alle licenties die in scope zijn en die hier beprijsd moeten worden. Ook de toelichting dat er rekening gehouden dient te worden met "de uitgangspunten en specificaties zoals beschreven in de Aanbestedingsstukken voor de Client Solution Provider (CSP)" roept meer vragen op daar we deze uitgangspunten en specificaties niet kunnen lokaliseren in de Aanbestedingsstukken. De tekst achter de bullet "Extra software .... beschikbaar wordt gemaakt", wordt ook onvoldoende begrepen. Kunt u in het licht van het voorgaande het onderdeel licentiekosten Managed Services verduidelijken en daarbij specifiek nagaan of geïntereseerden volledige / voldoende informatie hebben over alle in scope zijnde licenties om alle gevraagde licentie-onderdelen op een gekende en onderbouwde manier te beprijzen?	Onder 'Licentiekosten Managed Services' vermeldt u de licentiekosten die u per gebruiker per maand in rekening brengt via het CSP-beheer voor desbetreffende service. Vanuit de Marktconsultatie heeft Aanbestedende Dienst van het merendeel van de deelnemers het advies ontvangen deze indeling aan te houden. Wellicht dat u in de volgende vragenronde vragen kunt stellen naar de specifieke informatie die u hiervoor nodig heeft.
243	BD 6.8.1 - Licentiekosten Managed Security Services	Kunt u verduidelijken wat precies wordt bedoeld en verwacht met de zin: "Voor alle licenties geldt dat ze eeuwigdurend moeten zijn". Als uw uitleg neerkomt op een voorwaarde die in de markt (van licentieverstrekking) niet gebruikelijk is, kunt u deze eis dan laten vervallen?	Aanbestedende Dienst bedoelt met 'eeuwigdurend' dat deze licenties / gebruiksrechten geen vast bepaalde looptijd hebben. Deze licenties lopen al en blijven lopen ook na aflopen van de Overeenkomst.
244	BD 6.8.1 - Licentiekosten Managed Security Services	In het BD staat onder het Kopje "Licentiekosten (kosten programmatuur en/ of applicatiesoftware) Managed Security Services": "Extra software op aanvraag van de gebruiker". Het is niet duidelijk wat hier wordt bedoeld, welke extra software, van welke gebruiker en hoe kan iets dat nog niet bekend is al wel worden beprijsd). Kunt u dit toelichten? (De kopjes op het prijzenblad zijn overigens niet gelijk aan de kopjes in het Beschrijvend Document.)	Wij starten met een basisset van appllicaties die periodiek voorzien moeten worden van updates. Het gaat met name om dat stuk technisch beheer (updates, configuraties, uitrollen van applicaties etc). Hierin maken wij onderscheid tussen twee aanvragen die wij van gebruikers verwachten: (1) Als wij nieuwe applicatie aanvragen krijgen dan willen wij dat dit proces geborgd is bij de MSP. Wij kunnen hier afspraken over maken over max aantal applicaties en daar de prijs op hanteren. Alle extra nieuwe applicaties kunnen tegen meerkosten in beheer worden genomen. (2) Voor wat betreft een aantal bestaande applicaties is het zo dat niet alle gebruikers deze geinstalleerd krijgen op hun machine. Op het moment dat zij deze aanvragen dan zal de MSP deze uitrollen op de betreffende machines.
245	BD 6.8.1 - Overig	De vijfde bullet geeft aan dat exit-kosten een uitzondering zijn op het voorschrift dat geen bedragen van nul euro mogen worden ingevuld. Dit wordt echter ook onder Eenmalige Implementatieklosten (2x) genoemd als toegestaan. Welk voorschrift moet worden gevolgd?	Aanbestedende Dienst maakt onderscheid tussen Kosten opstellen exit-plan als onderdeel van de Implementatiekostenenerzijds, en Kosten voor de uitvoering van de Exit anderzijds. U mag in beide gevallen 0 invullen indien u geen kosten in rekening brengt voor hetzij het opstellen van het exit-plan, hetzij voor de uitvoering van de Exit.
246	BD algemeen / MSSP	Kunt u aangeven welke SIEM-oplossing momenteel in gebruik is binnen GGN ?	- Het huidige SOC bestaat uit 6 teamleden van SOC Data analisten en SOC technisch analisten en 1 SOC architect. - Applicaties: Ms-Sentinel, Ms-Defender, Splunk, Topdesk / ServiceNow - Logbronnen: Maatwerkapllicaties voor de GGD'en en Bedrijfsbrede toepassingen van Aanbestedende Dienst De levering van de softwarelicenties loopt via de CSP, deze overeenkomst eindigt in december 2026 en wordt geacht door de MSP te worden overgenomen.
247	BD algemeen / MSSP	Is het toegestaan om parallel aan de as-is inbeheername een verbeterde/gestandaardiseerde inrichting op te bouwen in “shadow mode” (passief), waarbij pas na gezamenlijke acceptatie een cut-over plaatsvindt?	Het staat Opdrachtnemer volledig vrij deze werkwijze te hanteren, mits er tenminste aan de eisen uit het Programma van Eisen wordt voldaan en mits verbeteringen en initiatieven tot standaardisatie eerst worden opgenomen in de Backlog MSSP en door Aanbestedende Dienst in overleg met Opdrachtnemer worden overeengekomen.
248	BD algemeen / MSSP	Kunt u toelichten hoe de samenwerking tussen opdrachtnemer en het GGN-eigen SOC wordt ingericht (rollen, verantwoordelijkheden, escalatielijnen)?	Op dit moment beschikt Aanbestedende Dienst over een eigen SOC met een SIEM (Sentinel) en een in eigen beheer ontwikkeld Logbuffet (Log verzamelaar) welke de loggingdata aanlevert bij een tweede SIEM (Splunk). De activiteiten van het SOC en de SIEM-voorzieningen dienen as-is door de MSSP in beheer te worden genomen en aan de hand van de backlog MSSP verder te worden geoptimaliseerd in de breedste zin van het woord. Aansturing van de MSSP zal in eerste instantie door het eigen SOC van aanbestedende dienst geschieden, echter het ligt in de lijn der verwachting dat het eigen SOC op termijn wordt veranderd naar een G-SOC of Governance SOC met uitsluitend een regiefunctie naar de MSSP.
249	BD algemeen / MSSP	Welke endpoint security oplossing wordt momenteel gebruikt (Microsoft Defender for Endpoint of een alternatieve oplossing)?	Microsoft defender for Endpoint - volledige XDR
250	BD algemeen / MSSP	Is een overzicht beschikbaar van de huidige Microsoft Security licenties (bijv. M365 E5, Security add-ons, Defender licenties)?	MS Windows 11 MS Office 365 MS SharePoint MS Power BI MS Azure Virtual Desktop MS Sentinel: MS Defender for Threat Intelligence MS Office 365 MS Defender for Endpoint Azure Services Entra ID MS Entra ID Protection MS Defender for Business MS Defender for Cloud Apps MS Defender for Office 365 (o.a. Purview alerting DLP) MS Defender for Vulnerability Management Aanbestedende Dienst heeft de Non Profitstatus conform de voorwaarden van Microsoft.

251	BD algemeen / MSSP	Welke logbronnen moeten minimaal worden aangesloten op de SIEM-omgeving (M365, Entra-ID, endpoints, firewalls, applicaties, ketenpartners)?	Sentinel: MS Defender for Threat Intelligence MS Office 365 MS Defender for Endpoint Azure Services Entra ID MS Entra ID Protection MS Defender for Business MS Defender for Cloud Apps MS Defender for Office 365 (o.a. Purview alerting DLP) MS Defender for Vulnerability Management Firewall syslog van HPZone omgeving Keeper SPLUNK: Delta Gateway (iMPeX en HPV18+) TOPdesk SOC SPLUNK via Logbuffet: HPZone GraphQL CoronIT iTBC iTBC IMS EVS Cluster TBC EVS Cluster SG (25 keer) PGA Registratieschil
252	BD algemeen / MSSP	Indien Microsoft Sentinel wordt gebruikt: betreft dit één centrale Sentinel-omgeving (workspace) of meerdere workspaces/subscriptions (bijv. per domein/omgeving)?	Eén centrale Sentinel-omgeving
253	BD algemeen / MSSP	Hoeveel maatwerk applicaties zijn momenteel toegevoegd aan de SIEM oplossing?	Op Sentinel: Keeper en Guardian360 en firewall Op Splunk is alles maatwerk applicaties
254	PvE eis 6	Accepteert GGN dat sommige Microsoft-diensten door Microsoft buiten de EER worden verwerkt (metadata, threat intelligence, logs)?	Aanbestedende Dienst is zich bewust van het feit dat het vrijwel onmogelijk is álle data (zoals metadata) binnen de EER te houden. De voorkeur van Aanbestedende Dienst is dat alle data binnen de EER blijft. Aanbestedende Dienst hanteert hier het Rijksbrede Cloudbeleid dat dit wél toestaat.
255	PvE eis 6	Geldt deze eis voor productie-data, voor logging, of ook voor telemetrie?	Aanbestedende Dienst is zich bewust van het feit dat het vrijwel onmogelijk is álle data (zoals metadata) binnen de EER te houden. De voorkeur van Aanbestedende Dienst is dat alle data binnen de EER blijft. Aanbestedende Dienst hanteert hier het Rijksbrede Cloudbeleid dat dit wél toestaat.
256	PvE eis 10	elke concrete organisatorische, juridische en technische maatregelen verwacht GGN om “schending, vertraging of aanvechten” van datasoevereiniteit te realiseren?	Aanbestedende Dienst is zich bewust van het feit dat het vrijwel onmogelijk is garanties voor Data Soevereiniteit te krijgen. Deze Eis is opgenomen omdat Aanbestedende Dienst het belangrijk vind dat Opdrachtnemer in een situatie waarbij de Data Soevereiniteit in het geding komt, alles wat technisch, juridisch en/ of organisatorisch mogelijk is in het werk stelt om schending te voorkomen / vertragen/ aan te vechten.
257	PvE eis 10	Welke acceptatiecriteria gebruikt GGN om te bepalen of hieraan voldaan is?	Zie vorige vraag - Denk hierbij aan voorzieningen als het gebruik van Ms Cloud for Sovereignty (technisch), controle over encryptiesleutels (organisatorisch) of de beschikking over juridische maatregelen om een dataverzoek aan te vechten.
258	PvE eis 13	Is GGN zich bewust dat Microsoft Defender, Sentinel, Entra en andere diensten standaard AI/ML gebruiken?	Aanbestedende dienst is zich bewust van- en maakt reeds gebruik van- de in Microsoftproducten geïntegreerde AI-functionaliteiten. Aanbestedende dienst wenst daarom Eis 13 als volgt aan te passen: Opdrachtnemer garandeert dat voor de levering van managed services en managed security services, geen gebruik gemaakt zal worden van Kunstmatige Intelligentie (AI), Large Language Models e.d. behoudens de reeds in Microsoftproducten aanwezige AI-functionaliteiten, tenzij dit in overleg met Opdrachtgever schriftelijk anders is overeengekomen en vooraf is getoetst aan het GGN AI-beleid en door het CISO-office.
259	PvE eis 13	Valt het gebruik van ingebouwde Microsoft AI-componenten onder dit verbod?	Aanbestedende dienst is zich bewust van- en maakt reeds gebruik van- de in Microsoftproducten geïntegreerde AI-functionaliteiten. Aanbestedende dienst wenst daarom Eis 13 als volgt aan te passen: Opdrachtnemer garandeert dat voor de levering van managed services en managed security services, geen gebruik gemaakt zal worden van Kunstmatige Intelligentie (AI), Large Language Models e.d. behoudens de reeds in Microsoftproducten aanwezige AI-functionaliteiten, tenzij dit in overleg met Opdrachtgever schriftelijk anders is overeengekomen en vooraf is getoetst aan het GGN AI-beleid en door het CISO-office.
260	PvE eis 22	Betekent “as-is” dat er geen directe wijzigingen mogen plaatsvinden, zelfs niet voor security-hardening?	U mag er van uitgaan dat Aanbestedende Dienst voldoet aan de beveiligingsnormen die zij ook aan Opdrachtnemer stelt. Indien bij de Due Diligence / Implementatieplanning blijkt dat Aanbestedende Dienst alsnog niet voldoet dan ligt er in dergelijk geval de taak voor Aanbestedende Dienst om alsnog voor de juiste randvoorwaarden te zorgen, dan wel hier met Opdrachtnemer afspraken/ uitzonderingen overeen te komen.
261	PvE eis 22	Zijn er uitzonderingen toegestaan wanneer huidige instellingen niet voldoen aan beveiligingsnormen (BIO, NEN, MS best practices)?	U mag er van uitgaan dat Aanbestedende Dienst voldoet aan de beveiligingsnormen die zij ook aan Opdrachtnemer stelt. Indien bij de Due Diligence / Implementatieplanning blijkt dat Aanbestedende Dienst alsnog niet voldoet dan ligt er in dergelijk geval de taak voor Aanbestedende Dienst om alsnog voor de juiste randvoorwaarden te zorgen, dan wel hier met Opdrachtnemer afspraken/ uitzonderingen overeen te komen.
262	PvE eisen 31 & 32	Dagelijkse volledige backup van alle M365-data => mogelijk? *Welke definitie hanteert GGN voor “volledige back-up” van M365-data?*	Alle in de eis genoemde M365-diensten inclusief bijbehorende data en configuraties die noodzakelijk zijn voor volledig herstel van functionaliteit.
263	PvE eisen 31 & 32	Welke definitie hanteert GGN voor “volledige back-up” van M365-data?	Alle in de eis genoemde M365-diensten inclusief bijbehorende data en configuraties die noodzakelijk zijn voor volledig herstel van functionaliteit.
264	Pve eis 85	Welke gegevens moeten real-time inzichtelijk zijn?	Aanbestedende Dienst bedoelt hier met name Incidenten.
265	Pve eis 85	Moeten dashboards ontwikkeld worden in specifieke tooling (Sentinel, Power BI, ServiceNow, iets anders)?	Aanbestedende Dienst bedoelt hier real-time dashboards die de SOC werkzaamheden / diensten actief en relevant ondersteunen. U moet hier denken aan bijvoorbeeld PowerBI (Management Info), Sentinel (Actuele Incidenten) en ServiceNow (status lopende tickets).
266	Pve eis 85	Hoe snel moet data ververst zijn om als “real-time” te gelden?	In het geval van applicatiemonitoring hanteren wij nu minimaal 15 minuten verversing
267		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:	

268	GIBIT 2023, artikel 4.1 & 4.2	i. De aanbestedende dienst zelf niet of niet tijdig de noodzakelijke medewerking verleent aan de uitvoering van de overeenkomst, of	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn. Aanbestedende Dienst heeft de noodzaak tot deze aanbesteding voldoende gemotiveerd, op basis waarvan u mag aannemen dat Aanbestedende Dienst alles in het werk zal stellen om de uitvoering van de te sluiten Overeenkomst te laten slagen.
269		ii. De aanbestedende dienst zelf niet of niet alle door voor de uitvoering van de overeenkomst benodigde informatie verstrekt, of	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn. Aanbestedende Dienst heeft de noodzaak tot deze aanbesteding voldoende gemotiveerd, op basis waarvan u mag aannemen dat Aanbestedende Dienst alles in het werk zal stellen om de uitvoering van de te sluiten Overeenkomst te laten slagen.
270		iii. De aanbestedende dienst zelf de voor de voortgang van de werkzaamheden van Leverancier benodigde besluiten niet of niet tijdig neemt; of	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn. Aanbestedende Dienst heeft de noodzaak tot deze aanbesteding voldoende gemotiveerd, op basis waarvan u mag aannemen dat Aanbestedende Dienst alles in het werk zal stellen om de uitvoering van de te sluiten Overeenkomst te laten slagen.
271		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	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn. Aanbestedende Dienst heeft de noodzaak tot deze aanbesteding voldoende gemotiveerd, op basis waarvan u mag aannemen dat Aanbestedende Dienst alles in het werk zal stellen om de uitvoering van de te sluiten Overeenkomst te laten slagen.
272		v. 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	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn. Aanbestedende Dienst heeft de noodzaak tot deze aanbesteding voldoende gemotiveerd, op basis waarvan u mag aannemen dat Aanbestedende Dienst alles in het werk zal stellen om de uitvoering van de te sluiten Overeenkomst te laten slagen.
273		vi. 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?	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn. Aanbestedende Dienst heeft de noodzaak tot deze aanbesteding voldoende gemotiveerd, op basis waarvan u mag aannemen dat Aanbestedende Dienst alles in het werk zal stellen om de uitvoering van de te sluiten Overeenkomst te laten slagen.
274	GIBIT 2023, artikel 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?	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn. Aanbestedende Dienst heeft de noodzaak tot deze aanbesteding voldoende gemotiveerd, op basis waarvan u mag aannemen dat Aanbestedende Dienst alles in het werk zal stellen om de uitvoering van de te sluiten Overeenkomst te laten slagen.
275	GIBIT 2023, artikel 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…*'?	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn. Aanbestedende Dienst is van mening dat de gevraagde dienstverlening breed verkrijgbaar en in hoge mate gestandaardiseerd worden aangeboden. Met Garanties worden derhalve resultaatverplichtingen aangegaan, een inspanningsverplichting is hierbij onvoldoende.
276	GIBIT 2023 artikel 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?	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn. Op basis van de eerdere Marktconsultatie heeft Aanbestedende Dienst begrepen dat de Gibit 2023 voorwaarden redelijk zijn.
277		Zo niet, bent u dan bereid akkoord te gaan met een ander plafondbedrag (anders dan de beperking per jaar)?	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn. Op basis van de eerdere Marktconsultatie heeft Aanbestedende Dienst begrepen dat de Gibit 2023 voorwaarden redelijk zijn, het schadebedrag is voor Aanbestedende Dienst bespreekbaar.
278	GIBIT 2023 artikel 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?	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn.
279	GIBIT 2023 artikel 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?	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn.
280	GIBIT 2023 artikel 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 10,000 EURO (ongeacht het aantal gebeurtenissen)?	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn.
281	GIBIT 2023 artikel 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)?	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn. Aanbestedende Dienst schaft geen software aan, maar neemt licenties af via het CSP-programma van Microsoft. Voor deze licenties is Aanbestedende Dienst reeds akkoord gegaan met de Licentievoorwaarden van Microsoft
282	GIBIT 2023 artikel 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.	
283	GIBIT 2023 artikel 25	Is opdrachtgever bereid aan dit artikel toe te voegen dat:	
284		- Een controle niet wordt verricht door een concurrent van Opdrachtnemer;	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn.
285		- Dat de partij die de controle uitvoert gehouden is aan geheimhoudingverplichtingen welke tenminste vergelijkbaar zijn met die welke zijn opgenomen in deze voorwaarden;	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn.
286		- Een controle altijd wordt uitgevoerd op basis van een vooraf tussen partijen overeengekomen auditplan;	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn.
287		- 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.	Aanbestedende Dienst hanteert de standaard GIBIT 2023 inkoopvoorwaarden welke voor elke aanbestedingsprocedure worden gehanteerd en in principe niet onderhandelbaar zijn.
288			

289	Beschrijvend document: Licenties	Kunt u specificeren welke Microsoft- en/of overige security-licenties momenteel aanwezig zijn binnen de bestaande SOC-dienstverlening, inclusief eventuele non-profit licentieconstructies?	MS Windows 11 MS Office 365 MS SharePoint MS Power BI MS Azure Virtual Desktop MS Sentinel: MS Defender for Threat Intelligence MS Office 365 MS Defender for Endpoint Azure Services Entra ID MS Entra ID Protection MS Defender for Business MS Defender for Cloud Apps MS Defender for Office 365 (o.a. Purview alerting DLP) MS Defender for Vulnerability Management Aanbestedende Dienst heeft de Non Profitstatus conform de voorwaarden van Microsoft.
290	Beschrijvend document: SOLL	Is het de expliciete wens dat de SOC-dienstverlening in de SOLL-situatie gebaseerd wordt op Microsoft-technologie? Of staat de MSSP vrij om, binnen de gestelde functionele vereisten, een best-of-breed oplossing aan te bieden?	Aanbestedende Dienst is volstrekt duidelijk dat op dit moment uitsluitend Microsoft-technologie wordt gehanteerd.
291	Beschrijvend document: IST	Kunt u een actuele architectuurplaat of -documentatie delen van de huidige SOC- en IT-omgeving, zodat duidelijk wordt welke componenten en verantwoordelijkheden door de MSSP moeten worden overgenomen?	Aanbestedende Dienst heeft bij de marktconsultatie een Bijlage Praatplaat gepubliceerd. Vanwege het vertrouwelijke karakter van de huidige SOC en IT-omgeving worden géén gedetailleerde architectuurplaten verstrekt en wordt het SOC SIEM uitsluitend functioneel gespecificeerd.
292	Beschrijvend document: G-SOC	Kunt u een uitgebreide beschrijving verstrekken van de taken, verantwoordelijkheden en positionering van het G-SOC, zodat helder wordt hoe de samenwerking en taakverdeling met de toekomstige MSSP vormgegeven moet worden?	Het G-SOC of Governance-SOC is naar verwachting de uitwerking van de Functionele Regie Organisatie in relatie tot het SOC/SIEM. Dit houdt in dat het G-SOC een regierol zal vervullen in de situatie dat de MSSP het SOC/SIEM volledig in beheer heeft overgenomen. In het G-SOC kunt u de rollen Product Owner, Service Level Manager, Privacy Officer, CISO Officer, Compliance & Audit Officer verwachten. Onderdeel van de implementatie zal zijn dat Aanbestedende Dienst in samenwerking met Opdrachtnemer een RASCI-matrix zal overeenkomen.
-	-	-	-
293	n.v.t.	Kunt u nader inzicht bieden in het huidige MSP-landschap? o de huidige Werkplek oplossing (fysiek & virtueel) o de architectuur van het volledige werkplekdomein o gebruikte applicaties lokaal o gebruikte applicaties cloud o Mate van beveiliging / toegepast beveiligingsbeleid	MS Windows 11 MS Office 365 MS SharePoint MS Power BI MS Azure Virtual Desktop MS Sentinel: MS Defender for Threat Intelligence MS Office 365 MS Defender for Endpoint Azure Services Entra ID MS Entra ID Protection MS Defender for Business MS Defender for Cloud Apps MS Defender for Office 365 (o.a. Purview alerting DLP) MS Defender for Vulnerability Management Splunk
294	BD Uitgangspunt hierbij is dat een groot deel van het momenteel door GGD GHOR Nederland beheerde landschap van applicaties voor de GGD'en en GHOR-bureaus zal worden afgebakend (carve-out) en in beheer zal worden gegeven aan een Landelijke Beheer Organisatie (LBO)	Welke applicaties of onderdelen worden op termijn overgedragen aan een landelijke beheerorganisatie en welke blijven onder verantwoordelijkheid van de MSP?	Of, wanneer en in hoeverre applicaties worden overgedragen is op dit moment nog onderwerp voor besluitvorming. De demarcatie zal liggen bij applicaties die van overheidswege gecontinueerd moeten worden en binnen overheidskaders in beheer moeten blijven. Aanbestedende Dienst GGD GHOR Nederland is géén Overheidsorganisatie in die zin. Wat zeker is is dat de bedrijfsbrede toepassingen zoals AFAS, Kantoorautomatisering, ServiceNow e.d. te allen tijde onder de verantwoordelijkheid van SOC/SIEM en MSSP blijven vallen. Technisch betreft het de logstromen van de systemen HPZone en CoronIT (t.b.v. infectieziektebestrijding) en de BI omgeving daaromtrent (DeltaGateway) aangevuld met de daar aanwezige datacollecties omtrent HPV18+ en ImPex. De vervangende systemen hiervoor zullen worden ondergebracht bij de LBO.
295	BD Aanzienlijk aantal verschillende leveranciers	tbv dienstovername is inzicht benodigd in het aantal leveranciers en wordt daarbij geacht dat Opdrachtnemer deze leveranciers gaat aansturen? In welke vorm wordt dit verwacht? (SPOC vs Service-integrator (SIAM))?	De lopende contracten (>12) met huidige leveranciers lopen af. Dit zijn allemaal losse contracten die tezamen de supply chain vormen voor de interne/ eigen Managed Services en Managed Security Services. In plaats van al deze contracten individueel te laten opvolgen en zodoende het versnipperde leverancierlandschap in stand te houden, is het doel van deze aanbesteding om 1 opdrachtnemer te selecteren die middels 1 Overeenkomst voorziet in alle elementen van de interne/ eigen Managed Services en Managed Security Services en die deze as a service (als dienst) beschikbaar maakt.
296	BD Kantoor Cloudhosting	Wat wordt concreet verstaand onder 'Kantoor Cloudhosting, betreft dit de 60x virtuele werkplekken zoals genoemd op Prijzenblad, of anders?	Aanbestedende Dienst verstaat onder Kantoor Cloudhosting: Het geheel van managed Cloudhosting voor de volgende domeinen: Productiviteit en samenwerking: Exchange online, Ms Office 365, Teams, Teams Manager, SharePoint Bestandsopslag: Persoonlijke en gedeelde OneDrives, SharePoint Bibliotheken en Azure Files, Back-up en Archivering Werkplekbeheer en Beveiliging: Ms Entra ID, Intune (Endpoint Manager) en security tools (Defender e.d.) Virtual Desktop Infrastructuur (VDI) voor Azure Virtual Desktop (AVD) en Windows 365

297	BD De huidige contracten zijn reeds verlengd en lopen einde 2026 af. Het is daarom noodzakelijk deze contracten tijdig te vervangen.	Is dit de verantwoordelijkheid van de Opdrachtnemer of adviseert de Opdrachtgever hierin? Aanvullend op de SPOC vraag (nr 1).	De lopende contracten (>12) met huidige leveranciers lopen af. Dit zijn allemaal losse contracten die tezamen de supply chain vormen voor de interne/ eigen Managed Services en Managed Security Services. In plaats van al deze contracten individueel te laten opvolgen en zodoende het versnipperde leverancierlandschap in stand te houden, is het doel van deze aanbesteding om 1 opdrachtnemer te selecteren die middels 1 Overeenkomst voorziet in alle elementen van de interne/ eigen Managed Services en Managed Security Services en die deze as a service (als dienst) beschikbaar maakt.
298	BD Beheer Servicedesk in samenwerking met de eigen GGD GHOR Nederland-servicedesk	Wat is de rol van de Opdrachtnemer in de samenwerking met GGD Servicedesk? Neemt de Opdrachtnemer de volledige Servicedesk over voor de MSP & MSSP dienstverlening (1e lijn Support), of vervult 2e lijn Support, of anders?	Aanbestedende Dienst verwacht (zie Beschrijvend Document) een groot aantal veranderingen door te voeren de komende jaren. Vooralsnog zal in het eerste jaar de eigen Servicedesk in stand worden gehouden die alle 1ste lijns supportitems in behandeling zullen nemen en waarbij MSP/ MSSP de 2de lijns support zal verzorgen. Indien het komt tot een besluit ook de eigen ServiceDesk af te bouwen dan zal dit in overleg met Opdrachtnemer worden uitgewerkt.
299	BD Aantal Mobiele toestellen 150	- Corporate, BYOD of mix van toestellen? -Worden deze toestellen beheerd, zo ja hoe?	Het is een mix van BYOD en corporate mobiele devices. Corporate devices worden volledig beheerd middels Mobile Device Management
300	BD Het fysieke kantoor van GGD GHOR Nederland	Klopt het dat alle statische componenten (servers, netwerkcomponenten, firewalls, printers en vergadervoorzieningen) op 1 locatie actief zijn, of zijn deze verdeeld over meerdere locaties? Zo ja, welke?	Het is correct dat al deze voorzieningen op 1 locatie aanwezig zijn op het kantoor van Aanbestedende Dienst in Utrecht.
301	BD Aantal Netwerkcomponenten 10	Gaat het hier alleen om vast netwerk, of ook draadloos (Wi-Fi) en zijn de geschatte aantallen daarmee realistisch?	Het aantal Netwerkcomponenten waarmee gerekend wordt is ten behoeve van de bepaling van de jaarsom in het Prijscriterium. Het tarief dat u daar invult zal worden gehanteerd voor de Overeenkomst. Aanbestedende Dienst beschikt op 1 kantoorlocatie over zowel een fysiek ethernet-netwerk alsook een draadloos WiFi Netwerk
302	Boven- en ondergrens	In de aanbestedingsdocumenten wordt een ondergrens en bovengrens genoemd, waarbij is aangegeven dat de uiteindelijke omvang van de opdracht niet vooraf is vastgesteld. Gezien het feit dat GGD GHOR Nederland een marktconsultatie heeft uitgevoerd en hieruit een indicatieve bandbreedte is bepaald, verzoeken wij om verduidelijking inzake de beoordeling van inschrijvingen die (significant) onder de ondergrens dan wel boven de bovengrens worden aangeboden. Kunt u bevestigen hoe om te gaan met inschrijvingen waarvan de prijsstelling mogelijk als niet-marktconform of als manipulatief wordt beschouwd? Wordt een inschrijving die duidelijk buiten de vastgestelde bandbreedte valt — zowel aan de onder- als aan de bovenzijde — terzijde gelegd, of wordt deze op een andere wijze beoordeeld binnen het kader van marktconformiteit en proportionaliteit?	De marktconsultatie en benchmark en de analyse van de kosten van de afgelopen jaren hebben gediend als basis voor de berekening van de Opdrachtwaarde. Tegelijkertijd is Aanbestedende Dienst zich bewust van het feit dat deze berekening (significant) kan afwijken van de daadwerkelijke offertes en heeft daarom het prijscriterium dusdanig uitgewerkt dat een goede beoordeling kan plaats vinden op basis van Implementatiekosten, kosten managed services en kosten van de uren voor alles wat niet standaard onder de kosten van de managed services valt. De ruwe berekening van de Opdrachtwaarde geeft een redelijke verwachting aan maar is geen dwingende bandbreedte.
303	BD Managed Data Intelligence	Kunt u nader inzicht bieden in het huidige Data Intelligence Voorziening? o De huidige architectuur o Gebruikte platform(en) o Betrokken afnemers en leveranciers o De technische rol van de MSP	Voor de huidige Managed Data Intelligence Services maakt Aanbestedende Dienst gebruik van 2 contractpartijen die uit oogpunt van vertrouwelijkheid hier niet bij naam genoemd worden. Voor de voorzieningen geldt dat er gebruik wordt gemaakt van: - Dataportaal, webapplicatie voor toegangsbeheer tot dashboards, rapportages en content - Power BI voor het samenstellen van dashboards en rapportages - Datakubussen & DeltaGateway voor de OTAP-omgeving, Operational Data Store en Data warehouse-laag De Managed Data Intelligence Services staan in principe los van de rol van de MSP.
304	BD Hetzij met gebruikmaking van de GGN-eigen ServiceNow-omgeving hetzij met een koppeling tussen de servicemanagement omgeving van Opdrachtnemer en de GGN-eigen ServiceNow-om	Zijn er minimale vereisten aan een interface tussen GGN-ServiceNow en ITSM-systeem van Opdrachtnemer, zo ja welke?	Uitgangspunt bij een koppeling tussen ITSM van Opdrachtnemer en ServiceNow van Aanbestedende Dienst is dat deze koppeling ISO27001 en specifiek BIO-compliant zijn. Hiermee wordt bedoeld de authenticatie- (oAuth) autorisatie- (Least Privilege) versleuteling- (TLS 1.3) en logging (Elke API call moet gelogd worden) eisen uit de BIO.
305	PvE Elke 24 uur een back-up van specifieke data	Hoe lang dient iedere type back-up bewaard te blijven, of wenst Opdrachtgever hier anders mee om te gaan?	Aanbestedende Dienst hanteert een duidelijk onderscheid tussen haar verplichtingen op basis van de Archiefwet en haar verplichtingen op basis van haar ISO27001 en BIO compliance. De back-up valt onder ISO27001, BIO en AVG die stellen dat de beschikbaarheid van informatie wordt geborgd (1 jaar) maar dat de persoonlijke data van medewerkers na 6 maanden dient te worden verwijderd.
306	PvE Alle Fysieke en Virtuele werkplekken te allen tijde middels Microsoft Intune (of gelijkwaardig) als Unified Endpoint Management (UEM)-oplossing centraal worden beheerd.	Zijn alle huidige werkplekken, zowel virtueel als fysiek, momenteel ook beheerd via Microsoft oplossingen (Intune, Azure)? En geldt dit ook voor de Applicaties die op de Werkplekken actief zijn?	Ja
307	PvE Opdrachtnemer werkt initieel samen met de GGN-eigen Servicedesk en neemt op aangeven van Opdrachtgever de servicedeskwerkzaamheden op termijn deels of in haar geheel als Managed Service over.	Aanvullend op Nr 5. Verschuiving verantwoordelijkheden Servicedesken tussen Opdrachtgever en Opdrachtnemer gedurende contractperiode. Kan aangegeven worden wat vanaf start contractperiode verwacht wordt van de Servicedesk samenwerking en kan de term 'op termijn' nader toegelicht worden in kader van tijd?	Ten tijde van de Inbeheername zal de eigen Servicedesk van Aanbestedende Dienst nog volledig de eerste lijns support verzorgen. De verwachting is dat dit na Inbeheername (na 1 jaar) per servicemanagement domein aan de MSP zal worden uitgefaseerd.
308	Ovk. Disaster Recovery Test	Wat verwacht de Opdrachtgever concreet van de jaarlijkse Disaster Recovery Test?	De jaarlijkse Disaster Recovery Test is een test waarbij de noodplannen in de praktijk worden getoetst.
309	Ovk. Werkplekken ≥99,5% en Applicaties ≥99,5%	In de concept SLA wordt gesteld dat: de beschikbaarheid van Werkplekken ≥ 99,5% per kwartaal bedraagt, gebaseerd op een beschikbaarheidsvenster van maandag t/m vrijdag van 08:00–18:00 uur; de beschikbaarheid van Applicaties (Office 365 en standaardapplicaties) ≥ 99,5% per kwartaal bedraagt, gebaseerd op een 24/7 beschikbaarheidsvenster; voor beide geldt een maximale downtime van ≤ 10,92 uur per kwartaal. In de bijbehorende toelichting wordt echter aangegeven dat het beschikbaarheidsvenster voor de Werkplekken eveneens 24/7 van toepassing is. Kunt u bevestigen welk beschikbaarheidsvenster leidend is voor de Werkplekken: ma–vr 08:00–18:00 uur of 24/7?	Voor de Werkplekken is het beschikbaarheidsvenster van ma-vr 08:00 - 18:00 van toepassing.
310	J SLA Beschikbaarheid fysieke werkplekken	In de aanbestedingsdocumentatie wordt een beschikbaarheidspercentage gehanteerd voor Werkplekken. Wij constateren dat het hier (mede) fysieke werkplekken betreft. Kunt u toelichten op welke objectieve en verifieerbare wijze de beschikbaarheid van fysieke werkplekken wordt gedefinieerd en gemeten, en hoe hierbij onderscheid wordt gemaakt tussen fysieke componenten (zoals bureau, monitor, dockingstation) en digitale diensten? Indien een betrouwbare en eenduidige meetmethodiek voor fysieke werkplekken niet kan worden vastgesteld, verzoekt u dan te bevestigen dat: * beschikbaarheidspercentages uitsluitend van toepassing zijn op digitale werkplekdiensten en applicaties, en * fysieke werkplekken worden geborgd via responstijden en hersteltijden na melding, in plaats van via beschikbaarheids-KPI's.	Aanbestedende Dienst stelt hier dat het om de software-matige beschikbaarheid van de werkplekken gaat.
311	J SLA De opdrachtnemer levert alle relevante configuratie- en assetgegevens aan, zodat deze volledig en correct kunnen worden opgenomen in het Asset Register van GGD GHOR Nederland.	In de aanbestedingsdocumentatie wordt gesteld dat "de opdrachtnemer alle relevante configuratie- en assetgegevens aanlevert, zodat deze volledig en correct kunnen worden opgenomen in het Asset Register van GGD GHOR Nederland." Kunnen wij ervan uitgaan dat GGD GHOR Nederland verantwoordelijk is voor het verwerken en beheren van deze door de opdrachtnemer aangeleverde informatie in het Asset Register van GGD GHOR Nederland, en dat de rol van de opdrachtnemer zich beperkt tot het aanleveren van juiste en volledige gegevens?	Uw aanname is correct