Title	Onderwerp	Vraag	Antwoord
312	TN vraagnr. 229 Tweezijdige instemming voor verlenging vanaf jaar 9.	Inschrijver kan zich vinden in de strekking van het antwoord op vraag 222. In aanvulling daarop vragen wij om het besluit voor de verlenging vanaf jaar 9 vanuit de partnergedachte tweezijdig te maken. Kunt u daarmee instemmen?	Akkoord, voor verlenging vanaf jaar 9.
313	TN vraagnr. 230 variabele kosten prijzenblad.	"Bij het invullen van het Prijzenblad constateren wij dat de variabele kosten voor inzet van medewerkers worden meegenomen in het totaalbedrag voor Jaar 1. Aangezien deze inzet naar zijn aard variabel en afhankelijk is van daadwerkelijke afname, leidt opname hiervan in het vaste totaalbedrag tot een kunstmatige verhoging van de vergelijkingsprijs en het risico op dubbele kosten, naast de vaste managed service tarieven. Indien de variabele tarieven voor de inzet van medewerkers als optioneel worden toegepast en buiten het totaalbedrag voor het eerste jaar worden gelaten, wordt het risico op dubbele kosten weggenomen en ontstaat een zuivere vergelijkingsprijs. Is het mogelijk deze aanpassing door te voeren in het Prijzenblad?"	De variabele kosten worden zowel voor de MSP als de MSSP uitgevraagd op basis van uurtarieven en op basis van een fictief aantal uren per jaar. Voor de MSP bedraagt dat fictief aantal uren 3.744 (2 FTE) per jaar. Voor de MSSP bedraagt dat fictief aantal uren 3.360 (1.5 FTE) per jaar. Dit is een realistische verwachting. Aanbestedende Dienst is van mening daarmee tot een realistische jaarsom te komen en dat er geen sprake is van een kunstmatige ophoging. Het prijzenblad wordt derhalve niet aangepast. Bij uitvoering van de Opdracht is het aan Aanbestedende Dienst ter beoordeling of en wanneer deze FTE's naast de reguliere dienstverlening moeten worden ingezet.
314	Eis 49 uit Bijlage A PvE	Om de beheerlast (application packaging en lifecycle management) in te schatten: om hoeveel unieke (packaged) applicaties gaat het momenteel in de as-is situatie?	Aanbestedende Dienst hanteert op dit moment 9 windows store apps en 44 packaged apps die nog worden terug gebracht naar ongeveer 35. Mogelijk dat op termijn van die 35 nog een deel om te zetten zijn naar Store apps.
315	Eis 45 uit Bijlage A PvE	GGN wenst zowel de devices als het Cloud Print Management als dienst af te nemen van Opdrachtnemer. Wat omvat dit precies? Alleen de ondersteunende server/software en de apparaten of ook supplies/cartridges, papier, etc?	Aanbestedende Dienst heeft momenteel een contract met Veenman voor de huur van de printers, remote beheer en de mogelijkheid om supplies te bestellen en geleverd te krijgen. Dit contract loopt net als de contracten voor managed services af in december 2026. Aanbestedende Dienst heeft in het PvE de eis gesteld dat deze voorzieningen eerst as-is in (remote) beheer moeten worden genomen, waarbij na einde contract met Veenman het 'Managed Printen en Reproductie' volledig door Inschrijver wordt verzorgd. Het staat Inschrijver vrij om dit ten behoeve van Aanbestedende Dienst bij bijvoorbeeld Veenman of andere leverenciers te betrekken. Voor aantallen en specificaties zie Nota van Inlichtingen 1.
316	Eis 44 uit Bijlage A PvE	Worden het beheer en onderhoud van deze (Hello-ID) infrastructuur en de daaraan gekoppelde flows ook as-is overgedragen aan de Opdrachtnemer of blijft het functioneel beheer hiervan bij GGN?	Hello-ID is een IAM as a service en wordt als zodanig afgenomen. Hello-ID blijft vooralsnog in Functioneel Beheer bij Aanbestedende Dienst. Zie over IAM ook Eis 68 waar de Inbeheername van IAM middels Entra-ID wordt vermeld.
317	Eis 43 uit Bijlage A, PvE	Is zo'n portal/omgeving/platform op dit moment al in gebruik en zo ja welke?	Aanbestedende Dienst maak reeds gebruik Intune.
318	Eis 47 uit Bijlage A PvE	Kunt u specificeren wat deze telefonieomgeving precies omvat? Graag ontvangen wij een overzicht van in ieder geval: •Het type telefonie (bijv. VoIP, vaste telefonie, Microsoft Teams Telefonie, mobiele telefonie of een combinatie daarvan); •Het aantal gebruikers van deze telefonie, toestellen en eventuele callcenter/wachtrijfunctionaliteit; •Eventuele aanvullende componenten, zoals SBC's, SIP trunks, en integraties met andere systemen;	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. Het is een mix van BYOD en corporate mobiele devices. Corporate devices worden volledig beheerd middels Mobile Device Management.
319	Beschrijvend document MSP MSSP, pag 48	Er is op deze pagina sprake van '100 Gigabyte storage per maand' terwijl elders (pag. 20) gesproken wordt over een datavolume van 10 Gigabyte logdata per dag. Dat lijkt elkaar tegen te spreken. Hoe moet Inschrijver dit zien en welk logvolume per dag/maand moet worden aangehouden voor het Prijzenblad?	U dient voor het Prijzenblad uw fee per GigaByte per maand in te vullen. Het Prijzenblad rekent dit door naar Jaarkosten op basis van 100 Gb per maand. Momenteel is er sprake van 10 GigaByte logdata per dag = 300 GigaByte logdata per maand maar dit zal naar verwachting snel afnemen (zie LBO Carve Out).
320	Beschrijvend document MSP MSSP, pag 48	'...in de wetenschap dat binnen 2 jaar mogelijk het GGD GHOR Nederland-eigen SOC volledig wordt uitbesteed': Aanbestedende Dienst vraagt om samenwerking van het SOC van Inschrijver met die van GGN. In de uitvraag herkennen we echter geen duidelijk governance: wie is eindverantwoordelijk? Inschrijver stelt voor: Het GGN SOC is vanaf de start van de dienstverlening verantwoordelijk voor governance, toezicht en is de escalation authority. Inschrijver is dan direct operationeel eindverantwoordelijk als MSSP. Gaat Aanbestedende Dienst akkoord?	Het GGN SOC is en blijft verantwoordelijk voor governance, toezicht en is de escalation authority - zie hiervoor Bijlage K - Concept SLA MSSP.

321	Licenties	Graag ten aanzien van de volgende Managed Security Services (eis 64, 66, 68 - 70, 76 - 78, 82 en 83): a) bevestigen dat het om reeds bestaande oplossingen gaat die beheerd en gemonitord moeten worden; b) indien bestaand, aangeven om welke merk/type oplossingen het gaat.	A:) het gaat om reeds bestaande oplossingen die beheerd en gemonitord moeten worden. B:) 64: MS Defender for Endpoint, 66: MS Defender for Cloud Apps, 68: MS Entra ID Protection, 70: Guardian 360 en ZCert Vulnerability Scanner, 76: Sentinel, 77: Log Analytics en Logbuffet 2.5 (eigen ontwikkeling), 78: Splunk, 82: Thinks Canary, 83: Guardian 360 en ZCert Vulnerability Scanner.
322	Bijlage A - Programma van Eisen MSP en MSSP	Wat verwacht GGN precies qua dienstverlening van de volgende Managed Security Services: Threat Hunting (eis 67), Vulnerability Management (eis 70), Cyber Threat Intelligence (eis 71), en Functionele Log Monitoring (eis 78).	Aanbestedende Dienst is van mening dat deze definities standaard begrippen zijn uit Managed Security Services en heeft deze als zodanig eerder in de Marktconsultatie getoetst.
323	Bijlage A - Programma van Eisen MSP en MSSP	Wat is het verschil tussen eis 70 (Vulnerability Management) en eis 83 (Vulnerability Scanning Functionaliteiten / Voorzieningen)?	Eis 70 Vulnerability Management - dienst, het onder controle houden van kwetsbaarheden. Eis 83 betreft de voorzieningen voor het scannen op deze kwetsbaarheden.
324	Bijlage A - Programma van Eisen MSP en MSSP: Eis 73	Wie beheert nu de Splunk-omgeving en is het de verwachting van GGN, dat ook dit beheer door Inschrijver wordt overgenomen? Idem voor Logbuffet?	Beide SIEM-voorzieningen, dus ook de Splunk-omgeving zijn momenteel in eigen beheer bij Aanbestedende Dienst. Het is inderdaad de verwachting dat dit door inschrijver wordt overgenomen, idem voor logbuffet.
325	Bijlage A - Programma van Eisen MSP en MSSP: Eis 84	Op basis van de uitvraag lijkt GGN slechts een minimale on-premise IT-omgeving te hebben, alles bevindt zich in de cloud waar NDR nog nauwelijks toegepast wordt. Wat is de reden dat u toch een geïntegreerde NDR-oplossing uitvraagt en bent u bereid om deze eis te laten vallen?	Behoudens de fysieke Kantoor Infrastructuur-voorzieningen heeft Aanbestedende Dienst inderdaad geen on-premise IT-omgevind en bevindt alles zich in de cloud. Aanbestedende Dienst handhaaft deze eis maar stelt hierbij dat NDR in de XDR/ SIEM-oplossing mag zijn verwerkt.
326	Bijlage A - Programma van Eisen MSP en MSSP: Eis 84	Bedoelt GGN dat Opdrachtnemer een nieuwe technische NDR-oplossing levert en beheert die cyberdreigingen niet alleen kan detecteren, maar ook blokkeren? Of gaat het om IDS/IPS-functionaliteit op de bestaande (of nieuw te leveren?) firewalls die in beheer genomen moeten worden? Graag toelichten. Indien een nieuwe netwerksensor oplossing is bedoeld, dan ook graag aangeven op hoeveel locaties het netwerkverkeer gemonitord moet worden, de hoeveelheden netwerkverkeer en de beschikbare koppelvlakken (SPAN-poorten en hun interface snelheid) om dit netwerkverkeer af te tappen voor monitoring. Indien een nieuwe firewall oplossing bedoeld wordt, dan graag de daarvoor benodigde specs opgeven.	Behoudens de fysieke Kantoor Infrastructuur-voorzieningen heeft Aanbestedende Dienst inderdaad geen on-premise IT-omgevind en bevindt alles zich in de cloud. Aanbestedende Dienst handhaaft deze eis maar stelt hierbij dat NDR in de XDR/ SIEM-oplossing mag zijn verwerkt. In het kader van uw vraag worden de bestaande Firewalls bedoeld.
327	Bijlage A - Programma van Eisen MSP en MSSP: Eis 13 en 86	GGN geeft aan dat er alleen in overleg gebruik mag worden gemaakt van AI / LLM. In ons SOC gebruiken wij standaard SOAR-tooling die deze mogelijkheden juist benut om om false positives significant te verminderen en het analysewerk van veel voorkomende dreigingen van lagere prioriteit te vereenvoudigen zodat high-prio cases maximale aandacht kunnen krijgen. 1. Is dit toegestaan? 2. Waarom deze beperking, kunt u dat toelichten?	1. Aanbestedende Dienst is graag vooraf op de hoogte welke AI-tooling ingezet wordt, waar, met welk doel en onder welke voorwaarden. We verwachten met dit specifieke voorbeeld geen probleem. 2. We nemen graag onze verantwoordelijkheid bij de inzet van AI. Beoordeling/ selectie bij de poort voorkomt kwetsbaarheden achteraf.
328	Bijlage O - Prijzenblad	Wat is precies de bedoeling van prijsregel 136 waar een fee per gebruiker per maand ten behoeve van de 6 GGN-SOC medewerkers moet worden opgegeven? Welke kosten gaat het hier over en waarom hebben de betreffende GGN-SOC medewerkers toegang nodig tot het SIEM dat Opdrachtnemer gebruikt in haar dienstverlening?	Dit betreft een prijsregel die u kunt invullen indien u licentiekosten in rekening brengt voor toegang tot het SIEM voor de SOC-medewerkers van Aanbestedende Dienst. Aanbestedende Dienst neemt deze voorziening mee uit oogpunt Trust but Verify.
329	Nvl-1: Vraag 42	GGN lijkt hier te eisen dat loginformatie minimaal 5 jaar bewaard wordt. Hoe verhoudt zich dit t.o.v. de veel kortere retentietijden die genoemd worden bij het antwoord op vraag 88?	Er is verschil tussen bewaartermijnen (SOC) en bwaartermijnen Back-up.
330	Nvl-1: Vraag 143 (en 212)	Kan GGN bevestigen dat de genoemde overdracht naar de opvolgende partij niet geldt voor de standaard use cases, dashboards, playbooks, rapportages en dergelijke die Opdrachtnemer ontwikkeld heeft voor al haar Managed Security Services klanten? (Alles wat specifiek voor GGN ontwikkeld is, wordt uiteraard wel volledig overgedragen bij exit.)	Het betreft hier overdracht van use cases, dashboards, playbooks, rapportages en dergelijke die Opdrachtnemer beschikbaar heeft gemaakt dan wel ontwikkeld heeft voor Aanbestedende Dienst.
331	Nvl-1: Vraag 198	Beschikt GGN naast de Microsoft E3-licentie over de Security Add-on die security monitoring op E5-licentie niveau mogelijk maakt? Zo niet, kunt u dan vereisen dat deze in elke aanbieding wordt meegenomen? Dat biedt iedere aanbieder gelijke kansen en deze uitbreiding is nodig om serieuze security monitoring op Microsoft te kunnen uitvoeren, bijvoorbeeld op Defender for Endpoint/Server.	Ja, Aanbestedende Dienst beschikt al over de Security E5 add-on.
332	Nvl-1: Vraag 248	'Aansturing van de MSSP zal in eerste instantie door het eigen SOC van aanbestedende dienst geschieden' Hoe ziet dit er volgens GGN in de praktijk precies uit? Met andere woorden, hoe werkt het MSSP-SOC samen met het GGN-SOC zolang de laatste nog niet volledig is omgevormd tot G-SOC?	De interne samenstelling (rollen, verantwoordelijkheden en daarbij behorende personen) van het GGN-eigen SOC zal komende tijd worden aangepast. Aanbestedende Dienst stelt zich hierbij voor dat eerst op inhoud wordt samengwerkt en dat in overleg met de MSSP Aansturing en Uitvoering worden afgestemd.

333	Nvl-1: Vraag 253	Waar zet GGN de applicatie Guardian360 precies voor in? Met andere woorden, welke security functionaliteit biedt Guardian360 aan GGN?	Aanbestedende Dienst gebruikt Guardian360 voor vulnerability scans op websites en webapplicaties die eigendom zijn van GGN of waarvan GGN gebruik maakt. Dit zodat zei tijdig kwetsbaarheden detecteren en dit rapporteren aan de eigenaar van de website of webapplicatie.
334	Bijlage K	De Aanbestedende Dienst wil gebruikmaken van GIBIT 2023, echter onder artikel 1.4 bijlage K wordt verwezen naar compliance met de GIBIT 2025. Gezien het tijdstip van publicatie van de aanbestedingsdocumenten lijkt het erop dat de Aanbestedende Dienst wil verwijzen naar de GIBIT 2023-voorwaarden. Kunt u dit bevestigen?	Het betreft hier inderdaad de GIBIT 2023 voorwaarden.
335	Bijlage B,D,K, Nvl 1, vraag 129,130	In de aanbestedingsstukken constateert Inschrijver de volgende tegenstrijdigheden met betrekking tot aansprakelijkheid: 1.Bijlage K (juridisch addendum): In Bijlage K wordt bepaald dat de MSSP aansprakelijk is voor directe schade veroorzaakt door nalatigheid tot een maximum van [bedrag], waarbij aansprakelijkheid voor indirecte schade in beginsel is uitgesloten, met uitzondering van gevallen van grove nalatigheid. 2.Bijlage D: In de GIBIT worden aansprakelijkheidsbepalingen opgenomen die bijvoorbeeld geen indirecte schade uitsluiten. 3.Bijlage B: In Bijlage B wordt wederom een afwijkend aansprakelijkheidsartikel opgenomen, waarmee ook weer wordt afgeweken van bijlage D en K. 4.Nota van Inlichtingen (vraag 129/130): In de beantwoording van vraag 129/130 geeft de Aanbestedende Dienst aan dat indirecte schade niet wordt uitgesloten. Dit staat echter haaks op het juridisch addendum in Bijlage K, waarin uitsluiting van indirecte schade als uitgangspunt wordt gehanteerd, met uitzondering van gevallen van grove nalatigheid. Gelet op het bovenstaande verzoekt Inschrijver de Aanbestedende Dienst: 1.De geconstateerde tegenstrijdigheden tussen Bijlage K, Bijlage B en de GIBIT te verhelpen door één eenduidige en consistente aansprakelijkheidsregeling op te nemen in de aanbestedingsstukken.	Bijlage K, het juridisch addendum is correct, : In Bijlage K wordt bepaald dat de MSSP aansprakelijk is voor directe schade veroorzaakt door nalatigheid tot een maximum, waarbij aansprakelijkheid voor indirecte schade in beginsel is uitgesloten, met uitzondering van gevallen van grove nalatigheid.
336	Bijlage B en D	Artikel 25.1 van de Overeenkomst bepaalt dat de Opdrachtgever de Overeenkomst te allen tijde kan opzeggen op grond van artikel 7:408 BW. Artikel 24.2 van de GIBIT bepaalt echter uitdrukkelijk dat artikel 7:408 lid 1 BW niet van toepassing is. De GIBIT wordt gezien als een proportioneel samenstel van voorwaarden. Daarom acht Inschrijver het risico op tussentijdse opzegging dermate groot dat zij dit als disproportioneel beschouwt, zoals vastgelegd in de Overeenkomst. Kan de Aanbestedende Dienst bevestigen dat zij aansluit bij de in de GIBIT vastgelegde opzeggingsregeling? Zo nee, kan de Aanbestedende Dienst dit nader toelichten?	Indien er gegronde redenen zijn, zoals bijvoorbeeld aanhoudende wanprestatie, kan de Opdrachtgever op basis van artikel 7 in de Overeenkomst de Overeenkomst opzeggen. Uiteraard zal Opdrachtgever, omwille van de continuiteit van de bedrijfsvoering, hier niet zo maar toe overgaan. Daarvoor zit in de praktijk nog een uitgebreid escalatie pad.
337	Bijlage B en Nvl 1 vraag 172	In Nvl 1 (vraag 172) heeft de Aanbestedende Dienst gesteld dat er ruimte bestaat om te onderhandelen over het schadebedrag in de GIBIT. Echter, artikel 19 van de Overeenkomst bevat reeds uitdrukkelijk vastgestelde schadebedragen. Gelet op het feit dat de Overeenkomst prevaleert boven de GIBIT, gaat Inschrijver ervan uit dat de schadevergoedingsregeling in de Overeenkomst is vastgelegd. Op grond daarvan stelt Inschrijver voor om de aansprakelijkheidsbedragen in een verhouding van 1:2 op te nemen in de Overeenkomst. Kunt u dit bevestigen?	Ja, de Overeenkomst prevaleert hier boven de Algemene voorwaarden.

338	Bijlage D, E en Nvl 1	De Aanbestedende Dienst hanteert de GIBIT 2023 als standaard inkoopvoorwaarden en heeft aangegeven in Nvl 1 dat deze in principe niet onderhandelbaar zijn. Voorgestelde wijzigingen door inschrijvers worden derhalve niet geaccepteerd. Dit standpunt lijkt echter op gespannen voet te staan met twee andere punten van de Aanbestedende Dienst: 1.De Aanbestedende Dienst heeft zelf een Addendum opgesteld waarin wordt afgeweken van de GIBIT 2023. Dit roept de vraag op waarom afwijkingen door de Aanbestedende Dienst zelf wel mogelijk zijn, maar voorgestelde wijzigingen door inschrijvers niet worden geaccepteerd. Is dit standpunt redelijk en proportioneel te noemen in het kader van een aanbestedingsprocedure? 2.Daarnaast geeft de Aanbestedende Dienst aan dat inschrijvers gewenste afwijkingen ten aanzien van de GIBIT kunnen voorleggen in de vragenronde. Dit staat echter haaks op het eerder ingenomen standpunt dat de GIBIT in principe niet onderhandelbaar is. Kan de Aanbestedende Dienst verduidelijken hoe deze punten zich tot elkaar verhouden en op welke wijze inschrijvers daadwerkelijk aanspraak kunnen maken op de geboden onderhandelingsruimte?	De reden voor het Addendum staat vermeld in het Addendum. Deze voorwaarden zijn in principe niet onderhandelbaar, bij uitzondering wijken we hier, in specifieke situaties soms van af, zoals in het geval van een Addemdum voor alle ICT opdrachten van GGD GHOR Nederland. Indien er in een uitzonderlijke situatie specifieke zaken moeten worden aangepast is dit bespreekbaar gedurende de Nvl vraag en antwoord fase.
339	Vraag 132 Nvl 1	In de beantwoording van vraag 141 wordt niet expliciet bevestigd noch ontkend dat audits uitsluitend mogen worden uitgevoerd door een partij die geen concurrent is van de Inschrijver. Kan de Aanbestedende Dienst alsnog bevestigen dat de door haar in te schakelen derde partijen voor het uitvoeren van audits geen organisaties mogen zijn die als concurrent van de Inschrijver kunnen worden aangemerkt?	Aanbestedende Dienst heeft zelf een Team Audit & Compliance en Audits worden te allen tijde uitgevoerd door daartoe geaccrediteerde functionarissen of organisaties: functionarissen en organisaties die gespecialiseerd zijn in audits en zelf aantoonbaar geen belang hebben bij het resultaat van betreffende Audits. Aanbestedende Dienst acht de kans daarom uitermate klein tot uitgesloten dat een concurrerende MSP of MSSP zal worden aangewend voor een Audit op haar MSP of MSSP.
340	(Vraag 116 Nvl 1)	Kan de Aanbestedende Dienst bevestigen dat, wanneer persoonsgegevens buiten de Europese Economische Ruimte (EER) worden verwerkt en de verwerker aantoonbaar voldoet aan de voorwaarden van artikel 45 of 46 AVG en de verwerkingsverantwoordelijke hiervan voorafgaand schriftelijk op de hoogte stelt, dit voldoende is conform artikel 4.3 van de Verwerkersovereenkomst?	Met inachtneming van een mogelijkheid tot bezwaar en bijbehorende bezwaartermijn, ja.
341	Bijlage B	Artikel 16 lid 2 sub c Overeenkomst, deze bepaling lijkt niet te vallen binnen de uitzonderingsgronden zoals opgenomen in artikel 18.1 van de GIBIT, welke limitatief bepaalt dat vertrouwelijke informatie uitsluitend openbaar gemaakt mag worden indien: een wettelijk voorschrift daartoe verplicht, een bevoegde toezichthouder of rechter dan wel een door partijen aangewezen geschillenbeslechter daartoe verplicht, of bekendmaking noodzakelijk is voor de uitvoering van de overeenkomst of voor intern beraad. Artikel 16 lid 2 sub c valt buiten deze limitatieve uitzonderingen en is daarmee strijdig met artikel 18.1 GIBIT. Inschrijver wenst dat uitsluitend vertrouwelijke informatie met derden wordt gedeeld na voorafgaande schriftelijke toestemming. De in artikel 16.2 sub c genoemde uitzondering is daarom ook onacceptabel. Inschrijver verzoekt de Aanbestedende Dienst uitdrukkelijk om uitsluitend aan te sluiten bij de regeling zoals vastgelegd in artikel 18.1 van de GIBIT. Kunt u dit bevestigen?	Correct, hier sluiten we aan bij GIBIT artikel 18.1. De Overeenkomst wordt hierop aangepast bij ondertekening.
342	Bijlage B artikel 17.1	Kunt u bevestigen dat de verwijzingen naar de verschillende wet- en regelgeving uitsluitend gelden voor zover deze daadwerkelijk van toepassing zijn op Inschrijver? Kunt u daarbij tevens bevestigen dat de Aanbestedende Dienst zelf ook alle op haar van toepassing zijnde wet- en regelgeving zal naleven?	De Aanbestedende Dienst is net als Inschrijver gehouden aan alle van haar op toepassing zijnde wet- en regelgeving.
343	Bijlage B artikel 5.5 en 5.6	Het lijkt erop dat hier sprake is van een omissie, waarbij onduidelijkheid bestaat over de verhouding tot het Landelijk Elektronisch Patiëntendossier voor Seksuele Gezondheid. Kan de Aanbestedende Dienst dit nader verduidelijken?	Dit is inderdaad een omissie in een standaard contract. Hier komt de onderhavige opdracht te staan.
344	Eis 75 en Nvl vraag 88	1. Kunt u aangeven welke specifieke norm prevaleert bij eventuele tegenstrijdigheid? 2. In eis 75 wordt verwezen naar het actuele informatiebeveiligingsbeleid van GGN als aanvullende norm voor logging in de zorg, echter heeft de Aanbestedende Dienst dit document niet beschikbaar gesteld in de aanbestedingsdocumenten. Kan de Aanbestedende Dienst dit document alsnog beschikbaar stellen of deze aanvullende norm laten vallen?	Ja - Aanbestedende Dienst heeft hiertoe Bijlage X en Bijlage Y op TenderNed beschikbaar gemaakt.

345	Bijlage W en prijzenblad	In bijlage W geeft u de aantallen van uw licenties weer. Hierbij zijn er grote verschillen in de aantallen licenties die u afneemt. In het prijzenblad vraagt u uit voor 300 gebrukers. A) Moet inschrijver alle licenties in bijlage W aanhouden voor 300 gebruikers? B) Moet inschrijver alle aantallen licenties zo houden en het totaal verdelen over 300 gebruikers? C) Waar meer dan 300 licenties nu worden gebruikt, moet inschrijver deze beperken tot 300 licenties? D) U maakt waarschijnlijk gebruik van de constructie om 1 A5 licentie af te nemen om hiermee het gebruik van Sentinel mogelijk te maken. Hierdoor ontstaan wel functionele gaps. Moet inschrijver de A3 licenties aanhouden, of dienen alle A3 licenties reeds nu in de beantwoording vervangen te worden door A5 licenties?	Bijlage W geeft de huidige aantallen aan maar doet geen uitspraak over de toekomstige aantallen. U dient daarom in het prijzenblad de te prijzen posten aan te houden in kolom F, welke dan automatisch worden doorgerekend naar een jaarsom. Uit de eerdere Marktconsultatie heeft het merendeel van de deelnemers geadviseerd deze functionele prijsindeling per gebruiker aan te houden. U kunt hierbij uitgaan van A5 licenties.
346	Beschrijvend document	Kunt u beschrijven welke activiteiten inschrijver dient uit te voeren voor "Beheer Fysieke Werkplekken van de medewerkers "?	De hardware lifecycle, uitgifte en inname van de Fysieke Werkplekken geschiedt door ons zelf op kantoor. Al het overige valt onder Beheer Fysieke Werkplekken.
347	Antwoord op vraag 106, 219 en 232 Nvl 1	Wij willen u erop wijzen dat het beheer van fysieke print devices (inclusief onderhoud, vervanging en supplies) in de markt doorgaans wordt belegd bij gespecialiseerde print-/MPS-contracten en daarmee wezenlijk afwijkt van generieke managed services. Om die reden adviseren wij u om: het beheer, onderhoud, vervanging en levering van verbruiksartikelen voor print devices expliciet buiten scope van deze aanbesteding te plaatsen; en de scope te beperken tot het technisch applicatiebeheer van de Printix printmanagementsoftware (bijvoorbeeld hosting, configuratie en eerstelijns support). Kunt u bevestigen dat: De fysieke print devices (inclusief onderhoud, vervanging en supplies) buiten scope van deze aanbesteding vallen? De Opdrachtnemer uitsluitend verantwoordelijk is voor het beheer van de printmanagementsoftware en de bijbehorende integraties? Eventuele toekomstige vervanging van print devices via een separaat contract of aanbesteding zal plaatsvinden?	Aanbestedende Dienst heeft momenteel een contract met Veenman voor de huur van de printers, remote beheer en de mogelijkheid om supplies te bestellen en geleverd te krijgen. Dit contract loopt net als de contracten voor managed services af in december 2026. Aanbestedende Dienst heeft in het PvE de eis gesteld dat deze voorzieningen eerst as-is in (remote) beheer moeten worden genomen, waarbij na einde contract met Veenman het 'Managed Printen en Reproductie' volledig door Inschrijver wordt verzorgd. Het staat Inschrijver vrij om dit ten behoeve van Aanbestedende Dienst bij bijvoorbeeld Veenman of andere leverenciers te betrekken. Voor aantallen en specificaties zie Nota van Inlichtingen 1.
348	Antwoord op vraag 106, 219 en 232 Nvl 1	In uw antwoord op vraag 106 bevestigt u dat alle nieuw aan te schaffen hardware buiten scope valt. In uw antwoord op vraag 232 geeft u aan dat u op dit moment gebruik maakt van print devices van Veenman en Printix voor secure Cloud Print Management. Hierbij geeft u ook aan dat de verwachting ten aanzien van de Inschrijver is dat deze de printvoorzieningen as-is in beheer overneemt, waarna u de overeenkomst met de huidige leverancier kunt beëindigen en vanaf dat moment zowel de devices als het Cloud Print Management als dienst worden afgenomen van Opdrachtnemer. Wij constateren dat hier mogelijk sprake is van een discrepantie tussen beide antwoorden. Kunt u verduidelijken wat u exact verstaat onder “printvoorzieningen”? Beperkt dit zich tot de Printix printmanagementsoftware en bijbehorende configuratie/integratie? Of omvat dit tevens de fysieke print devices (zoals printers en multifunctionals)? Indien u ook de fysieke print devices onder de printvoorzieningen schaart, verzoeken wij u de volgende punten te verduidelijken: Hoe verhoudt dit zich tot uw antwoord op vraag 106, waarin u aangeeft dat (nieuwe) hardware buiten scope valt? Betekent dit dat de Opdrachtnemer verantwoordelijk wordt voor lifecycle management van deze devices (inclusief onderhoud, storingen, vervanging en verbruiksartikelen zoals toner)? Zo ja, kunt u aangeven welke volumes, typen devices, contractuele verplichtingen en huidige SLA’s hierbij van toepassing zijn?	Aanbestedende Dienst heeft momenteel een contract met Veenman voor de huur van de printers, remote beheer en de mogelijkheid om supplies te bestellen en geleverd te krijgen. Dit contract loopt net als de contracten voor managed services af in december 2026. Aanbestedende Dienst heeft in het PvE de eis gesteld dat deze voorzieningen eerst as-is in (remote) beheer moeten worden genomen, waarbij na einde contract met Veenman het 'Managed Printen en Reproductie' volledig door Inschrijver wordt verzorgd. Het staat Inschrijver vrij om dit ten behoeve van Aanbestedende Dienst bij bijvoorbeeld Veenman of andere leverenciers te betrekken. Voor aantallen en specificaties zie Nota van Inlichtingen 1

349	Hardware printers en copiers	In paragraaf 2.2 Out of Scope geeft u aan dat de levering van hardware buiten scope is geplaatst. In tegenspraak daarop begrijpen wij uit het antwoord op vraag 222 van de Nvl dat u de printer en copier hardware van de Inschrijver wenst te betrekken. Dit is zeer specifieke expertise met eigen klantwensen. Inschrijver adviseert de hardware van printers en copiers bij een specifieke leverancier te blijven betrekken incl. service. Hierbij verzorgt GGD-GHOR de regie functie. Neemt u dit advies over?	Aanbestedende Dienst heeft momenteel een contract met Veenman voor de huur van de printers, remote beheer en de mogelijkheid om supplies te bestellen en geleverd te krijgen. Dit contract loopt net als de contracten voor managed services af in december 2026. Aanbestedende Dienst heeft in het PvE de eis gesteld dat deze voorzieningen eerst as-is in (remote) beheer moeten worden genomen, waarbij na einde contract met Veenman het 'Managed Printen en Reproductie' volledig door Inschrijver wordt verzorgd. Het staat Inschrijver vrij om dit ten behoeve van Aanbestedende Dienst bij bijvoorbeeld Veenman of andere leverenciers te betrekken. Voor aantallen en specificaties zie Nota van Inlichtingen 1.
350	Hardware laptops en Desktop PC's	In paragraaf 2.2 Out of Scope geeft u aan dat de levering van hardware buiten scope is geplaatst. Wij nemen aan dat de laptop en desktop PC's door GGD-GHOR worden aangeschaft en ook reparaties en vervanging door GGD-GHOR wordt verzorgd. Klopt deze aanname?	Dat is correct. De hardware lifecycle, uitgifte en inname van de Fysieke Werkplekken geschiedt door ons zelf op kantoor. Al het overige valt onder Beheer Fysieke Werkplekken.
351	Antwoord op vraag 101 Nvl 1	Op de vraag voor het aantal netwerkcomponenten wordt geantwoord dat er 4 switches en 25 AP's zijn van Unify. Wat zijn de typenummers van de switches en de AP's en wat is de leeftijd van de apparatuur?	U mag er hierbij van uitgaan dat dit technisch en economisch actuele apparatuur is welke remote te beheren zijn.
352	Antwoord op vraag 92 Nvl 1	Op de vraag voor het aantal netwerkcomponenten wordt geantwoord dat er 2 Fortigate firewalls in gebruik zijn. Wat is het typenummer van deze firewalls, de leeftijd en welke software bundel is actief op de firewall?	U mag er hierbij van uitgaan dat dit technisch en economisch actuele apparatuur is welke remote te beheren zijn.
353	Antwoord op vraag 92 Nvl 1	Op de vraag voor het aantal netwerkcomponenten wordt geantwoord dat er 2 Fortigate firewalls in gebruik zijn. Is dit een firewall cluster op de locatie in Utrecht? Of is dit een firewall op locatie en een firewall binnen Microsoft Azure?	Er is 1 fysieke Fortigate forewall op het Zwarte woud (okt 2025 geplaatst). en 1 virtuele firewall in Azure
354	Antwoord op vraag 219 en 232 Nvl 1	In de markt is het gebruikelijk dat de IT-dienstverlener verantwoordelijk is voor de technische aansturing en integratie vanuit de werkplekomgeving, terwijl de fysieke apparaten, onderhoud, reparaties en verbruiksmaterialen normaliter worden geleverd door een gespecialiseerde printer- en kopieerleverancier. Welke werkzaamheden en diensten verwacht de aanbestedende dienst van de inschrijver naast de technische aansturing en de integratie vanuit de werkplekomgeving?	Aanbestedende Dienst heeft momenteel een contract met Veenman voor de huur van de printers, remote beheer en de mogelijkheid om supplies te bestellen en geleverd te krijgen. Dit contract loopt net als de contracten voor managed services af in december 2026. Aanbestedende Dienst heeft in het PvE de eis gesteld dat deze voorzieningen eerst as-is in (remote) beheer moeten worden genomen, waarbij na einde contract met Veenman het 'Managed Printen en Reproductie' volledig door Inschrijver wordt verzorgd. Het staat Inschrijver vrij om dit ten behoeve van Aanbestedende Dienst bij bijvoorbeeld Veenman of andere leverenciers te betrekken. Voor aantallen en specificaties zie Nota van Inlichtingen 1
355	Antwoord op vraag 219 en 232 Nvl 1	Kunt u aangeven welke vorm van overeenkomst de Aanbestedende Dienst heeft afgesloten met Veenman voor de levering en het beheer van de printer- en kopieeromgeving (koop, lease, huur)?	Huur, full operational.
356	prijzenblad, bijlage O	U vraagt in regel 151 een maandprijs voor een CSIRT. In de tenderdocumenten vinden we geen enkele wens of eis over CSIRT. Wij gaan er daarom van uit dat een CSIRT out of scope is. Kunt u dit bevestigen?	Tijdens de Marktconsultatie heeft het merendeel van de deelnemers aangegeven de mogelijkheid om een Computer Security Incident Respons Team als vast onderdeel van de reguliere Managed Security Services te bieden. Indien dit vast onderdeel is van uw Managed Security Services dan kunt de prijsstelling / retainer fee op deze regel vermelden.
357	prijzenblad, bijlage O	In de aanbestedingsdocumenten wordt niet gespecificeerd welke eisen GGD GHOR stelt aan de Threat Intelligence (TI) feeds die onderdeel uitmaken van de MSSP-dienstverlening. TI-feeds kunnen gratis of betaald zijn, waarbij een kostengedreven keuze voor gratis feeds mogelijk tot kwaliteitsverschillen tussen inschrijvers kan leiden. Kunt u aangeven welke verwachtingen, kwaliteitscriteria of minimale eisen GGD GHOR hanteert voor TI-feeds, zodat alle inschrijvers dezelfde uitgangspunten hanteren en er een gelijk speelveld ontstaat?	Aanbestedende Dienst bedoelt met de Prijsregel Threat Intelligence Feeds uitsluitend 'Betaalde feeds' - de kosten per feed die Inschrijver in rekening brengt om deze feed beschikbaar te maken.
358	prijzenblad, bijlage O	In het prijzenblad (Bijlage O) wordt in veld C127 het onderdeel 'nulmeting / Security Assessment' genoemd. In de aanbestedingsdocumenten kunnen wij echter geen nadere toelichting of definitie van dit onderdeel vinden. Kunt u aangeven wat GGD GHOR onder deze nulmeting / Security Assessment verstaat, welke scope en diepgang wordt verwacht, en hoe deze zich verhoudt tot de Due Diligence-activiteiten die elders in de stukken zijn benoemd?	De prestaties van de MSSP worden in KPI's (SLA en DAP) overeengekomen. Met de Nulmeting / Security Assessment - regel geeft Aanbestedende Dienst u de mogelijkheid om het gezamenlijk vaststellen van de Baseline (startpunt KPI"s) in te prijzen.

359	Antwoord op vraag 228 Nvl 1	In het antwoord op vraag 228 geeft u aan dat uw huidige provider van Zakelijke telecom Odido is. Mogen wij als inschrijver ervan uitgaan dat u met Odido heeft afgestemd dat de winnende inschrijver het beheer van de zakelijke telecom mag overnemen en Inschrijver toegang krijgt tot de beheerportalen? Verwacht u dat inschrijver ook de Odido dienstverlening in facturatie neemt?	Aanbestedende Dienst heeft momenteel een contract met Odido voor Zakelijke telecommunicatie. Dit contract loopt per december 2026 af. Aanbestedende Dienst heeft in het PvE de eis gesteld dat deze voorzieningen eerst as-is in (remote) beheer moeten worden genomen, waarbij na einde contract met Odido de Zakelijke Telecommunicatievoorzieningen (met uizondering van de Abonnementen) volledig door Inschrijver worden verzorgd. Het staat Inschrijver vrij om dit ten behoeve van Aanbestedende Dienst bij bijvoorbeeld Odido of andere leveranciers te betrekken.
360	Programma van eisen	In eis 68 wordt gevraagd dat de opdrachtnemer het geheel van Identity & Access Management (IAM, middels Entra-ID) als Managed Security Service verzorgt. Onze dienstverlening kent een strikte scheiding tussen MSP en MSSP, conform de aanbestedingseisen. IAM-beheer leveren wij vanuit onze MSP-dienst, terwijl de security-specifieke controls, monitoring en optimalisatie binnen onze MSSP-dienst vallen. Is deze verdeling – waarbij functioneel en technisch IAM-beheer onder MSP valt, en de beveiligingsaspecten binnen MSSP worden uitgevoerd – acceptabel binnen de interpretatie van eis 68?	Uw aangegeven verdeling is akkoord. 1- interne IAM: dit is dus Entra/ azure ad / enterprise app etc valt onder MSP/ is dus gebruikersbeheer / groepen /rollen/ enterprise appps/ claims/ attributen/ certificaten/ MFA/ etc.. 2- Governance en compliance: Dit is meer regie en iam beleid en auditing. Dit moet intern blijven. 3- MSSP is vooral: Monitoring / datalekken/ incident mbt security/ etc.
361	G1. Implementatie en uitrolplan	U schrijft in de vraagstelling: 'Wordt er gewerkt met een Minimal Viable Product waarvoor een zo kort mogelijke doorlooptijd benodigd is en/of is er een indeling in geplande sprints?' Deze vraagstelling suggereert dat u een bouw/implementatie verwacht, terwijl het begrip "inbeheername" het in beheer nemen van een bestaande situatie suggereert. Wilt u nader toelichten hoe u dit ziet?	Voor Aanbestedende Dienst is het belangrijk dat de dienstverlening van de MSP en MSSP dusdanig ver is ingericht, dat met vertrouwen afscheid kan worden genomen van de huidige leveranciers (vanwege aflopen contracten). In dat kader wordt het Minimal Viable Product bedoeld. Er is in de stukken nergens sprake van een bouwplan. Onder Implementatie verstaat Aanbestedende Dienst het geheel van activiteiten (due dilligence, inbeheername) om dit mogelijk te maken.
362	Eis 24 en eis 56	U geeft in de eisen 24 en 56 de fasering aan. Verwacht u de beschrijving van de fase 'b. Definitie- en Planningsfase' in G1 of in G2? Verwacht u de beschrijving van de fase 'c. Uitvoer- en optimalisatiefase' in G1 of in G2?	Waarschijnlijk wordt hier vraag 24 en 55 bedoeld. Aanbestedende Dienst wil met deze fasering duidelijk maken dat éérst op basis van de as-is situatie in beheer moet worden genomen, alvorens er grote veranderingen/ verbeteringen e.d. kunnen worden doorgevoerd. Aanbestedende Dienst ondergaat grote veranderingen, de veranderingen en/ of verbeteringen van de managed services en managed security services moeten deze kunnen volgen. Inschrijver wordt verwacht zich aande vraagstelling in G1 en G2 te houden en hierbij rekening te houden met hetgeen in het Programma van Eisen wordt gesteld.
363	Eis 24 en eis 55	U geeft in de eisen 24 en 55 de fasering en het werken met backlogs aan. Is uw beeld dat we tijdens de uitvoering van de dienstverlening blijvend werken met backlogs om zo doorlopend te blijven optimaliseren? Of ziet u de realisatie van de backlogs als een tijdelijke 'transformatie-fase'?	Aanbestedende Dienst werkt intern Prince2Agile en hanteert momenteel voor alle veranderingen en verbeteringen (Changes) een gestructureerde Backlog (zowel voor MSP als MSSP) welke worden beheerd door Product Owners. De verwachting is dat ook in de nieuwe situatie alle veranderingen en verbeteringen (Changes) zo door Aanbestedende Dienst intern gemanaged zullen worden. Het spreekt voor zich dat Aanbestedende Dienst haar interne werkwijze afstemt met de service management processen van Opdrachtnemer.
364	Programma van eisen	in eis 66 staat dat de Opdrachtnemer de rol van Cloud Access Security Broker (CASB) invult voor de beveiliging van externe cloudapplicaties. In de aanbestedingsdocumenten is echter geen informatie opgenomen over de huidige CASB-inrichting of bestaande usecases. Kunt u aangeven: Welke CASB-functionaliteit GGD GHOR Nederland momenteel reeds inzet (indien aanwezig), en welke beleidsregels of usecases daarbij horen?	In Nota van Inlichtingen 1 vindt u (vraag 225) de specificaties van de SOC/SIEM voorzieningen. Eis 66 gaat echter over de ROL van CASB ten behoeve waarvoor de beleidsregels in overleg worden gedeeld.

365	prijzenblad, bijlage O	Kunt u bevestigen of de genoemde tarieven voor Junior, Medior en Senior Security Specialist bedoeld zijn als respectievelijke equivalenten van Tier 1-, Tier 2- en Tier 3-SOC-analisten, of dat u deze functieniveaus op een andere manier bedoeld heeft? Indien een andere interpretatie wordt gehanteerd, ontvangen wij graag een korte toelichting, zodat inschrijvers hun inzet en kostencalculatie correct kunnen afstemmen op uw verwachtingen.	De niveaus Junior, Medior en Senior zijn opgenomen met als doel ruimte te geven voor verschillende tarieven op basis van kennis- en ervaringsniveau en hangen niet samen met de Tier-niveaus.
366	G4.Kansendossier MDIS	Hoeveel processen/pipelines zijn operationeel en met welke diversiteit?	U kunt hierbij uitgaan van 12 processen/ pipelines welke zijn onderverdeeld naar leden-processen (GGD's en GHOR's), bedrijfvoeringsprocessen en externe bronnen.
367	G4.Kansendossier MDIS	Hoeveel tabellen heeft de databases van het huidige Data Intelligence service ongeveer?	U kunt hierbij uitgaan van 300 tabellen.
368	G4.Kansendossier MDIS	Hoeveel brontabellen/bronbestanden worden ongeveer verwerkt binnen de huidige Data Intelligence Service?	U kunt hierbij uitgaan van 120 brontabellen/bronbestanden.
369	G4.Kansendossier MDIS	Hoeveel bronsystemen worden ongeveer ontsloten door de huidige Data Intelligence Service?	U kunt hierbij uitgaan van 12 bronsystemen.
370	G4.Kansendossier MDIS	Wat is de huidige architectuur van de Data Intelligence Service?	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.
371	G4.Kansendossier MDIS	Hoeveel tijd besteedt uw Team Data Intelligence gemiddeld per week/maand aan beheeractiviteiten (incidenten, problems, changes/releases, autorisatiebeheer, ...)	Op dit moment betreft dit 1 FTE manager, 1 FTE product owner, 1 FTE projectmanager, 3 FTE Bi specialisten en 1 FTE informatiemanager.
372	G4.Kansendossier MDIS	Hoeveel incidenten zijn er ongeveer per maand?	U kunt hierbij uitgaan van 10 incidenten.
373	G4.Kansendossier MDIS	Wat is het huidige datavolume en hoe snel groeit dat ongeveer?	U kunt hierbij uitgaan van 500 Gb.
374	G4.Kansendossier MDIS	Welke datamodelleringsaanpak (bijvoorbeeld Kimball, Inmon, Data Vault) is toegepast bij de ontwikkeling?	U kunt hierbij uitgaan van Data Vault in Power BI.
375	G4.Kansendossier MDIS	Hoeveel dashboards/rapportages zijn er ongeveer?	U kunt hierbij uitgaan van 69 dashboards.
376	Bijlage K - Concept Service Level Agreement MSSP GGD GHOR Nederland	Bijlage K – Concept SLA MSSP bevat in §1.6 een uitgebreide beschrijving van de scope van de MSSP-dienstverlening (waaronder threat detection, incident response, security governance, assessments, awareness en consultancy). Deze scope is anders dan de eisen uit het Programma van Eisen. Inschrijver gaat er van uit dat het Programma van Eisen leidend is en de beschrijving in het template Bijlage K uitsluitend als voorbeeld is bedoeld en in lijn wordt gebracht tijdens de implementatie van de dienstverlening. Kunt u dit bevestigen?	Het PvE is hierin leidend, SLA is een nadere uitwerking daarvan waarin wordt aangegeven wat de minimum service level requirements zijn.
377	Programma van eisen	Voor eis 87 doen wij de aanname dat de werkzaamheden rondom consultancy, training en advies — die uitsluitend op aanvraag en in overleg met Opdrachtgever worden uitgevoerd — niet binnen de vaste MSSP-dienstverlening fee vallen. Graag ontvangen wij bevestiging dat de kosten voor deze werkzaamheden separaat, op basis van uurtarieven, aan Opdrachtgever mogen worden doorbelast.	Correct, werkzaamheden rondom consultancy, training en advies, die uitsluitend op aanvraag en in overleg met Opdrachtgever worden uitgevoerd, vallen niet binnen de vaste MSSP-dienstverlening fee.

378	Programma van eisen	In relatie tot eis 84 verzoekt Inschrijver om nadere toelichting op de huidige inrichting van NDR/IDS/IPS binnen het GGD GHOR-domein. De aanbestedingsdocumenten beschrijven geen bestaande oplossing, tooling, netwerkdekking of operationele status. Kunt u aangeven: Hoe de huidige NDR/IDS/IPS-voorziening is ingericht (technologie, leveranciers, integraties, dekking van netwerksegmenten, koppelingen met SIEM/SOC)? Of de bestaande oplossing volledig operationeel is, of dat er op dit moment onderdelen ontbreken of nog te realiseren elementen op de backlog staan? Welke minimale functionele en technische eisen GGD GHOR verwacht dat de nieuwe geïntegreerde NDR/IDS/IPS-oplossing moet overnemen of verbeteren ten opzichte van de huidige situatie?	Deze Eis 84 verschilt inde formulering. Aanbestedende Dienst heeft hiervoor momenteel nog geen voorzieningen en heeft deze voorziening daarom in het Programma van Eisen opgenomen (Opdrachtnemer levert..). Het gaat dut niet om een as-is inbeheername.
379	Programma van eisen	In NVI-1, vraag 225 wordt gevraagd naar de huidige inrichting van vulnerability management. Echter blijft onduidelijk wat de beoogde scope van vulnerability management binnen deze aanbesteding is. Kunt u toelichten: Welke onderdelen precies binnen scope vallen (bijv. alleen MSP/MSSP-componenten of is het meer) Welke verwachtingen GGD GHOR heeft ten aanzien van tooling, opvolging, prioritering en rapportage? tevens de vraag hoe verwacht men dat dit in het prijzenblad verwerkt?	Het Vulnerability Management is ingericht middels Ms-Defender. Eis 70 betreft de Dienstverlening hieromtrent, Eis 83 betreft de voorziening. Uit de Marktconsultatie hebben wij geleerd / geadviseerd gekregen hiervoor een algemeen prijsitem voor de dientverlening op te nemen in de vorm van een vaste fee per maand. Deze vindt u in het Prijzenblad: Security Monitoring & Triage. U dient de kosten voor Vulnerability Management in deze fee mee te nemen.
380	Beschrijvend document	Op pagina 9 heeft u in de Aanleiding een verwijzing naar IV-voorzieningen. Wij interpreteren deze alinea als volgt: A) GGD GHOR neemt zelf de regierol als Functionele Regie Organisatie B) de IV/ICT-voorzieningen worden gesplitst In twee delen B-1) voorzieningen van en voor GGD-GHOR --> uit te besteden aan de MSP B-2) voorzieningen voor pandemische paraatheid en infectieziektebestrijding --> uit te besteden aan de Landelijke beheer Organisatie. I) Op welke punten is deze interpretatie niet correct II) Welke applicaties (graag type applicaties) maken straks gebruik van de voorzieningen gemanaged door de MSP III) Als in aanvang de uitbesteding naar LBO nog niet plaats vindt; welke applicaties maken dan in beginsel ook gebruik van de MSP cloud-voorzieningen IV) wat is de beoogde datum voor de splitsing V) op welke wijze dienen MSP en LBO met elkaar te integreren	A + B zijn grotendeels correct - Aanbestedende Dienst - GGD GHOR Nederland transformeert vwb IV ICT-voorzieningen naar een Functionele Regie Organisatie. Een flink deel van het (maatwerk) applicatielandschap wordt in beheer gegeven bij een Landelijke Beheer Organisatie. Wat resteert zijn de eigen basis IV-ICT-voorzieningen (kantoorautomatisering, werkplekbeheer e.d.) welke zoveel mogelijk worden uitbesteed aan de MSP. Het eigen SOC verzorgt het werkveld van Privacy & Security en wordt zoveel mogelijk uitbesteed aan de MSSP volgend op de hierboven bescrheven veranderingen. Alle maatwerk applicaties (Covid, Pandemische Paraatheid e.d.) worden elders betrokken als SaaS, PaaS e.d. en vallen niet onder de scope van deze Aanbesteding. Aanbestedende Dienst heeft gepland dat er medio '26 een Freeze zal plaatsvinden, wat betekent dat er geen grote veranderingen meer worden toegevoegd. Aanbestedende Dienst is mede afhankelijk van de (politieke en bestuurlijke) besluitvorming en kan daarom geen concrete datum geven. De MSP die de managed services verzorgt voor GGD GHOR Nederland staat los van de LBO. De komst van de LBO impliceert dat GGD GHOR Nederland minder werknemers zal hebben.
381	GGN AI beleid	Eis 13 verwijst naar toetsing aan het GGN AI-beleid, dat in deze fase niet gedeeld kan worden. Omdat de reikwijdte van dit beleid impact heeft op de inzet van tooling en de hieraan gerelateerde pricing, verzoeken wij om een korte functionele samenvatting van de relevante beperkingen (bijvoorbeeld welke categorieën AI of automatisering wel/niet zijn toegestaan). Dit stelt ons in staat een realistische en goed onderbouwde aanbieding te doen.	Aanbestedende Dienst heeft inzake het AI-Beleid een aanpassing gemaakt in de Nota van Inlichtingen 1.
382	Kenbaarmaking beleidsstukken	Bevestigt u dat alleen kenbaar gemaakte beleidstukken (met versie + datum) bindend zijn, met formeel wijzigingsbeheer (schriftelijke kennisgeving en redelijke inwerkingtredingstermijn)? Achtergrond: Nvl#1 refereert aan intern AI-beleid en CISO-toets, maar de conceptovereenkomst en verwerkersovereenkomst bepalen geen regime voor kenbaarheid/versiewijzigingen.	Uitsluitend kenbaar gemaakte documenten / beleidsstukken zijn bindend.

383	Contractstatus Uitvoeringsdocumenten	Krijgen uitvoeringsdocumenten (Implementatieplan, DAP, MSP/MSSP-Backlogs, Exitplan, RASCI, Autorisatiematrix) ook contractstatus, en zo ja, via welke route (appendix/ addendum) worden ze onderdeel van de Overeenkomst?	Uitvoeringsdocumenten zoals het Implementatieplan, DAP, MSP/MSSP-Backlogs, het Exitplan, RASCI, Autorisatiematrix, etc. hebben een contractstatus en worden in de Overeenkomst genoemd als onderdeel van de Inschrijving. Ook al worden deze stukken eventueel op een later moment dan de Inschrijving uitgewerkt.
384	Bijlage SLA	In het "Beschrijvend document EA procedure MSP en MSSP v1.0" staat op pagina 40 dat inschrijver wordt gevraagd om een standaard concept SLA voor managed services en Managed Security services als extra bijlagen toe te voegen. De door GGH GHOR meegestuurde template bevat informatie die wij vooral hebben opgenomen in ons gestandaardiseerde Dossier Afspraken en Procedures (DAP). Is het akkoord om in plaats van één SLA document twee documenten (DAP + SLA) toe te voegen?	De Concept SLA's die zijn bijgevoegd bevatten het minimu-niveau van service levels waaraan voldoen moet worden (Programma van Eisen). In Gunningscriterium G2 vragen wij Inschrijver haar eigen SLA's mee te sturen zodat Aanbestedende Dienst hiervan samen met uitwerking G2 kennis kan nemen. Volgens Aanbestedende Dienst komt het DAP (Dossier Afspraken en Procedures) pas gezamenlijk tot stand bij het aangaan van het SLA.
385	Bijlage K - Concept Service Level Agreement MSSP GGD GHOR Nederland	Bijlage K – SLA MSSP stelt dat de MSSP patchmanagement uitvoert, inclusief het plannen en implementeren van patches op systemen en infrastructuur. Dit staat haaks op Bijlage A – Programma van Eisen, waarin patching expliciet behoort tot het MSP-domein (werkplekken, kantoorautomatisering, netwerkcomponenten, firewalls, cloudhosting). Wij gaan ervan uit dat patchmanagement — inclusief de daadwerkelijke implementatie van patches — volledig binnen de MSP-scope valt, en dat de MSSP uitsluitend verantwoordelijk is voor signalering, advisering en risicoclassificatie vanuit een security-perspectief. Graag ontvangt Inschrijver bevestiging dat de interpretatie correct is, zodat geen overlap of dubbele verantwoordelijkheden ontstaan tussen MSP en MSSP.	Correct.
386	Compliance en kosten risico	Kunt u de minimale maatregelen (encryptiesleutelbeheer/klant-keys, verzet-clausules, notificatie, LE-request-procedure) en kosten-/aansprakelijkheidsverdeling vastleggen? Achtergrond: er staat niets over de CLOUD-Act in de concept- en verwerkersovereenkomst. Zonder afspraken is compliance- en kostenrisico (enigszins) onbepaald.	Aanbestedende Dienst begrijpt deze vraag niet. Aanbestedende Dienst hanteert de kaders die in deze Aanbesteding zijn meegegeven.
387	Audits	Kunt u bevestigen dat audits uitsluitend plaatsvinden op basis van objectieve triggers, met een vooraf overeengekomen frequentie, een verplicht vooraf gedeeld auditplan, redelijke aankondigingstermijnen (behoudens spoed) en een heldere kostenregeling voor door de Aanbestedende Dienst geïnitieerde audits?	Audits vinden plaats op initiatief van Opdrachtgever en in overleg met Opdrachtnemer met een vooraf overeengekomen kostenregeling. Zie ook het antwoord op soorgtelijke vraag in deze Nota van Inlichtingen
388	Audits en Pentests	Kunt u bevestigen dat audits en/of pentests uitsluitend worden uitgevoerd door onafhankelijke, geaccrediteerde derden, niet zijnde directe concurrenten van de inschrijver, en dat deze plaatsvinden onder strikte geheimhouding en binnen een vooraf afgebakende need-to-know scope?	Pentesten worden op initiatief van Aanbestedende Dienst uitgevoerd en altijd in overleg met Opdrachtnemer onder vermelding van de reikwijdte en scope. De frequentie is tenminste eenmaal per jaar en indien de situatie dat vereist.
389	Doorbelasting toezichthouder-boetes	Bevestigt u dat doorbelasting van toezichthouder-boetes alleen plaatsvindt bij een vastgestelde, aan de opdrachtnemer toerekenbare tekortkoming binnen diens verwerkers-scope, met proportionele weging van de rol en verantwoordelijkheid van Opdrachtgever als verwerkingsverantwoordelijke?	Correct, onder de voorwaarden vermeld in GIBIT 2023. - 16.6 - IV - 2a en 2b.
390	Boetes	Nu boeteplafonds niet worden gehanteerd en art. 3.6 van de conceptovereenkomst een 5% boete introduceert: wilt u objectieve toepassingscriteria, maatstaf ernst/duur, cumulatieregels en mitigatiefactoren formaliseren?	Artikel 3.6 beschrijft de werkwijze alsook de condities waaronder de boete van toepassing is: het niet tijdig realiseren van het implementatieplan en/ of het verbeterplan. Er zijn dus duidelijke escalatie- afstemmingsmomenten.
391	prijzenblad, bijlage O	Deel A - Managed Service Provider MSP: Dit deel van het prijzenblad bevat een blok 'Periodieke Maandkosten Managed Services' (gebaseerd op een fee per maand) en een blok 'Kosten per Gebruiker per Maand - Managed Services' (gebaseerd op een fee per gebruiker per maand). In beide blokken zijn dezelfde 12 prijselementen opgenomen. Staat het de Inschrijver vrij om te bepalen op welke verrekeneenheid zij haar diensten wil aanbieden, hetgeen kan betekenen dat er prijselementen op 0,00 EUR blijven staan, of verwacht Opdrachtgever op elk van de afzonderlijke prijselementen in beide blokken een ingevulde prijs?	U dient uw prijzen zo realistisch mogelijk toe te rekenen naar de prijselementen uit het Prijzenblad. In het Beschrijvend Document vindt u de regels die hier gelden. Het is derhalve binnen die regels de mogelijkheid de prijslementen die niet van toepassing zijn op 0,00 te laten staan.

392	Vormvereisten	Bij de vormvereisten voor de Gunningscriteria geeft u een maximaal aantal pagina's A4 (enkelzijdig), inclusief eventuele voorblad, inhoudsopgave, afbeeldingen, diagrammen, tijdsbalken e.d.. Kunt u dit wijzigen naar: "exclusief eventueel voorblad, inhoudsopgave achterblad en inclusief afbeeldingen, diagrammen, tijdsbalken e.d."? Alle inhoudelijkheid staat dan in het maximaal aantal pagina's.	Akkoord, exclusief eventueel voorblad, inhoudsopgave achterblad maar inclusief afbeeldingen, diagrammen, tijdsbalken.
393	Exit Plan	Kunt u een limitatieve lijst van standaard exit-activiteiten en een definitie van 'onvoorzien' vastleggen om de inschatting van de exit inspanning mogelijk te maken?	Aanbestedende Dienst is wettelijk verplicht een Exit-plan te eisen bij het aangaan van bijvoorbeeld een MSP en/ of MSSP contract. De expertise hoe een veilige Exit eruit ziet bij beeindiging van een contract hoort bij de MSP/MSSP.
394	KPI-afwijkingen	Bevestigt u dat KPI-afwijkingen die (mede) voortvloeien uit externe (SaaS-)leveranciers niet aan de opdrachtnemer worden toegerekend en dat dit expliciet wordt gereflecteerd in SLA-rapportages?	Indien KPI-afwijkingen ontstaan als gevolg van externe invloeden die niet aan Opdrachtnemer kunnen worden toegerekend, dan zal dit in de SLA-rapportages worden gereflecteerd.
395	Opschaling	Kunt u de noodprocedure, objectieve activeringscriteria, tijdelijkheid, schriftelijke vastlegging en ex-ante kostenafstemming formaliseren? Achtergrond: Art. 21.2 van de conceptovereenkomst geeft ruime bevoegdheid voor directe opschaling en KPI-verzwaring, procedurele waarborgen en kostentransparantie ontbreken.	Artikel 21.2 betreft een crisis-situatie. Aanbestedende Dienst bedoelt hiermee een situatie
396	pijzenblad, bijlage O	Deel A - Managed Service Provider MSP - Eenmalige implementatiekosten: Inschrijver doet de aanname dat bij prijselement 'Inbeheername Samenwerking met ServiceDesk' wordt bedoeld dat Opdrachtgever zelf de ServiceDesk (eerstelijn) verzorgt en Inschrijver het tweede- en derdelijns beheer verzorgt. Kan Opdrachtgever dit bevestigen?	De minimum-service level requirements voor MSP en MSSP vindt u in de bijlagen Concept SLA MSP en Concept SLA MSSP. In eerste instantie wordt verwacht dat Opdrachtgever zelf de eerste lijn verzorgt, maar dat dit geleidelijk overgaat naar de MSP resp MSSP.
397	prijzenblad, bijlage O	Deel A - Managed Service Provider MSP - Licentiekosten Managed Services: Internettoegang en Internetverbindingen zijn out of scope van de aanbesteding. Kan Opdrachtgever aangeven welke licentiekosten zij verwacht bij het prijselement 'Kantoor Internettoegang en Internetverbinding als managed service'?	Het is aan Inschrijver om te bepalen of er - gegeven de beperking - Licentiekosten van toepassing zijn op de post Kantoor Internettoegang en Internetverbinding.
398	prijzenblad, bijlage O	Deel A - Managed Service Provider MSP - Licentiekosten Managed Services: kan Opdrachtgever verduidelijken wat zij bedoelt met 'Kantoor Cloudhosting' en welke licenties zij hier verwacht?	Hier gaat het om de Azure Abonnementen.
399	prijzenblad, bijlage O	Deel A - Managed Service Provider MSP - Licentiekosten Managed Services: verwacht Opdrachtgever een prijs bij het prijselement 'Kantoor Back-up & Recovery als managed service'? In NvI-1, vraag 197, geeft Opdrachtgever aan dat licenties voor Avepoint reeds zelf zijn ingekocht.	Hier wordt bedoeld dat MSP wordt verwacht ook de Avepoint licenties te verzorgen
400	prijzenblad, bijlage O	Deel A - Managed Service Provider MSP - Licentiekosten Managed Services: voor welke producten/tools verwacht Opdrachtgever licentiekosten bij het prijselement 'Kantoorautomatisering Algemeen als managed service'?	Het is aan Inschrijver om te bepalen of er Licentiekosten van toepassing zijn op de post Kantoorautomatisering Algemeen.
401	Bijlage J - Concept Service Level Agreement MSP GGD GHOR Nederland	Bijlage J – Concept SLA MSP bevat in §1.6 een uitgebreide beschrijving van de scope van de MSP-dienstverlening. Deze scope is anders dan de eisen uit het Programma van Eisen. Inschrijver gaat er van uit dat het Programma van Eisen bepalend is en de beschrijving in het template Bijlage J uitsluitend als voorbeeld is bedoeld en in lijn wordt gebracht tijdens de implementatie van de dienstverlening. Kunt u dit bevestigen?	Dat is correct.
402	pijzenblad, bijlage O	Deel A - Managed Service Provider MSP: Regels 68, 83 en 98 van de Excel - Inschrijver doet de aanname dat bij prijselement 'Beheer in samenwerking met ServiceDesk' wordt bedoeld dat Opdrachtgever zelf de ServiceDesk (eerstelijn) verzorgt en Inschrijver het tweede- en derdelijns beheer verzorgt. Kan Opdrachtgever dit bevestigen?	De minimum-service level requirements voor MSP en MSSP vindt u in de bijlagen Concept SLA MSP en Concept SLA MSSP. In eerste instantie wordt verwacht dat Opdrachtgever zelf de eerste lijn verzorgt, maar dat dit geleidelijk overgaat naar de MSP resp MSSP.

403	Huidig MSSP-landschap & situatie	In de aanbestedingsstukken wordt geen expliciete vermelding gemaakt van een verplichting tot overname van personeel (zoals bedoeld onder overgang van onderneming ex artikel 7:662 BW e.v.) of andere vormen van 'werk-naar-werk' constructies. Kunt u bevestigen dat: er geen sprake is van een verplichting tot overname van personeel van de huidige leverancier(s) of opdrachtgever; er geen verplichting bestaat tot het aanbieden van arbeidsovereenkomsten aan betrokken medewerkers; er geen andere verplichtingen gelden in het kader van werk-naar-werk of vergelijkbare regelingen; inschrijvers volledig vrij zijn in de inrichting van hun eigen organisatie en personele bezetting, mits wordt voldaan aan de gevraagde dienstverlening? Indien bovenstaande niet volledig juist is, verzoeken wij u om expliciet aan te geven welke verplichtingen wel van toepassing zijn, inclusief de relevante juridische grondslag en scope.	Correct, er is geen sprake van overname van personeel (zoals bedoeld onder overgang van onderneming ex artikel 7:662 BW e.v.) of andere vormen van 'werk-naar-werk' constructies. Inschrijvers zijn vrij in de inrichting van hun eigen organisatie en personele bezetting, mits wordt voldaan aan de eisen met betrekking tot de gevraagde dienstverlening.
404	Huidig MSSP-landschap & situatie	In NVI ronde 1 wordt bij het antwoord op vraag 88 niet verder ingegaan op de rol en toekomst van de 6 SOC mensen die werkzaam zijn bij GGD GHOR. Kan GGD GHOR aangeven of het (op termijn) outsourcen van dit team (6 SOC mensen) onderdeel is van de uitvraag?	Het overnemen van de mensen van het eigen SOC van Aanbestedende Dienst is geen onderdeel van de uitvraag. Uitsluitend de Dienstverlening / ICT-prestaties die momenteel door het eigen SOC wordt/ worden geleverd, moeten ind e toekomst door de MSSP worden geleverd.
405	Beschrijvend document, Periodieke Maandkosten Managed Security Services	Door aanbestedende dienst wordt aangegeven dat de scope 300 actieve use cases zijn. Indien dit er meer worden hoe worden deze verrekend in het prijzenblad, er is geen mogelijk voor het invullen van variabele kosten.	Inschrijver wordt geacht de kosten om te rekenen naar kosten per use case. Deze kosten per use case kunt u invullen in het Prijzenblad - MSSP - Use Case Management - Fee per Use Cae per Maand.
406	Huidig MSSP-landschap & situatie	In NVI ronde 1 wordt bij het antwoord op vraag 77 aangegeven dat GGD GHOR ten aanzien van het beheer van het SOC/SIEM op termijn naar een regieorganisatie gaat. Is nu niet juist het moment voor de GGD GHOR om deze transitie in gang te zetten en staat GGD GHOR daarom voor open om (na afloop van huidige licentieconract) het MSSP als een dienst af te nemen bij een leverancier?	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 Voor de snelheid en de besluitvorming is Aanbestedende Dienst afhankelijk van de politieke en bestuurlijke besluiten. Het is per definitie (zie Beschrijvend Document en Programma van Eisen) om het geheel van SOC-dienstverlening binnen de Overeenkomt bij de MSSP te beleggen.

407	Beantwoording vragen met betrekking tot servicedesk	In uw antwoord geeft u aan dat ten tijde van de Inbeheername de eigen servicedesk van de Aanbestedende Dienst nog volledig de eerstelijns ondersteuning verzorgt, en dat de verwachting is dat deze eerstelijnsactiviteiten na Inbeheername — na 1 jaar — per servicemanagementdomein aan de MSP zullen worden uitgefaseerd. Gezien de aanbesteding een contractduur van vier (4) jaar betreft, leidt deze onzekerheid over het exacte moment en tempo van de uitfasering tot een situatie waarin inschrijvers moeten speculeren over de daadwerkelijke scope en hiermee samenhangende kosten. Om een eerlijk, transparant en controleerbaar prijsvergelijk mogelijk te maken, verzoeken wij u te verduidelijken: Op welk(e) moment(en) binnen de 4-jarige contractduur de overgang van eerstelijnsactiviteiten naar de MSP daadwerkelijk plaatsvindt of geacht wordt plaats te vinden; Of er een vast, geharmoniseerd uitfaseringsscenario beschikbaar wordt gesteld dat door alle inschrijvers moet worden gehanteerd bij het invullen van het prijzenblad; Hoe het prijzenblad moet worden ingevuld wanneer de overdrachtsmomenten nog niet vaststaan, om te voorkomen dat inschrijvers ongelijkmatig of strategisch kosten verdelen; Of de Aanbestedende Dienst bereid is het prijzenblad aan te passen zodat dit de volledige 4-jarige scope en het gewenste uitfaseringspad eenduidig weerspiegelt, zodat manipulatieve of onvergelijkbare inschrijvingen worden voorkomen.	De as-is Inbeheername van de voorzieningen dient in 2026 te zijn afgerond (MVP). De verwachting is dat de overname van de Servicedesk binnen het eerste jaar van de Overeenkomst zal plaatsvinden en zodoende voor alle 4 jaren van toepassing zal zijn. Het prijzenblad wordt dan ook niet aangepast.
408	Beschrijvend document EA procedure MSP MSSP v1.0	In de aanbestedingsdocumenten wordt gesproken over ‘feeds per maand’ en daarbij vermeld dat binnen twee jaar mogelijk het GGD GHOR Nederland-eigen SOC volledig wordt uitbesteed. Tevens is aangegeven dat deze toekomstige uitbesteding géén onderdeel vormt van de scope van deze aanbesteding. Kunt u toelichten wat hiervan precies de betekenis is voor deze aanbesteding? Specifiek vernemen wij graag: Of en hoe deze mogelijke uitbesteding binnen twee jaar invloed heeft op de omvang, aard of frequentie van de aan te leveren feeds gedurende de contractperiode; Of deze mogelijke uitbesteding aanleiding geeft tot aanvullende of gewijzigde eisen aan de inschrijver; Of deze ontwikkeling enige rol speelt in de beoordeling van de inschrijvingen; En hoe het genoemde maximum van 6 medewerkers binnen het uitbestede SOC zich verhoudt tot de verplichtingen binnen deze aanbesteding, bijvoorbeeld ten aanzien van capaciteit, samenwerking en aanlevering van informatie.	Eerst dienen de SOC/SIEM-voorzieningen as-is in beheer te worden genomen en dient er te worden samengewerkt tussen Opdrachtnemer en het SOC van aanbestedende dienst om zo ook geleidelijk de dientverlening van het SOC bij de MSS onder te brengen. Dit betreft de Dienstverlening, de mensen worden niet uitbesteed. In paragraaf 2.2 van het Beschrijvend Document vindt u een opsomming wat expliciet niet tot de odpracht behoort. Initieel betekent dit dat bestaande feeds worden overgenomen en dat gezamenlijk gekeken wordt of deze feeds vervangen of verbeterd moeten worden bijvoorbeeld met feeds van Opdrachtnemer. Deze uitbesteding verandert niets aan de eisen, noch aan eisen aan de Inschrijver, noch aan de beoordeling. U dient aan de eisen in het PvE te voldoen.
409	Bijlage O - Prijzenblad	In het huidige prijzenblad wordt uitsluitend een prijs per jaar weergegeven, zonder de volledige initiële looptijd van het contract te reflecteren. Daarnaast biedt het prijzenblad geen inzicht in de invloed van afbouwscenario’s op de totale kosten. Hierdoor ontstaat het risico op een manipulatieve inschrijving, doordat inschrijvers vaste en variabele kosten ongelijkmatig kunnen verdelen over de contractjaren. Kunt u een aangepast prijzenblad aanleveren dat de volledige contractduur van vier (4) jaar weergeeft, inclusief de financiële impact van afbouw, en dat tevens als beoordelingsgrondslag voor de prijscomponent wordt gebruikt?	U dient het Prijzenblad aan te houden en er wordt geen aangepast Prijzenblad beschikbaar gemaakt. Zoals u kunt zien onder Totaalprijs worden de Implementatie- en Jaar 1 kosten apart gesommeerd aan de hand waarvan Aanbestedende Dienst verwacht (Artikel 2.116 Aanbestedingswet 2012) te kunnen vaststellen of er sprake is van abnormaal lage of manipulatieve inschrijving ten opzichte van bijvoorbeeld de benchmark uit de Marktconsultatie. Zie hiervoor ook het Beschrijvend Document, pagina 49 onder 'Overig" . Aanbestedende dienst gaat er voorts vanuit dat de Jaar 1 kosten (kolom L) ook in jaar 2, 3 en 4 van toepassing zullen zijn (behoudens indexering). De financiele impact van de afbouw is bewust niet in het Prijzenblad verwerkt, omdat op dit moment nog niet duidelijk is hoe diep en snel deze afbouw zal verlopen. Wij rekenen derhalve voor jaar 2, 3 en 4 met dezelfde parameters.
410	Monitoring scope assets PvE MSSP + Beschrijvend document	Kunt u een volledig en actueel overzicht verstrekken van het aantal assets dat binnen de scope van de MSSP-dienstverlening valt, inclusief endpoints, servers, netwerkcomponenten, cloudresources, mobiele apparaten, virtuele werkplekken, service-accounts en eventuele OT- of IoT-componenten, zodat een realistische inschatting van de benodigde monitoringcapaciteit en kosten kan worden gemaakt?	Deze vraag is reeds in de eerste Nota van Inlichtingen beantwoord.

411	Monitoring subset PvE MSSP	Kunt u bevestigen of de monitoring betrekking heeft op alle assets binnen het GGD GHOR-domein of uitsluitend op een gedefinieerde subset van bedrijfskritische systemen en omgevingen?	Dit betreft een voorgedefinieerde subset van systemen en omgevingen.
412	CMDB inhoud NVI vraag 208 + DAP	Kunt u toelichten in hoeverre de beschikbare CMDB volledig is voor alle assets binnen scope van MSP en MSSP en of deze informatie bevat over eigenaar, classificatie, criticality en dataclassificatie en wordt gebruikt als leidend systeem voor monitoring, vulnerability management en incidentafhandeling?	De CMDB is volledig voor alle in beheer te nemen onderdelen MSP en MSSP en bevat alle relevante informatie die noodzakelijk is voor de uitvoering van de dienstverlening.
413	SLA MSSP monitoring hoofdstuk	Kunt u bevestigen of mobiele apparaten, VDI-omgevingen en service-accounts volledig onderdeel uitmaken van de MSSP-monitoringsscope en welke aanvullende eisen hieraan worden gesteld?	het concept SLA MSSP heeft als doel de minimum Service Level Requirements te stipuleren en doet geen uitspraken over de monitoringsscope. De scope vindt in de eerste Nota van Inlichtingen.
414	Scanmethodiek PvE MSSP vulnerability scanning	Kunt u aangeven welke scanmethodiek wordt verwacht binnen de dienstverlening, inclusief de mate waarin agent-based scanning, authenticated scanning en netwerk-gebaseerde scanning dient te worden toegepast per type asset?	Nee hier zijn geen specifieke verwachtingen. In Eis 70 en Eis 83 vragen wij functioneel het vulnerability management en vulnerability scanning uit als dienst. In de eerste Nota van Inlichtingen vindt u (o.a. vraag 251) de specificaties hoe dat nu is geregeld.
415	Scanfrequentie SLA MSSP security monitoring	Kunt u aangeven welke frequentie wordt verwacht voor vulnerability scans per assetcategorie en welke retesting-eisen gelden na het doorvoeren van mitigerende maatregelen?	Nee hier zijn geen specifieke verwachtingen. In Eis 70 en Eis 83 vragen wij functioneel het vulnerability management en vulnerability scanning uit als dienst. In de eerste Nota van Inlichtingen vindt u (o.a. vraag 251) de specificaties hoe dat nu is geregeld. Het Concept SLA MSSP geeft de minimum Service Level Requirements aan waarbinnen dit moet plaatsvinden.
416	Scope lifecycle - PvE MSSP + SLA MSSP	Kunt u bevestigen of de MSSP naast detectie van kwetsbaarheden ook verantwoordelijk wordt geacht voor triage, mitigatieadvies, change-coördinatie, retesting en rapportage richting audits en compliance-processen zoals BIO en ENSIA?	De MSSP wordt verantwoordelijk geacht de Managed Security Services uit het PvE binnen de Service Levels uit het concept SLA MSSP te leveren. De rechten, plichten en verantwoordelijkheden staan in de overeenkomst en de voorwaarden. Triage = Tier 1,Change-coordinatie hoort bij de Product Owner van Aanbestedende Dienst etc.
417	Tool integratie NVI vraag 209	Kunt u toelichten in hoeverre integratie wordt verwacht tussen vulnerability tooling van de MSSP en bestaande SIEM- en ITSM-omgevingen van Opdrachtgever, inclusief eisen ten aanzien van real-time event-doorzetting en workflow-integratie?	Wij begrijpen deze vraag niet goed. Waarom zou Vulnerability Tooling worden geintegreerd met ITSM? Het is de bedoeling dat u de GGN-eigen SIEM-voorzieningen in beheer neemt en dat het daarbij behorend servicemanagement inricht in of met ServiceNow van Aanbestedende Dienst.
418	Pentest scope SLA MSSP security assessments	Kunt u aangeven welke systemen, applicaties en infrastructuurcomponenten binnen scope vallen voor periodieke pentesten, inclusief interne infrastructuur, externe perimeter, webapplicaties, API's, cloudplatformen en eventuele OT- of IoT-omgevingen?	Pentesten worden op initiatief van Aanbestedende Dienst uitgevoerd en altijd in overleg met Opdrachtnemer onder vermelding van de reikwijdte en scope
419	Pentest frequentieSLA MSSP KPI / governance	Kunt u toelichten welke frequentie wordt verwacht voor pentesten en security assessments gedurende de contractperiode en in hoeverre aanvullende testen kunnen worden gevraagd bij wijzigingen of incidenten?	Pentesten worden op initiatief van Aanbestedende Dienst uitgevoerd en altijd in overleg met Opdrachtnemer onder vermelding van de reikwijdte en scope. De frequentie is tenminste eenmaal per jaar en indien de situatie dat vereist.
420	Rapportage formatCompliance eisen BIO / ENSIA	11Kunt u aangeven of er een verplicht rapportformat of template wordt gehanteerd voor pentestresultaten en in hoeverre deze moeten aansluiten op BIO- of ENSIA-verantwoordingsstructuren?	Aanbestedende Dienst hanteert hierin te allen tijde de BIO, de ENSIA komt hier uit voort. Deze hebben echter betrekking op Audit en Verantwoording. In dat licht ziet Aanbestedende Dienst de ENSIA als de verantwoording en de Pentest-resultaten als onderbouwend bewijs.
421	Opvolging bevindingenPvE MSSP backlog	12Kunt u bevestigen of de MSSP verantwoordelijk wordt geacht voor het coördineren van opvolging van pentestbevindingen inclusief prioritering, acceptatie en retesting?	Pentesten worden op initiatief van Aanbestedende Dienst uitgevoerd en altijd in overleg met Opdrachtnemer onder vermelding van de reikwijdte en scope. Indien de resultaten van de Pentesten opvolging vergen dat zal dit altijd het change-proces volgen.
423	EscalatiecriteriaSLA MSSP incident management	14Kunt u toelichten welke escalatiecriteria worden gehanteerd door het huidige SOC en op welk moment betrokkenheid van de MSSP wordt verwacht?	het concept SLA MSSP heeft als doel de minimum Service Level Requirements te stipuleren en doet geen uitspraken over de inhoudelijke escalatiecriteria. Deze worden na gunning bij het definitief vaststellen van het SLA MSSP overeengekomen (ITIL).
422	SOC taakverdelingNVI vraag 19 + PvE SOC samenwerking	13Kunt u per processtap specificeren welke taken momenteel door het interne SOC worden uitgevoerd en welke taken door de MSSP worden verwacht, inclusief monitoring, triage, containment, forensics, communicatie, patch-coördinatie en afsluiting van incidenten?	Alle functioneel uitgevraagde MSSP-diensten (PVE) worden momenteel door het SOC van Aanbestedende Dienst zelf verzorgt. Het is de bedoeling dat Inschrijver eerst de SOC/SIEM-voorzieningen in beheer neemt en daarna de volledige dienstverlening van het SOC van Aanbestedende Dienst. Aanbestedende Dienst verwacht dat dit geleidelijk zal gaan, daarom de Eis om eerst met SOC van Aanbestedende Dienst samen te werken.

424	VerantwoordelijkheidSLA MSSP governance	15Kunt u bevestigen wie eindverantwoordelijk is per fase van incident response en in hoeverre deze verantwoordelijkheid gedurende de contractperiode kan verschuiven?	Alle functioneel uitgevraagde MSSP-diensten (PVE) worden momenteel door het SOC van Aanbestedende Dienst zelf verzorgt. Het is de bedoeling dat Inschrijver eerst de SOC/SIEM-voorzieningen in beheer neemt en daarna de volledige dienstverlening van het SOC van Aanbestedende Dienst. Aanbestedende Dienst verwacht dat dit geleidelijk zal gaan, daarom de Eis om eerst met SOC van Aanbestedende Dienst samen te werken.
425	Consultant rolSLA MSSP consultancy services	Kunt u toelichten welke concrete werkzaamheden worden verwacht van de securityconsultant, waaronder vulnerability lifecycle-beheer, deelname aan risk boards, stakeholdermanagement, use-case optimalisatie en auditondersteuning?	Aanbestedende Dienst gaat er vanuit dat de MSSP de Managed Security Services levert op basis van het bestek van deze aanbesteding. Eventuele aanvullende security consultancy zal altijd apart worden aangevraagd en moeten worden begroot.
426	Consultant inzetBeschrijvend document capaciteit	Kunt u aangeven welke structurele inzet wordt verwacht van de consultant, bijvoorbeeld in aantal dagen per maand, en of inzet op afroep of buiten kantooruren noodzakelijk is?	Aanbestedende Dienst gaat er vanuit dat de MSSP de Managed Security Services levert op basis van het bestek van deze aanbesteding. Eventuele aanvullende security consultancy zal altijd apart worden aangevraagd en moeten worden begroot.
427	Back-up consultantContinuïteitseisen SLA	Kunt u bevestigen of beschikbaarheid van een back-up consultant vereist is voor continuïteit van dienstverlening?	Aanbestedende Dienst begrijpt deze vraag niet. Aanbestedende Dienst vraagt om een managed Security Services Provider die tenminste binnen de kaders van het Concept SLA MSSP haar prestaties kan leveren. Het is niet aan Aanbestedende Dienst om te bepalen of MSSP daar een back-up consultant nodig acht.
428	Awareness doelgroepSLA MSSP awareness hoofdstuk	Kunt u aangeven welke doelgroepen binnen scope vallen voor security awareness dienstverlening en hoeveel medewerkers dit betreft?	Het betreft hier primair de medewerkers binnen Aannbestedende Dienst. Het aantal medewerkers vindt u in het Beschrijvend Document
429	Awareness vormenSLA MSSP human risk	Kunt u toelichten welke vormen van awareness worden verwacht, zoals e-learning, phishing-simulaties, klassikale trainingen en maatwerkcampagnes?	De vormen die u vraagt vallen hieronder.
430	Awareness KPISLA MSSP KPI rapportage	Kunt u aangeven welke KPI's worden gehanteerd voor awarenessprogramma's en in hoeverre rapportage per afdeling of organisatiebreed vereist is?	Het concept SLA MSSP heeft als doel de minimum Service Level Requirements te stipuleren en doet geen uitspraken over de inhoudelijke KPI's ten aanzien van Awareness. Deze worden na gunning bij het definitief vaststellen van het SLA MSSP overeengekomen (ITIL)
431	CampagnebeheerGovernance communicatie	Kunt u bevestigen of de MSSP verantwoordelijk wordt geacht voor planning en uitvoering van interne communicatie rondom awarenesscampagnes?	Interne communicatie wordt te allen tijde door Aanbestedende Dienst verzorgd, tenzij explciet anders overeengekomen.
432	Capaciteit inzetBeschrijvend document omvang opdracht	Kunt u aangeven welke maandelijkse inzet wordt verwacht voor consultancy, awareness en operationele MSSP-activiteiten en of er piekperioden zijn zoals audits, migraties of releases die aanvullende inzet vereisen?	Consultancy en Awareness zijn te allen tijde in overleg en worden vooraf per opdracht / taak/ ticket overeengekomen. Operationele MSSP-activiteiten (PvE en SLA) worden geacht onderdeel uit te maken van de Managed Security Services.
433	OverlegstructuurSLA MSSP governance meetings	Kunt u toelichten welke overlegstructuur wordt verwacht inclusief frequentie, deelnemers en duur van operationele, tactische en strategische overleggen?	Het concept SLA MSSP heeft als doel de minimum Service Level Requirements te stipuleren en doet geen uitspraken over de overlegstructuren. Deze zullen bij het defintief vaststellen van het SLA MSSP overeen worden gekomen tussen SLM van Opdrachtgever en Opdrachtnemer.
434	Tooling stackNVI vraag 10 ICT infra	25Kunt u inzicht geven in de huidige security tooling stack inclusief SIEM, EDR/XDR, vulnerability tooling, SOAR en GRC-oplossingen en het aantal actieve logbronnen en use-cases?	Zie hiervoor de antwoorden uit de Nota van Inlichtingen 1. en dezelfde vragen in deze Nota van Inlichtingen 2.
435	Pricing aannamesPrijzensheet + Beschrijvend document	26Kunt u bevestigen welke aantallen leidend zijn voor prijsstelling, waaronder aantal locaties, gebruikers, endpoints, servers en cloudresources en welke diensten als optioneel of meerwerk moeten worden aangeboden?	Voor het Prijzenblad heeft Aanbestedende Dienst het advies van deelnemers aan de Marktconsultatie gevolgd om op deze wijze Functioneel de prijzen uit te vragen. Indien u een andere calculatiemethode hanteert dan het Prijzenblad, dan verzoeken wij u uw calculatie te converteren naar de items in kolom F van het Prijzenblad. Aanbestedende Dienst gaat er hierbij vanuit dat de ' Variabele Kosten Managed Services' en de ' Variabele Kosten & Incident resporns Tier3 (MSSP) optioneel en/ of meerwerk zijn.