			TN 341345 Aanbesteding SIEM SOC GGD HN	Nota van Inlichtingen d.d. 13 januari 2022
Ref. nr.	Label	Onderwerp	Vraag	(Concept) Antwoord
1		1.1 Inhoud van de Opdracht	Wilt u een eigen Security Operating Center (SOC) creëren, waarbij medewerkers volledig zelfstandig detectie en opvolging doen? Of verwacht u dat de dienstverlener een SOC als dienst levert, die de eigen medewerkers van relevante informatie voorziet?	In het begin zullen we steunen op inzet van de leverancier en daarna willen we het in de eigen organisatie borgen.
2		1.1 Inhoud van de Opdracht	Wenst u een SIEM aan te schaffen waarbij inschrijver een MDR (Managed Detect and Respond) oplossing leveren of wenst u een"as a Service" dienst waarbij SIEM opgenomen is in de dienst?	As a service
3		1.1 Inhoud van de Opdracht	Een SIEM is gebaseerd op logbronnen (200 volgens de uitvraag) maar ook op EPS (events per second) welke van logbron tot logbron sterk kunnen verschillen en de gewenste retentie tijd van de log. Een CMDB van de logbronnen kan een indicatie geven van de EPSen maar bij voorkeur horen wij graag de totale verwachte hoeveelheid log in GB/dag tesamen met de gewenste retentie. - Kunt u een CMDB van alle logbronnen aanleveren? - Hoeveel EPS genereren deze bronnen? - wat is de retentietijd die u wilt aanhouden?	De verwachte hoeveelheid log in GB/dag tesamen hangt van de scope die we kunnen krijgen voor het budget wat we willen investeren. De retentietijd hangt af van prijs en risico.
4	Inhoud	Verwerking data	Bent u akkoord met een oplossing waarbij verwerking van data binnen de EU plaatsvindt?	Ja
5	Juridisch	13.4 GIBIT	Bent u bereid te aanvaarden dat Leverancier niet aansprakelijk is voor indirecte schade?	Uw opmerking staat niet in betreffend artikel. Wij vermoeden dat u verwijst naar de GIBIT 2016, artikel 13 van de GIBIT 2020 is van toepassing. Ten overvloede willen wij erop wijzen dat naast de bepalingen in de GIBIT het Burgerlijk Wetboek (en andere wetgeving) onverkort van toepassing is.
6	Juridisch	7.5 GIBIY	Bent u bereid te aanvaarden dat ontbinding van de overeenkomst, hetgeen voor beide partijen immers een zeer zwaar middel is, niet eerder plaats vindt dan nadat (i) GGD vruchteloos een ingebrekestelling met een specificatie van de tekortkomingen heeft gestuurd, en (ii) beide partijen bovendien vruchteloos op het hoogste niveau overleg hebben gehad?	In art 7.4 van de GIBIT 2020 staat de nuancering aangegeven.
7	Inhoud	Aantal GB	Voor het bepalen van de licentieprijs is het nodig om een inschatting te krijgen hoeveel GB per dag moet worden gemonitord. Kunt u deze informatie aanleveren?	Is niet bekend
8	Inhoud	Aantal GGD HN Gebruikers	– Hoeveel Actieve Active Directory / Azure AD / O365 gebruikers zijn er bij de GGD HN? – Hoeveel daarvan hebben een (thuiswerk) werkplek (Laptop/VDI/desktop, dus meer dan alleen webbased-O365 email/sharepoint) ?	Tijdens coronatijd 1800 medewerkers, normale situatie 700 medewerkers. Alleen kantoormedewerkers beschikken over een laptop 1200/700
9	Inhoud	Bestaande SIEM oplossingen	Bestaan er al SIEM oplossingen binnen de organisatie die voorzien in bijvoorbeeld Continuiteits Monitoring of Business Intelligence?	Nee
10	Juridisch	13.5 GIBIT	De aansprakelijkheid van Leverancier voor boetes van de toezichthouder zijn volgens de voorgestelde regeling in bedrag niet beperkt. Dat staat op gespannen voet met art. 6 van de voorgestelde verwerkersovereenkomst, welke bepaling een beperking van aansprakelijkheid suggereert. Het beperken van aansprakelijkheid tussen verwerkingsverantwoordelijke en verwerker is toegestaan en het is niet ongebruikelijk dat dan ook te doen. Bent u bereid onderdeel (iv) van art. 13.5 GIBIT tevens te onderwerpen aan de algemene beperking van aansprakelijkheid (dus: de beperking opgenomen in art. 13.4 GIBIT)?	Wij vermoeden dat u verwijst naar de GIBIT 2016, artikel 13 van de GIBIT 2020 is van toepassing. Hier is geen sprake van onbeperkte aansprakelijkheid.
11	Juridisch	Artikel 13.4 GIBIT	De aansprakelijkheid voor andere schade dan persoons- en zaakschade betreft onder meer de schade bij – kort gezegd – wanprestatie bij de uitvoering van de securitydiensten. Die aansprakelijkheid kent onder GIBIT 2020 een extreme en buitenproportioneel plafondbedrag: 10 maal de jaarvergoeding per gebeurtenis en maximaal 20 maal de jaarvergoeding (ongeacht het aantal gebeurtenissen) per jaar. Deze plafonds zijn buiten iedere reële proportie. Wij dringen er met klem op aan deze plafondbedragen substantieel te verlagen. Bent u bereid de totale aansprakelijkheid van Leverancier wegens een toerekenbare tekortkoming in de nakoming van de overeenkomst of uit enige andere hoofde te beperken maximaal driemaal de bedongen jaarvergoeding? Zo neen, bent u bereid akkoord te gaan met een ander plafondbedrag?	Uw opmerking staat niet in betreffend artikel. Wij vermoeden dat u verwijst naar de GIBIT 2016, artikel 13 van de GIBIT 2020 is van toepassing. Ten overvloede willen wij erop wijzen dat naast de bepalingen in de GIBIT het Burgerlijk Wetboek (en andere wetgeving) onverkort van toepassing is.
12	Juridisch	Artikel 6.1 GIBIT	Deze bepaling verlangt dat Leverancier voldoet aan de in de overeenkomst (nader) gespecificeerde interoperabiliteitseisen. Eventuele eisen op dit punt in de overeenkomst – en dus de daarin genoemde interoperabiliteitseisen – kent Leverancier nu niet. Kan daarover thans duidelijkheid worden verschaft?	is op dit moment niet bekend (nader te specificeren in overleg).

13	Juridisch	15.5 GIBIT	Een niet gemaximeerde boete zoals opgenomen in art. 15.5 GIBIT 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 maximale bedrag dat Leverancier aan boetes verschuldigd kan zijn onder deze overeenkomst, bijv. dat het totaal aan boetes gemaximeerd is op 100.000 EURO (ongeacht het aantal gebeurtenissen)?	Art 15.5 geeft wel een maximering aan de boete.
14	Contract	Artikel 10 GIBIT 2020	Gegadigde acteert in de uitvoering van de onderhavige opdracht als intermediair en is in de dienstverlening richting de aanbestedende dienst afhankelijk van derden, te weten de software fabrikanten. Echter, verlangt u onder artikel 10.1 van de GIBIT bijvoorbeeld wel van een leverancier een garantie dat de ICT Prestatie de overeengekomen eigenschappen zal bevatten en voldoet aan het Overeengekomen gebruik. T.a.v. het licentiecomponent van de uitvraag ligt een dergelijke garantie ligt bij de eigenaar/maker van de software, in deze; de software fabrikant. Immers, de software fabrikant heeft toegang tot de licenties c.q. gebruiksrechten en kan derhalve bijvoorbeeld onderhoud plegen en support bieden. Gegadigde heeft op geen enkele wijze toegang tot de licenties c.q. gebruiksrechten en kan deze garanties t.a.v. het licentiecomponent niet zonder meer afgeven. Derhalve verzoeken wij u akkoord te gaan met de garanties zoals die geboden worden door de desbetreffende software fabrikanten welke zijn vastgelegd in de toepasselijke licentie, onderhouds- en contractvoorwaarden (EULA). Dit in lijn met artikel 19.1 van de GIBIT. Graag uw akkoord?	Niet akkoord. Zie ook eerdere beantwoording.
15	Contract	Artikel 13.3 GIBIT 2020	De mogelijke aansprakelijkheid wordt beperkt in artikel 13.2. Echter, wordt de aansprakelijkheid (i) slechts beperkt per gebeurtenis, de maximale aansprakelijkheid voor meerdere gebeurtenissen is niet vastgelegd en (ii) is de omvang van dit bedrag, met het oog op de aard en omvang van de aan deze aanbesteding onderliggende opdracht, disproportioneel. Gegadigde kan zich niet verzekeren tegen schade voor onbeperkt aantal gebeurtenissen en zou daarmee een disproportioneel groot financieel risico nemen. In deze overeenkomst geldt dit temeer nu gegadigde fungeert als intermediair om de licenties c.q. gebruiksrechten aan de aanbestedende dienst te leveren en de licenties c.q. gebruiksrechten over het algemeen worden verstrekt middels een directe overeenkomst tussen de software fabrikant en de eindgebruiker (de aanbestedende dienst) onder toepasselijkheid van de licentie-, onderhoud- en contractvoorwaarden vanuit de software fabrikant. De Gids Proportionaliteit schrijft in 3.9.1.1 (voorschrift 3.9D, punt 2) voor dat de aanbestedende dienst rekening dient te houden met de risico's die aanbestedende dienst daadwerkelijk loopt én met de gebruikelijke aansprakelijkheidseis in de betreffende branche of voor de opdracht naar aard en omvang. Een voor de aanbestedende dienst gebruikelijke beperking van de aansprakelijkheid in de betreffende branche of voor de opdracht naar aard en omvang is €1.000.000,- per gebeurtenis met een maximum van €2.500.000,- per jaar. Wij zouden graag zien dat de aansprakelijkheid wordt beperkt in zoverre dat dit gebruikelijk is bij soortgelijke opdrachten binnen uw sector tot een bedrag van €1.000.000,- per gebeurtenis met een maximum van €2.500.000,- per jaar. Graag uw akkoord?	Niet akkoord. Zie ook eerdere beantwoording.
16	Inhoud	PVE - Eis 13	Er wordt gesproken over IPS/IDS. Ook wordt in de offerteaanvraag gesproken over netwerkmonitoring. Kunt u aangeven of netwerkmonitoring (-sensoren) ook onderdeel is van deze uitvraag.	Ja

17	Contract	Artikel 13.4 GIBIT 2020	De aansprakelijkheid voor overige schade is beperkt tot tien maal de “Jaarvergoeding” per gebeurtenis. U stelt daarbij dat de totale aansprakelijkheid per jaar evenwel nooit meer dan twintig maal de Jaarvergoeding zal bedragen (ongeacht het aantal gebeurtenissen). Gegadigde fungeert in deze uitvraag als intermediair om de licenties c.q. gebruiksrechten aan de aanbestedende dienst te leveren en de licenties c.q. gebruiksrechten over het algemeen worden verstrekt middels een directe overeenkomst tussen de software fabrikant en de eindgebruiker (de aanbestedende dienst) onder toepasselijkheid van de licentie-, onderhoud- en contractvoorwaarden vanuit de software fabrikant. De vergoedingen die uit de nadere overeenkomsten resulterend uit de onderhavige raamovereenkomst kunnen volgen kunnen variëren van kleine bedragen (de uitvraag van een licentie bij een Tier 3 software fabrikant) tot aan substantiële bedragen (een verlenging bij een Tier 1 software fabrikant). Gezien de algemene definitie van “Jaarvergoeding” opgenomen in artikel 1 van de GIBIT, de vrijheid van de aanbestedende dienst om een opdracht wel of niet onder de raamovereenkomst uit te vragen én de vermenigvuldiging factor opgenomen in het onderhavige artikel is het voor gegadigde niet mogelijk om het bedrijfsrisico in te calculeren. De onderhavige mogelijke aansprakelijkheid is een niet calculeerbaar bedrijfsrisico (een disproportioneel groot financieel risico) dat redelijkerwijs niet door gegadigde kan worden geaccepteerd. Gegadigde verzoekt de aanbestedende dienst dat de totale aansprakelijkheid zoals bepaald in Artikel 13.3 wordt aangepast van Jaarvergoeding naar een maximale aansprakelijkheid van € 2.500.000 per jaar. Graag uw akkoord?	Er is geen sprake van onbeperkte aansprakelijkheid. Er wordt ook niet gesproken tot een beperking van 10 maal de jaarvergoeding.
18	Contract	Artikel 15.5 GIBIT 2020	Het hanteren van een boeteclausule naast een aansprakelijkheidsclausule voldoet niet aan het proportionaliteitsvereiste van artikel 1.10 Aanbestedingswet 2012 en is als zodanig disproportioneel te noemen. Het hanteren van een boeteclausule naast een aansprakelijkheidsclausule resulteert namelijk in een onevenredig risico voor de winnende Inschrijver bij de uitvoering van deze overeenkomst. Daarnaast is een boeteclausule in welke hoedanigheid dan ook niet wenselijk voor een prettige en strategische samenwerking tussen de aanbestedende dienst en de winnende inschrijver. Wij willen u dan ook graag wijzen op de inhoud van artikel 3.9d uit de Gids Proportionaliteit. Ook is het naar onze mening niet noodzakelijk omdat in de contractvoorwaarden een vangnet is opgenomen ten aanzien van onze aansprakelijkheid en de daaruit voortvloeiende verplichting tot vergoeding van schade, in geval van schending van geheimhoudingsverplichtingen. De aanbestedende dienst heeft voldoende andere sanctionerende maatregelen tot haar beschikking in relatie tot een schending van dergelijke verplichtingen. Daarbij is de boete verschuldigd zonder dat in rechte vast is komen te staan dat gegadigde daadwerkelijk een geheimhoudingsbepaling heeft geschonden. Immers, niet iedere vermeende schending van de geheimhoudingsbepaling is aan gegadigde te wijten. Wij willen u verzoeken u om artikel 15.5 van de GIBIT te laten vervallen. Indien de aanbestedende dienst deze bepalingen niet buiten toepassing verklaart, verzoekt gegadigde om een toelichting.	Niet akkoord. Zie ook eerdere beantwoording.
19	Contract	Artikel 20.3 GIBIT 2020	De aanbestedende dienst wenst de mogelijk te hebben om in het geval dat meerdere overeenkomsten een onderlinge samenhang vertonen, gerechtigd te zijn slecht een deel van de overeenkomsten op te kunnen zeggen en stelt daarbij dat een dergelijke opzegging geen effect op de overige samenhangende overeenkomsten. Gegadigde begrijpt de wens van de aanbestedende dienst en zal als intermediair in de uitvoering van de opdracht hier in trachten te voorzien. Wel wijzen wij op de toepasselijke licentie, onderhouds- en contractvoorwaarden (EULA), in lijn met artikel 19 van de GIBIT. De licentie-, onderhoud- en contractvoorwaarden maken integraal onderdeel uit van de aankoop en het gebruik van de software. In deze voorwaarden treft de aanbestedende dienst of een licentie c.q. gebruiksrecht opzegbaar is en indien dit het geval is of dit ook geldt voor samenhangende overeenkomsten, in deze voorwaarden treft de aanbestedende dienst de randvoorwaarden die daarbij van toepassing zijn. Gegadigde acteert in de samenwerking als intermediair. Wij kunnen derhalve geen toezeggingen vanuit software fabrikanten doen ten aanzien van dit onderwerp ook niet ten aanzien van een eventuele opzegging. Uiteraard kan gegadigde de aanbestedende dienst ondersteunen in dergelijke situaties. De mogelijkheid tot opzegging kunnen wij derhalve enkel bevestigen ten aanzien van de raamovereenkomst. Uiteraard beïnvloed die opzegging niet de o.a. licentie overeenkomsten die de aanbestedende dienst is aangegaan met de software fabrikanten. Graag uw akkoord op het gestelde.	Niet akkoord. Zie ook eerdere beantwoording.

20	Contract	Artikel 21 GIBIT 2020	Gegadigde verzoekt de aanbestedende dienst om in het kader van het proportionaliteitsbeginsel ex artikel 1.10 Aanbestedingswet 2012 af te zien van het controle-/auditrecht zoals genoemd in artikel 21 GIBIT. Gegadigde is van mening dat de aard en omvang van de aan deze aanbesteding onderliggende opdracht een middel als controle/audit niet rechtvaardigen. Graag uw akkoord?	Niet akkoord. In het kader van de redelijkheid is bepaald dat de controle moet zien op de nakoming van *wezenlijke* verplichtingen.
21	Juridisch	Artikel 8 GIBIT	Het bepaalde in art. 8 GIBIT in relatie tot de gevraagde dienstverlening is weinig duidelijk. Bent u bereid te aanvaarden dat enkel die verplichtingen op het punt van onderhoud gelden welke door partijen eventueel later in een onderhoudsovereenkomst c.q. Service Level Agreement zijn overeengekomen?	Uitgangspunt van de GIBIT is dat na de Acceptatie de onderhoudsfase volgt. De GIBIT biedt een kader voor de onderhoudsfase. Dit kader kan nader worden uitgewerkt in een afzonderlijke onderhoudsovereenkomst of SLA.
22	Contract	Artikel 30.2 GIBIT 2020	De aanschaf van het gebruiksrecht op een licentie geeft geen recht op de broncode van de software. Gegadigde is geen eigenaar van de broncode. De software fabrikant is eigenaar van de broncode en de rechten en plichten die daarmee gepaard gaan. De broncode omvat de verzameling van alle door de software fabrikant geschreven computercodes voor het desbetreffende product. Derhalve kan gegadigde nimmer aan de omschreven Escrow verplichting voldoen. Graag verzoeken wij u dit artikel buiten toepassing te verklaren.	Art 30.2 gaat niet over broncodes.
23	Contract	Artikel 4.1, 4.2 & 20.9 GIBIT 2020	Behoudens de situatie dat nakoming blijvend onmogelijk is verzoeken wij u om een hersteltermijn toe te voegen in de vorm van een ingebrekestelling in het geval dat nakoming tijdelijk onmogelijk is. Gegadigde is voor een levering afhankelijk van derden (software fabrikanten). Een fatale termijn en het daaruit vloeiende verzuim heeft namelijk verregaande consequenties voor gegadigde. Gegadigde verzoekt daarom verzuim pas in te laten gaan na een ingebrekestelling met daarin een redelijke termijn om alsnog na te komen. Graag uw akkoord?	De definitie in art 4.1 en 4.2 van de GIBIT 2020 is helder. Verdere nuancering achten wij niet nodig.
24	Juridisch	Artikel 5.3 GIBIT	Het implementatieplan/plan van aanpak kan op punten afwijken van de verantwoordelijkheden en verplichtingen van Leverancier genoemd in art. 5.3 GIBIT. Bent u bereid te accepteren dat het door Leverancier aan te leveren plan van aanpak/implementatieplan prevaleert?	Niet akkoord.
25	Juridisch	Conceptovereenkomst	Hier wordt melding gemaakt van aanvullende afspraken. Leverancier wil graag een beeld vormen van de inhoud en de rechten en verplichten die GGD voor Leverancier voor ogen heeft. Kan GGD aangeven welke aanvullende afspraken zij wenst op te nemen? Bent u bereid deelnemers in de gelegenheid te stellen om vragen over eventuele aanvullende afspraken te stellen?	In gezamenlijk overleg kunnen aanvullende afspraken gemaakt worden, echter kunnen zij niet leiden tot een wezenlijke wijziging van de opdracht.
26	Juridisch	Conceptovereenkomst	In de overeenkomst wordt in art. 2.1 aangegeven dat die voor een periode van 4 jaar wordt afgesloten. Bent u met inschrijver van mening dat dit 2 jaar dient te zijn en de overeenkomst daarna eventueel tweemaal voor 1 jaar verlengd kan worden?	Zo staat het omschreven in de aansluitende zin van de conceptovereenkomst.
27	Inhoud	Asset management systeem	Beschikt GGD HN over een up-to-date asset management systeem waar de SIEM geautomatiseerd contact mee kan maken?	Nee
28	Juridisch	Artikel 27 GIBIT	In dit artikel wordt verwezen naar de Gemeentelijke ICT-kwaliteitsnormen. Kunt u aangeven welke normen relevant zijn in dit concrete geval en zou u – waar nodig – nader invulling willen geven aan de toepasselijke normen?	Zoals gepubliceerd door de VNG/VNG Realisatie.
29	Proces	Beoordelingscommissie	Welke rollen zitten in de beoordelingscommissie?	Teamleider ICT, systeembeheer, technisch specialist, projectleider. Procesbegeleiding door inkoop.
30	Inhoud	PVE - eis 10	In uw uitvraag vraagt u om encryption at rest, echter is de waarde van het encrypten van de data m.b.t. dataverwerking enkel en alleen door uw cyber security leverancier, bijna altijd lager dan de kosten voor de encryptie. Gaat u in plaats daarvan akkoord met een gedegen implementatieplan waarbij gevoelige informatie niet in het SIEM terecht komt, waardoor encryption at rest van de data niet meer noodzakelijk is en kosten bespaard kunnen worden?	Nee, we kunnen nu de scope tijdens het aanbestedingsproces niet wijzigen.
31	Inhoud	Bewaking van mobiele devices	In welke mate is de bewaking van mobiele devices gewenst ? Hoe ziet de mobiele device populatie er uit en hoe zijn deze beschermd ?	Niet van toepassing
32	Inhoud	Bijlage Offerteaanvraag Europees openbare aanbesteding SIEM SOC GGD Hollands Noorden - Pagina 7	Op welke termijn (bijvoorbeeld 1 maand, 1 jaar etc) verwacht GGD HN zelf de signalen te interpreteren en op te volgen.	6 maanden
33	Inhoud	Bijlage 1 Offerteaanvraag Europees openbare aanbesteding SIEM SOC GGD Hollands Noorden - Pagina 7	Het aantal logbronnen die initieel opgenomen moeten worden in het systeem zijn rond de 200. Wat is de definitie van een logbron volgens GGD HN en kunnen deze logbronnen gespecifiseerd worden in een lijst.	Denk hierbij aan actieve netwerk componenten en servers
34	Inhoud	Verwerking data	Is de beslissing van de EU om de GDPR-UK adequaat, en daarmee gelijk, aan de GDPR-EU te zien voor u reden om ook verwerking van data in het Verenigd Koninkrijk toe te staan?	We volgen het advies van de Autoriteit Persoonsgegevens.
35	Inhoud	Bijlage A Programma van Eisen - Eis 12	Gesteld: "Bescherming tegen insider threats. Monitoring en logging moet gericht zijn op zowel aanvallen van buitenaf als van binnenuit". Welke technische maatregelen zijn er getroffen die afwijkend oost-west netwerk verkeer opmerkt?	Geen

36	Inhoud	Bijlage A Programma van Eisen - Eis 12	Gesteld: "Bescherming tegen insider threats. Monitoring en logging moet gericht zijn op zowel aanvallen van buitenaf als van binnenuit". Welke technische maatregelen heeft de GGD getroffen om downloads op endpoints te voorkomen of te detecteren?	MS Defender, Conditional Access Policies
37	Inhoud	Bijlage A Programma van Eisen - Eis 12 Bescherming tegen insider threats	"Monitoring en logging moet gericht zijn op zowel aanvallen van buitenaf als van binnenuit". Welke maatregelen heeft de GGD getroffen om te loggen op applicatieniveau?	Geen
38	Inhoud	Bijlage A Programma van Eisen - Eis 12 Bescherming tegen insider threats	Gesteld: "Bescherming tegen insider threats. Monitoring en logging moet gericht zijn op zowel aanvallen van buitenaf als van binnenuit". Hoe heeft de GGD data geclassificeerd?	Niet
39	Inhoud	Bijlage A Programma van Eisen - Eis 13	Gesteld: "IDS/IPS (Intrusion Detection and Prevention) functionaliteit. “Hacker Alert”." Kan de GGD beschrijven welke security maatregelen bestaan (zoals firewalls, proxies, endpont security)?	Fortigate, MS Defender 365, mShield
40	Inhoud	Bijlage A Programma van Eisen - Eis 14	Gesteld: "Detecteren ongeautoriseerdeIT assetsop de infrastructuur van GGD HN". Kan de GGD aangeven welke endpoint security gebruikt wordt, welke tooling wordt ingezet voor vulnerability scanning en hoeveel endpoints bekend zijn?	MS Defender voor 1800/700 endpoints
41	Inhoud	Bijlage A Programma van Eisen - Eis 16	Gesteld: "SOC (Security Operations Center) functionaliteit. 24/7 actief, opvolging in overleg". Verwacht de GGD 24x7 'eyes on screen', of in de toekomst uitbreiding hier naar toe?	Toekomst
42	Inhoud	Bijlage A Programma van Eisen - Eis 16	Is er bij de GGD HN een 24X7 dienst welke te bereiken is na kantooruren voor het doorgeven van incidenten? Hoe kunnen deze incidenten worden doorgegeven, bv telefonisch, mail? Welk niveau IT-medewerkers hebben deze IT medewerkers, kunnen ze bv bij kritische incidenten systemen uitschakelen welke direct impact hebben op de continuïteit van de IT omgeving?	nader te bepalen niveau HBO systeem- en netwerkbeheer
43	Inhoud	Bijlage A Programma van Eisen - Eis 2 NEN 7510 compliant	Inschrijver ziet graag verduidelijking op uw eis 'NEN7510'-compliant. Omdat de gevraagde dienstverlening geen toegang zal hebben tot medische dossiers, lijkt ons een NEN7510-certificering overbodig. Inschrijver stelt voor om deze eis te wijzigen naar ISO27001-certificering. Gaat de GGD Hollands hiermee akkoord? Zo niet, dan ontvangt Inschrijver graag uw toelichting.	Ondanks dat de basis van beide normen hetzelfde is vinden wij de NEN 7510 als norm ontwikkeld voor informatiebeveiliging in de zorgsector van belang voor onze uitvraag. In deze norm worden maatregelen beschreven die zorginstellingen en toeleveranciers moeten nemen om op adequate wijze met patiëntgegevens om te gaan.
44	Inhoud	Bijlage A Programma van Eisen - Eis 20	Gesteld: "Dagelijkse updates over bedreigingen en de status van de technische informatie beveiliging richting IT-Beheer en ISO. Custom rapportage mogelijkheid." Inschrijver vermoedt dat het in het belang van de GGD is om real-time dashboards te hebben over status en dreigingen. Onderschrijft de GGD dit?	Ja
45	Inhoud	Bijlage A Programma van Eisen - Eis 22.	Wordt er verwacht vanuit de SIEM SOC oplossing een aanbieding te doen voor een alternatieve vulnerability management dienst?	Ja, maar is in deze out of scope
46	Inhoud	Bijlage A Programma van Eisen – Eis 22.	Welke vulnerability scanner wordt momenteel gebruikt door GGD HN?	Geen
47	Inhoud	Bijlage A Programma van Eisen - Eis 23.	Kunt u aangeven welke use-cases minimaal worden verwacht aanwezig te zijn in de bibliotheek?	Deze scope is onderdeel van de implementatie.
48	Inhoud	Bijlage A Programma van Eisen - Eis 25	Gesteld: "Heldere communicatie strategie, met name in geval van calamiteiten. Overzicht van contactpersonen en case-managers." Heeft GGD een incident response-plan?	Op dit moment nog niet beschikbaar, is in ontwikkeling
49	Inhoud	Bijlage A Programma van Eisen - Eis 5 Heldere afspraken (in SLA)	De GGD heeft geen expliciete eisen opgegeven waar de logging bewaard dient te worden. Kan inschrijver ervan uit gaan dat de data binnen de Europese Unie bewaard moet worden?	Die aanname is correct.
50	Inhoud	Bijlage A Programma van Eisen - Eis 9 Ondersteunen audit-trails en logging	Heeft de Opdrachtgever specifieke eisen voor de retentietijden?	De retentietijd hangt af van prijs en risico.
51	Inhoud	Bijlage D: PRIJSINVULFORMULIER - Excel	De aangeboden SIEM SOC dienst is gelicenseerd op de totale som van het aantal assets in de GGD HN omgeving (workstations, desktop, laptops & servers zowel virtuele als fysieke systemen.) Kunt u aangeven hoeveel assets GGD HN heeft in de totale omgeving?	1200 laptops (tijdens Coronaperiode), normaal ongeveer 700 laptops, 40 virtuele servers
52	Inhoud	Bijlage D: PRIJSINVULFORMULIER - Excel	De door ons aan te bieden n SIEM SOC dienst is gelicenseerd op de totale som van het aantal assets in de GGD HN omgeving (workstations, desktop, laptops & servers zowel virtuele als fysieke systemen.) Kunt u aangeven hoeveel assets GGD HN heeft in de totale omgeving?	1200 laptops (tijdens Coronaperiode), normaal ongeveer 700 laptops, 40 virtuele servers
53	Proces	Bijlage F - (Concept)raamovereenkomst - Artikel 5 Vergoeding vs Bijlage D - Prijsinvulformulier	Inschrijver constateert dat Bijlage D onderdeel is van de Inschrijving (Raamovereenkomst § 5), echter maakt dit document geen onderdeel uit van de In te dienen documenten (Offerte aanvraag, II.7). Inschrijver stelt voor om Bijlage D op TenderNed onder Gunningscriteria 2 Prijs te uploaden. Gaat de Aanbestedende dienst hiermee akkoord.	Bijlage D, het prijsinvulformulier is als Excel bestand bij de aanbestedingsdocumenten geupload.
54	Juridisch	Bijlage G - GIBIT 2020 - Artikel 13.3	Opdrachtnemer wil aansprakelijkheid maximaliseren tot EUR 1.250.000 per gebeurtenis, waarbij een reeks van samenhangende gebeurtenissen als één gebeurtenis wordt beschouwd en tot maximaal EUR 3.000.000 in totaal. Kunt u hiermee instemmen? Indien u hiermee niet kan instemmen, kunt u aangeven waarom niet en eventueel een alternatief voorstel aandragen?	Zie eerdere beantwoording.

55	Juridisch	Bijlage G - GIBIT 2020 - Artikel 13.4	Opdrachtnemer wenst dat Aansprakelijkheid voor schade door stilstand, productieverlies of verlies van data (indirecte schade) ook is uitgesloten van compensatie. Dit dient niet alleen bij ARBIT 2020 en te zijn uitgesloten maar voor alle documenten die horen bij de Raamovereenkomst die gedurende de looptijd horen bij te leveren Prestatie. Is dit akkoord? We wensen de reden te vernemen in geval er afwijkend van ons voorstel wordt geoordeeld.	Zie eerdere beantwoording.
56	Juridisch	Bijlage G - GIBIT 2020 - Artikel 17.4	Opdrachtnemer verzoekt Opdrachtgever dit artikel niet van toepassing te verklaren omdat Opdrachtnemer niet in het bezit is van broncodes en deze door de fabrikant niet ter beschikking worden gesteld. Gaat u hiermee akkoord? Zo niet, waarom niet en kunt u dit motiveren?	Vermoedelijk verwijst u naar art 17.5. Broncodes worden gevraagd bij nieuw te ontwikkelen programmatuur.
57	Juridisch	Bijlage G - GIBIT 2020 - Artikel 4.1/5.5	Opdrachtnemer vindt in artikel 4.1/5.5 niet redelijk, daarom wenst opdrachtnemer het voldoende op te nemen in plaats van deze artikelen, 'Indien overeengekomen termijnen voor leveringen of prestatie van diensten overschreden worden zal Opdrachtgever de Leverancier schriftelijk in gebreke stellen waarbij Leverancier een redelijke termijn voor nakoming wordt gesteld. Het verzuim treedt in als nakoming binnen deze redelijke termijn achterwege blijft.' Kunt u hiermee instemmen? Zo niet waarom niet en kunt u dit onderbouwen?	Zie eerdere beantwoording.
58	Contract	Bijlage H - Verwerkersovereenkomst	De aanbestedingsstukken bevatten een concept verwerkersovereenkomst. Gegadigde acteert als intermediair/reseller in deze aanbesteding. Bij het opstellen van een verwerkersovereenkomst is het belangrijk om te bepalen wie daadwerkelijk verwerker is. Om dit te kunnen vaststellen dient de data gevolgd te worden. Bij het leveren en/of verhuren van licenties c.q. gebruiksrechten (zoals opgenomen in de scope van deze aanbesteding) is nimmer sprake van het verwerken van persoonsgegevens. Dit aangezien gegadigde simpelweg géén toegang tot enige persoonsgegevens heeft. Een verwerkersovereenkomst kan dan ook niet van toepassing zijn op de onderhavige (raam)overeenkomst en dient enkel afgesloten te worden in het geval een software fabrikant persoonsgegevens verwerkt. In dergelijke gevallen zal gegadigde de concept verwerkersovereenkomst meesturen met de uitvraag naar de desbetreffende software fabrikant. In het geval dat de desbetreffende fabrikant aangemerkt wordt als verwerker van persoonsgegevens zal gegadigde volledig meewerken en zich maximaal inspannen om de verwerkersovereenkomst te laten ondertekenen door de desbetreffende software fabrikant (verwerker). Echter, gegadigde kan niet op voorhand akkoord geven dat de desbetreffende fabrikant (en de verwerker van de persoonsgegevens) de concept verwerkersovereenkomst accepteert. Graag uw akkoord?	Nee
59	Inhoud	Buitenlocaties	Verwacht GGD HN dat alleen het DC wordt gemonitord of heeft GGD HN ook de verwachting dat de 40 buitenlocaties worden meegenomen in de monitoring? Zo ja, zijn daar relevante systemen aanwezig en wordt er verwacht dat er ook netwerkmonitoring aanwezig is?	Netwerkmonitoring DC en buitenlocaties
60	Inhoud	Capaciteit	Wat is de maximale capaciteit per virtuele appliance (RAM/vCPU/Storage)?	nader te bepalen
61	Contract	Concept Overeenkomst, Artikel 2.1 & Offerteaanvraag, paragraaf I.2, p.7.	De onderhavige overeenkomst kan (optioneel) tweemaal door Opdrachtgever worden verlengd voor de duur van één jaar. Een verlenging van een overeenkomst moet door alle betrokken partijen geaccepteerd worden. Er dient immers wilsovereenstemming tussen de betrokken partijen te zijn. Gegadigde verzoekt de aanbestedende dienst om artikel 2.1 aan te passen met dat Opdrachtnemer eveneens dient in te stemmen (wederzijdse instemming) met de ingeroepen mogelijkheid tot verlenging van de overeenkomst.	Niet akkoord.
62	Inhoud	PVE - Eis 14	Is er een overzicht van alle geautoriseerde IT assets beschikbaar en is het niet logischer om toegang hardwarematig af te schermen met bijvoorbeeld MAC-filtering? Wordt er gebruik gemaakt van BYOD?	Geen BYOD, overzicht IT Assets beschikbaar.
63	Inhoud	PVE 23	Is het voldoende wanneer de GGD de usecases aanmaakt voor eigen gebruik? Custom Use Cases die door ons SOC worden gemonitord kunnen alleen in overleg worden opgeleverd.	Dat is niet voldoende
64	Inhoud	Plafondbedrag	Kan Opdrachtgever motiveren hoe het plafondbedrag van € 100.000 op jaarbasis tot stand is gekomen?	Dit betreft het beschikbare budget.
65	Inhoud	Datacenters	Beschikt Opdrachtgever over 1 Datacenter? Indien nee hoeveel Datacenters heeft Opdrachtgever ?	1 Datacenter

66		Diensten en functionaliteiten. Punt 13.	IDS/IPS is in vele varianten te vormen. Ten eerste is er een groot verschil tussen IDS en IPS waarbij IPS protectie biedt en vaak in de vorm van subscriptions/licenties op NG-Firewalls beschikbaar is. IDS kan een “inform only” variant zijn van de IPS subscription maar kan ook gevormd worden door volwaardige NDR (Network Detect and Respond) oplossingen zoals bijvoorbeeld ook binnen onze SOC-NDR dienst geboden. Voor SOC-SIEM is IDS/IPS een logbron. - Heeft u IDS/IPS momenteel geimplementeerd welke als SIEM logbron geschikt is? - Zo ja: Kunt u de details hiervan delen? (welke oplossing) - Zo nee: Ziet u een aanbieding voor IDS/IPS als onderdeel van de scope van deze uitvraag? - Hoe gaat u dit wegen daar de prijs van de aanbieding hiermee voor u negatief beinvloed wordt maar de kwaliteit van de omgeving omhoog gaat? - Indien u IDS/IPS als onderdeel van deze uitvraag ziet, kunt u een architertuur-plaat delen? Deze is benodigd om een goed IDS/IPS advies hierin te kunnen geven.	- Nee - - Het beschikbare budget bepaalt de scope. - -
67		Diensten en functionaliteiten. Punt 14.	Dit begint (uiteraard) met het weten wat WEL geautoriseerde assets zijn. Een volledige CMDB van alle assets en/of een volwaardige NAC oplossing vormt hier de basis. Om vervolgens juiste detecties te kunnen doen zullen alle infrastructuur-connecties ofwel gelogd moeten worden (dus alle switchpoorten, wireless, remote access etz) ofwel gemonitord moeten worden (bv via een NAC oplossing of NDR omgevingen). - Heeft u momenteel een actuele en volledige CMDB van geautoriseerde IT assets? Zo ja: in welk vorm/oplossing? - Heeft u momenteel een NAC oplossing? Zo ja: in welke vorm/oplossing?	- Ja, deze in ontwikkeling en wordt gecomplementeerd. - Nee
68	Inhoud	Eyes on screen	Kan GGD HN nader uitleggen wat zij precies verstaat onder een 24/7 actief SOC? Betekent dit 24/7 'eyes on screen' of consignatie/piketdienst?	24/7 monitoring in combinatie met consignatie/piketdienst
69	Uitvoering	FTE beschikbaarheid GGD HN personeel	Hoeveel eigen of ingehuurde GGD HN Security & IT FTE’s zijn er beschikbaar ter ondersteuning van de Implementatie, borging van de interne security processen en security incident response in het Jaar 2022, 2023, 2024, 2025?	1 FTE
70	Inhoud	Geselecteerde oplossingen	In welke mate zijn de oplossingen die GGD GHOR geselecteerd heeft voor een gelijkwaardig vraagstuk relevant voor GGD Hollands Noorden ?	Kunnen relevant zijn voor de toekomst. Ons is niet bekend dat GGD GHOR een keuze gemaakt heeft.
71	Inhoud	GGD HN netwerk & IP-devices	– Hoeveel Actieve interne IP devices zijn er op het totale GGD HN WAN netwerk ? – Hoeveel Actieve Centrale VLANs / Subnetten zijn er? – Hoeveel Actieve Decentrale VLANs / Subnetten zijn er? (op de locaties)	- ± 4000 devices - ± 5 vlan's centraal - ± 55 vlan's decentraal
72	Juridisch	GIBIT 2020 Algemeen	Aanbieder meent dat de GIBIT voorwaarden zeer specifiek zijn geschreven voor ICT contracten en derhalve niet geschikt zijn voor, bijvoorbeeld, telecommunicatiediensten en daaraan verbonden diensten. In het commentaar heeft aanbieder niet alleen rekening gehouden met de in de eerste zin genoemde vaststelling, maar ook met het commentaar dat door Nederland ICT is gegeven op de (concept) voorwaarden voor zover dit commentaar voor aanbieder relevant is en niet reeds in de definitieve tekst opgenomen is.	Naar onze mening is het onderwerp van deze aanbesteding niet specifiek telecommunicatiediensten en lijkt uw opmerking niet relevant.
73	Juridisch	GIBIT 2020 Artikel 12 lid 2	Graag 12 lid 2 laten vervallen Leverancier kan Opdrachtgever niet zomaar toelaten tot de besprekingen met haar klanten (derden). Hiervoor is immers ook de instemming van deze klanten noodzakelijk. Kunt u hiermee instemmen?	Niet akkoord, er wordt niet gevraagd om toegelaten te worden bij besprekingen met klanten.

74	Juridisch	GIBIT 2020 Artikel 13	Graag geheel vervangen: Graag geheel vervangen door: 13.1 Partijen aanvaarden over en weer slechts wettelijke verplichtingen tot schadevergoeding voor zover dat uit dit artikel en de navolgende artikelen blijkt. 13. 2 Partijen zijn aansprakelijk voor de door de andere partij geleden directe schade indien de aanspraken zijn ontstaan: • Een gevolge van een toerekenbaar tekortschieten in de nakoming van een of meerdere verplichtingen in haar verplichtingen jegens de andere partij; • Een gevolge van een buitencontractueel toerekenbaar handelen of nalaten bij de werkzaamheden die de andere partij haar medewerkers en/of haar onderaannemers verricht ter uitvoering van deze Overeenkomst. 13.3 Aansprakelijkheid van Partijen voor indirecte schade, daaronder begrepen gevolgschade, gederfde winst, gemiste besparingen, verlies van gegevens, gegevensbestanden en schade door bedrijfsstagnatie, is nadrukkelijk uitgesloten. 13.4 Dit artikel is van overeenkomstige toepassing op vrijwaring. 13.5 De Partij die toerekenbaar tekortschiet in de nakoming van zijn verplichtingen is tegenover de andere Partij uitsluitend aansprakelijk voor de door de andere Partij geleden of te lijden directe schade. 13.6 De hierboven bedoelde aansprakelijkheid voor directe schade is, per gebeurtenis, beperkt tot een bedrag van € 1.000.000,- per gebeurtenis, waarbij een reeks van samenhangende gebeurtenissen aangemerkt zal worden als één gebeurtenis, zulks met een maximum van € 2.000.000,- per kalenderjaar. Onder directe schade wordt uitsluitend verstaan: a. Schade aan producten en functies, waaronder in elk geval verstaan wordt: materiële beschadiging, gebrekkig of niet	Wij vermoeden dat u verwijst naar de GIBIT 2016, artikel 13 van de GIBIT 2020 is van toepassing.
75	Juridisch	GIBIT 2020 Artikel 14 lid 2	Graag schrappen Aanbieder zal een deugdelijke verzekering aanhouden. 14.1 is afdoende. Kunt u daarmee instemmen?	Artikel 14.2 blijft van kracht
76	Juridisch	GIBIT 2020 Artikel 15 lid 5	15 lid 5 laten vervallen Een boete op het schenden van een geheimhoudingsverplichting is niet marktconform. Indien uit schending geheimhouding schade voortkomt. Zal op basis van artikel 6:74 BW eventueel schade vergoed moeten worden. Indien desalniettemin een boete wordt opgelegd, dient deze in mindering te worden gebracht op schadevergoeding om te voorkomen dat Opdrachtgever zich ongerechtvaardigd zou verrijken. Zie ook artikel 6:92 lid 2 BW. Kunt u daarmee instemmen?	Het begroten van het schadebedrag bij schending is lastig te bepalen. Artikel 15.5 blijft van kracht net zoals het kader uit het BW.
77	Juridisch	GIBIT 2020 Artikel 20 lid 2	Graag verwijderen: heel artikel 20 lid 2. Te allen tijde het recht hebben om de overeenkomst op te zeggen is niet redelijk en kan commercieel ook niet altijd worden aangeboden. Looptijden en volume hebben een directe invloed op aangeboden werkzaamheden en vergoedingen. Kunt u hiermee instemmen?	Uw opmerking kunnen wij niet plaatsen in relatie tot GIBIT 2020 artikel 20 lid 2.
78	Juridisch	GIBIT 2020 Artikel 21 lid 1	Graag toevoegen na "gerechtigd": "indien overeengekomen, op de overeengekomen wijze" Auditrechten dienen specifiek te worden overeengekomen. Hetzelfde geldt voor de wijze van uitvoeren van de audit. Aanbieder heeft een eigen afdeling Audit waarmee hierover afspraken gemaakt kunnen worden. Kunt u hiermee instemmen?	In artikel 20 lid 1 gaat het over dat de controle moet zien op de nakoming van wezenlijke verplichtingen. Toevoeging lijkt niet relevant.
79	Juridisch	GIBIT 2020 Artikel 21 lid 3	Graag toevoegen voor "toegang verlenen tot de locatie": "indien mogelijk" Het is voor de leverancier niet altijd mogelijk toegang te verlenen tot de locatie waar de diensten worden verleend. Bijvoorbeeld in het geval de diensten worden verleend op een locatie van de Opdrachtgever en/of op een locatie van derde partijen. Kunt u hiermee instemmen?	In artikel 21 lid 3 staat niets opgenomen over de locatie.

80	Juridisch	GIBIT 2020 Artikel 21 lid 6	Graag verwijderen: ", tenzij de derde één of meer tekortkomingen van Leverancier constateert" Zo algemeen, voorbijgaand aan de aard en ernst van de tekortkoming, kan deze eis niet worden gesteld. Indien kosten voor rekening van de leverancier worden gebracht, moet dat proportioneel zijn en in verhouding tot de aard en ernst van de tekortkoming. Indien de tekortkoming zodanig is dat de leverancier schadevergoedingsplichtig is, zullen eventueel ook de kosten kunnen worden gevorderd van de controle. Het is onredelijk dit bij voorbaat ongeclausuleerd op te nemen. Kunt u hiermee instemmen?	Niet akkoord, zie de bepaling in lid 1 en eerdere beantwoording.
81	Juridisch	GIBIT 2020 Artikel 3 lid 2 i	Onder (i) In plaats van "Doelstellingen" beter om te spreken over bijvoorbeeld "Het door Opdrachtgever beoogde gebruik van de Prestatie, zoals dat door de Opdrachtgever kenbaar is gemaakt." Doelstellingen kunnen tegenstrijdig zijn. Hier ligt een taak voor de Opdrachtgever om de leverancier daarover te informeren. Kunt u hiermee instemmen?	Het doel van de aanbesteding dient voor Inschrijver duidelijk te zijn. Er wordt een pro actieve houding van inschrijver verwacht als dat niet helder is (zie ook art 3.3).
82	Juridisch	GIBIT 2020 Artikel 3 lid 3	Graag de volgende woorden toevoegen aan artikel 3 lid 3: "en Opdrachtgever zal ook (proactief) de Leverancier tijdig van adequate informatie voorzien." Goede informatieverschaffing door Opdrachtgever is essentieel voor goede overeenstemming tussen partijen over de ICT- Prestatie. Kunt u hiermee instemmen?	Akkoord.
83	Juridisch	GIBIT 2020 Artikel 4 lid 1	Voorstel: Overeengekomen termijnen voor levering en/of andere prestaties gelden niet als vast en fataal, tenzij schriftelijk anders overeengekomen. Alle termijnen definiëren als fataal is onredelijk. Een nadrukkelijk als zodanig door partijen overeengekomen termijn kan als fataal worden gedefinieerd. Uitgangspunt zou moeten zijn dat termijnen niet worden overschreden. Mocht dit onverhoopt toch plaatsvinden dan zou de leverancier een redelijke termijn moeten worden gegund (ingebrekestelling) om na te kunnen komen voordat de Leverancier in verzuim geraakt. Dat is redelijk en ook gebruikelijk binnen de IT branche. Kunt u hiermee instemmen?	U verwijst naar de GIBIT 2016 in de van toepassing verklaarde GIBIT 2020 is dit aangepast.
84	Juridisch	GIBIT 2022 Artikel 20 lid 1	Graag wederkerig maken: "Partijen zijn over en weer niet gerechtigd hun verplichtingen op te schorten dan na het sturen van een ingebrekestelling, waarin aan de andere partij een redelijke termijn (….)" Dit artikel dient in evenwicht te worden gebracht door het wederkerig te maken. Kunt u hiermee instemmen?	Niet akkoord.
85	Contract	GIBIT art. 13.3 en 13.4	Gezien de te verwachten opdrachtwaarde en hetgeen gebruikelijk is in onze markt (1x tot 2x de Jaarvergoeding per jaar) zijn wij van mening dat de aansprakelijkheid buiten proportioneel hoog is. Bent u bereid om dit bedrag (ook met betrekking tot zaakschade (zie artikel 13.3) te verlagen naar € 500.000 per jaar? Mocht u daartoe niet bereid zijn, kunt u motiveren waarom deze hoge aansprakelijkheid proportioneel is?	Wij vermoeden dat u verwijst naar de GIBIT 2016, artikel 13 van de GIBIT 2020 is van toepassing.
86	Contract	GIBIT, art. 1.26	Bent u bereid overeen te komen dat dit artikel luidt: “Overeengekomen gebruik: het door Opdrachtgever beoogde gebruik van de ICT Prestatie zoals dat ten tijde van het sluiten van de Overeenkomst kenbaar is gemaakt aan Leverancier."?	Vermoedelijk verwijst u naar art 1.23. Daar staat de definitie.
87	Contract	GIBIT, art. 13	Bent u bereid de aansprakelijkheid, zoals te doen gebruikelijk in de branch, te beperken tot directe schade en daarmee indirecte schade uit te sluiten? Zo nee, kunt u toelichten waarom u hiertoe niet bereid bent?	Niet akkoord, zie ook eerdere beantwoording.
88	Contract	GIBIT, art. 13.5, sub iii en sub iv	Onbeperkte aansprakelijkheid is voor leveranciers niet verzekerbaar en derhalve een groot risico. Tevens schrijft Voorschrift 3.9 D Gids Proportionaliteit voor dat de aansprakelijkheid gelimiteerd moet worden. Bent u derhalve bereid deze bepalingen te laten vervallen, waarmee de aansprakelijkheidslimiet als bedoeld in artikel 13.4 op deze situatie van toepassing is? Zo niet, kunt u motiveren waarom niet?	Wij vermoeden dat u verwijst naar de GIBIT 2016, artikel 13 van de GIBIT 2020 is van toepassing. Hier is geen sprake van onbeperkte aansprakelijkheid.

89	Contract	GIBIT, art. 20.11	Bent u akkoord om de volgende bepaling op te nemen in de overeenkomst? “In afwijking van artikel 20.11 GIBIT komen partijen overeen dat Opdrachtgever de Overeenkomst niet kan ontbinden wegens het enkele feit dat sprake is van een fusie, splitsing of overname van Leverancier, behalve wanneer dit wezenlijke aanpassingen in de uitvoering van de Overeenkomst meebrengt.”	Het gaat hier om situaties waarbij het in redelijkheid niet van Opdrachtgever kan worden gevergd om de Overeenkomst voort te zetten. Uiteraard is het bij inroepen van al deze ontbindingsgronden aan Opdrachtgever om te bewijzen dat deze gronden zich daadwerkelijk voordoen. In artikel 20.11 wordt niet gesproken over fusies e.d.
90	Contract	GIBIT, art. 6.1	Kunt u specificeren aan welke Gemeentelijke ICT kwaliteitsnormen de ICT Prestatie moet voldoen?	Zoals gepubliceerd door de VNG/VNG Realisatie.
91	Contract	GIBIT, art. 7	In de GIBIT staat geen termijn waarbinnen de Acceptatieprocedure door Opdrachtgever moet worden doorlopen. Wij zouden graag de afspraken hierover SMART vast willen leggen en stellen daarom voor om de onderstaande artikelen toe te voegen. Kunt u hiermee akkoord gaan? a. Opdrachtgever deelt binnen 14 dagen na oplevering aan Leverancier mee of hij de ICT Prestatie accepteert. Hij kan dat doen door een expliciet daarvoor bedoelde mededeling of door toezending van het testverslag. b. Indien Opdrachtgever niet in staat is om binnen de in artikel a genoemde termijn aan Leverancier mee te delen of hij de ICT Prestatie accepteert, meldt hij dat voor afloop van die termijn aan Leverancier onder opgaaf van redenen en van de termijn waarbinnen hij alsnog wel aan Leverancier zal meedelen of hij de ICT Prestatie accepteert. c. Bij het uitblijven van enige mededeling als bedoeld in artikelen a en b alsmede in het geval de aanvullende termijn voor Acceptatie, als bedoeld in artikel b, zonder nader bericht van Opdrachtgever is verstreken, geldt de ICT Prestatie als door Opdrachtgever geaccepteerd.	Niet akkoord, zie ook de bepalingen in art 5.2 GIBIT 2020.
92	Contract	GIBIT, art. 8.10, 10.1 en 19.2	Garanties en de gevolgen van garanties zijn niet wettelijk bepaald. In deze setting (deze aanbesteding) zal Leverancier enkel diensten verlenen. Opdrachtgever zal zich daarvoor inspannen (zoals van een vakbekwaam ICT leverancier mag worden verwacht) maar daarvoor is geen garantie af te geven, gericht op een bepaald resultaat waarbij Leverancier bij het niet behalen van het resultaat direct in verzuim is. Kunt u ermee instemmen om expliciet te maken dat indien de garanties onder deze aanbesteding niet worden nagekomen, Leverancier een redelijke termijn wordt gegund alsnog aan de verplichting te voldoen?	Wij kunnen uw opmerkingen niet plaatsen in relatie tot de artikelen waarnaar verwezen wordt.
93		GIBIT2020	Inschrijver mag vanuit de holding niet accoord gaan met alle in de GIBIT2020 gestelde regelementen. Gaat opdrachtgever er mee akkoord dat voor opdrachtverstrekking overleg plaats vindt, waarin op een aantal onderwerpen naar redelijkheid en billikheid maatwerk-afspraken worden gemaakt?	Naast de bepalingen in de GIBIT is het Burgerlijk Wetboek (en andere wetgeving) onverkort van toepassing.
94	Uitvoering	Huidige beschikbaarheid & bereikbaarheidstijden	Wat zijn de officiële werktijden, telefonische bereikbaarheidstijden, officiële piket-tijden en diensten? van de eigen of ingehuurde GGD HN Security en IT / crisis managers en ook van de IT leveranciers van GGD HN kritieke infrastructuur? (Volgens de huidige formele SLA & contract afspraken)	nader te bepalen
95	Inhoud	Hypervisor	Welke hypervisor gebruikt GGD HN?	VMware
96	Inhoud	Plafondbedrag	Kan Opdrachtgever motiveren waarom voor een plafondbedrag is gekozen in plaats van de tarieven volledig door de markt (lees: de inschrijvers) te laten vaststellen? Is Opdrachtgever zich bewust van het mogelijk uitsluitende karakter van het genoemde plafondbedrag van € 100.000 op jaarbasis?	Een plafondbedrag is gekozen omdat dit het budget is. Het overlaten aan de markt zou disproportioneel kunnen zijn indien er niet gegund zou kunnen worden i.v.m. ontoereikend budget.
97	Juridisch	Bijlage 3	Komt de medewerking die Leverancier in het kader van de verwerkersovereenkomst levert – waaronder audits en een eventuele gegevensbeschermingseffectbeoordeling – voor vergoeding in aanmerking?	Nee.
98	Inhoud	Implementatie en training	Voor veel van de opdrachtgevers in de Nederlandse markt is Nederlandstalige implementatie en training een vereiste. Geldt dit ook voor Opdrachtgever ?	Ja
99	Inhoud	Incident response team	Het de beschikking hebben over een eigen incident response team is vaak een vereiste in SIEM/SOC trajecten, hoe kijkt GGD Hollands Noorden hier tegenaan?	Op den duur is dat de bedoeling
100	Inhoud	Internet breakout punten	Over hoeveel internet breakout punten beschikt GGD HN?	twee
101	Inhoud	Internet capaciteit	Wat is de maximale internet capaciteit? En wat is het gemiddelde verbruik?	nader te bepalen
102	Inhoud	Internet connectiviteit	– Is alle GGD HN Internet connectiviteit via een centraal punt ontsloten? – Is de GGD HN Internet connectiviteit dubbel uitgevoerd ? over 2 verschillende fysieke locaties? – Welke technische mogelijkheden zijn er om centraal het belangrijkste interne verkeer en Internet verkeer “af te tappen/kopiëren”, bijvoorbeeld via een SPAN-port op core switches/routers/firewalls? – Welke technische interfaces en hoeveel zijn hiervoor nodig ? (Glas/Koper/ 1Gb /10Gb etc…) – Wat is de gemiddelde bandbreedte gebruik en Piek verkeer van de Internet connectiviteit? – Wat is de gemiddelde bandbreedte gebruik en Piek verkeer van het centraal belangrijkste interne verkeer ? (bijvoorbeeld naar de centrale / Azure servers)	- ja - nee -is mogelijk om in te stellen -onbekend -onbekend -onbekend

103	Inhoud	ITSM	Beschikt GGD HN over een ITSM (API/Webhook) zodat er geautomatiseerde koppeling kan worden gerealiseerd tussen GGD HN en inschrijver?	Nee
104	Inhoud	Kerncompetentie 1	Wij bieden een SIEM-oplossing dat zeer goed door Gartner (leader in het magic quadrant) wordt beoordeeld en dat wij binnen één maand bewezen kunnen implementeren. We hebben echter nog geen implementatie gedaan volgens NEN 7510. Bent u bereid om aan deze eis "of ISO 27001" toe te voegen, omdat deze twee normen grotendeels overeenkomen? Zo nee, kunt u toelichten waarom u deze eis niet wenst aan te passen.	Ondanks dat de basis van beide normen hetzelfde is vinden wij de NEN 7510 als norm ontwikkeld voor informatiebeveiliging in de zorgsector van belang voor onze uitvraag. In deze norm worden maatregelen beschreven die zorginstellingen en toeleveranciers moeten nemen om op adequate wijze met patiëntgegevens om te gaan.
105	Inhoud	Kerncompetentie 2	Kerncompetentie luidt als volgt: "Het opvolgen van loggegevens van aanvallen en verdacht gedrag vanuit de ICT-infrastructuur om mogelijke risico's op korte termijn te voorkomen bij een organisatie met meer dan 1.000 medewerkers." Het in de kerncompetentie gevraagde aantal medewerkers is groter dan het aantal medewerkers dat daadwerkelijk in dienst is bij GGDHN (conform uw programmabegroting 2022 zijn dit 463 voor de GGD (239 voor Corona)). Ben u bereid het in de kerncompetentie gevraagde aantal medewerkers, in het kader van de proportionaliteit, terug te brengen tot maximaal het aantal medewerkers dat u daadwerkelijk in dienst heeft?	Nee, in deze tijd van pandemie is het aantal medewerkers in vaste dienst niet relevant.
106	Inhoud	Kerncompetentie 2	Kerncompetentie d luidt als volgt: "Het opvolgen van loggegevens van aanvallen en verdacht gedrag vanuit de ICT-infrastructuur om mogelijke risico's op korte termijn te voorkomen bij een organisatie met meer dan 1.000 medewerkers." Het aantal medewerkers is veelal niet bepalend voor de complexiteit van het opvolgen van logggegevens. Deze complexiteit wordt eerer bepaald door het aantal assets dat gemonitord moet worden. Mag in deze kerncompetentie de term "medewerkers" ook vervangen worden door "assets"?	Nee
107	Proces	Language	Is it possible to submit our solution in English?	Nee, zie deel II.2 van het aanbestedingsdocument.
108	Contract	Licentie contract commitment	De meeste Security product leveranciers geven extra korting bij een Licenties commitment vanaf 3 jaar, staan jullie hiervoor open om de structurele kosten te verlagen?	Ja
109	Contract	Licentievoorwaarden	Bent u bereid om in het licht van artikel 19.1 van de GIBIT de licentievoorwaarden van de leverancier van onze SIEM-oplossing van toepassing te laten verklaren. Deze voorwaarden zijn wereldwijd op al hun klanten van toepassing en zoals gebruikelijk bij software en SaaS-diensten maken zij geen aparte afspraken met klanten. Mocht u hiermee niet akkoord gaan, kunt u toelichten waarom u hiermee niet akkoord kunt gaan?	Licentievoorwaarden van de leverancier kunnen niet zonder meer van toepassing verklaard worden. Artikel 19.1 bepaalt dat Leverancier de relevante derdenprogrammatuur uitdrukkelijk in zijn aanbod moet specificeren.
110	Inhoud	Llogbronnen	Opdrachtgever spreekt over ongeveer 200 logbronnen. Over welke logbronnen spreken we dan?	Actieve netwerkcomponenten en servers, SaaS en Azure
111	Proces	Beoordelingscommissie	Kunt u aangeven uit hoeveel personen en welke rollen de beoordelingscommissie voor G2.1 (Plan van Aanpak) bestaat?	Teamleider ICT, systeembeheer, technisch specialist, projectleider. Procesbegeleiding door inkoop.
112	Proces	NEN 7510	Wat bedoelt aanbestedende dienst precies met eis 2 NEN 7510 compliant? Aan de hand waarvan wenst aanbestedende dienst dit te toetsen? Op welke punten anders dan ISO 27001 verwacht aanbestedende dienst dat inschrijver compliant is?	U dient NEN 7510 gecertificeerd te zijn.
113	Juridisch	NEN 7510 kerncompetentie	In kerncompetentie 1 wordt net als in de PvE NEN 7510 vereist. Wat bedoelt aanbestedende dienst precies met leveren en implementeren volgens NEN 7510 anders dan ISO 27001? NEN 7510 is een wettelijke verplichting voor zorgorganisaties, als deze kerncompetenties om die reden ziet op zorgorganisaties dan wil inschrijver aanbestedende dienst verzoeken deze kerncompetenties breder te omschrijven. Zodanig dat inschrijver ook kan terugvallen op referenties uit andere sectoren, zoals vitale sector bedrijven. Kunt u hiermee akkoord gaan? Kunt u uw antwoord zonodig nader toelichten?	Ondanks dat de basis van beide normen hetzelfde is vinden wij de NEN 7510 als norm ontwikkeld voor informatiebeveiliging in de zorgsector van belang voor onze uitvraag. In deze norm worden maatregelen beschreven die zorginstellingen en toeleveranciers moeten nemen om op adequate wijze met patiëntgegevens om te gaan.
114	Inhoud	NEN7510	Opdrachtgever bevraagt nadrukkelijk NEN7510 compliance Is gelijkwaardig of strikter ook akkoord voor Opdrachtgever ?	Vereist is NEN 7510. Gelijkwaardig of strikter is opdrachtgever niet mee bekend.
115	Inhoud	Offerteaanvraag - Deel I.1 Inhoud van de opdracht	Inschrijver vraagt aan de GGD om specifieker te zijn over: "het opleiden van een viertal medewerkers van de GGD HN om op termijn zelf de signalen te interpreteren en op te volgen" Wat is het huidige opleidingsniveau van de vier medewerkers? Welke functie hebben deze medewerkers? Wat wordt de rol van deze medewerkers als de SOC dienst actief is?	HBO niveau, systeem- en netwerkbeheer

116	Inhoud	Offerteaanvraag - Deel II.1 Aanbestedingsprocedure	Inschrijver merkt op dat het snel implementeren van de oplossing van groot belang is voor de GGD. Mede ook door het dringende verzoek van de Autoriteit Persoonsgegevens zoals vermeld op pagina 9 van de offerteaanvraag. De afgegeven planning in het plan van aanpak is niet bindend, althans er is geen milestone opgenomen wanneer de dienst live moet zijn. Inschrijvers hoeven ook in het eisen overzicht geen "commitment" af te geven dat de dienst tijdig is opgeleverd zodat de GGD geen boetes krijgt opgelegd door de Autoriteit Persoonsgegevens. Er zijn ook geen boetes voor het te laat implementeren van de oplossing in de GIBIT en in de raamovereenkomst opgenomen. Inschrijver denkt dat het opleveren van de dienst op korte termijn van essentieel belang is voor de GGD. Kan de GGD toelichten hoe belangrijk de tijdige implementatie is, concrete data hiervoor opnemen en hier consequenties aan verbinden om te voorkomen dat hier onduidelijkheid over bestaat?	De toelichting is reeds gegeven, Concrete data opgeven is nu niet realistisch. Wij verwachten van inschrijver een pro actieve houding en het bewustzijn van de urgentie.
117	Inhoud	Offerteaanvraag Aanbestedingsprocedure	De AP heeft de GGD opgedragen om op korte termijn meer maatregelen te nemen om persoonsgegevens beter te beschermen. Het blijkt dat er nog steeds wezenlijke risico's bestaan voor de bescherming van persoonsgegevens bij het testen, vaccineren en het bron- en contactonderzoek tijdens de coronapandemie. Is de opdracht primair bedoeld om de bescherming van persoonsgegevens te waarborgen? Zoja, kan Opdrachtgever aangeven welke logbronnen en usecases gebruikt moeten worden om de bescherming van de persoonsgegevens te kunnen monitoren?	dat is niet mogelijk
118	Inhoud	Offerteaanvraag EU GGD HN SIEM SOC	Inschrijver leest in DEEL: V GUNNINGSCRITERIUM EN BEOORDELING "Voor G1.1 de jaarlijkse structurele kosten (abonnementstarief) geldt een plafondbedrag van € 100.000 excl. btw op jaarbasis." Wat verstaat opdrachtgever onder abonnementstarief? Is dit plafondbedrag uitsluitend voor de SOC diensten, of is dit inclusief aanschaf van licenties?	Dit betreft inclusief licentiekosten.
119	Inhoud	Offerteaanvraag EU GGD HN SIEM SOC | DEEL: I OMSCHRIJVING OPDRACHT(GEVER) | I.1 INHOUD VAN DE OPDRACHT | Blz 7	'Het opvolgen van de signalen en het opleiden van een viertal medewerkers van de GGD HN om op termijn zelf de signalen te interpreteren en op te volgen" Om cybersecurity incidenten binnen een omgeving 24/7/365 te detecteren, analyseren, rapporteren, erop te reageren en te voorkomen is er een team nodig van minimaal 6 analisten. Derhalve loont het niet voor kleinere organisaties om in eigen huis SOC diensten op te tuigen. Wij vragen u daarom of we een full managed oplossing mogen aanbieden?	Dat is akkoord
120	Inhoud	Offerteaanvraag EU GGD HN SIEM SOC | DEEL: I OMSCHRIJVING OPDRACHT(GEVER) | I.1 INHOUD VAN DE OPDRACHT | Blz 7	'Het aantal logbronnen die initieel opgenomen moeten worden in het systeem zijn rond de 200' • Bevinden deze logbronnen zich in een eigen datacenter of ook in de cloud? • Indien een gedeelte van deze logbronnen in de cloud staat, welke cloud is/zijn dit dan?	Hybride: on-prem, IaaS en SaaS
121	Inhoud	Offerteaanvraag EU GGD HN SIEM SOC | DEEL: I OMSCHRIJVING OPDRACHT(GEVER) | I.1 INHOUD VAN DE OPDRACHT | Blz 7	Over hoeveel endpoints (werkstations, servers etc) beschikt de opdrachtgever?	1200 laptops (tijdens Coronaperiode), normaal ongeveer 700 laptops, 40 virtuele servers
122	Inhoud	Offerteaanvraag EU GGD HN SIEM SOC | DEEL: I OMSCHRIJVING OPDRACHT(GEVER) | I.1 INHOUD VAN DE OPDRACHT | Blz 7	Staat het beleid van opdrachtgever het toe dat de aangeboden oplossing data opslaat in de cloud?	Ja, mits in EU
123	Inhoud	Offerteaanvraag EU GGD HN SIEM SOC | DEEL: I OMSCHRIJVING OPDRACHT(GEVER) | I.1 INHOUD VAN DE OPDRACHT | Blz 7	Gaat opdrachtgever bij configuratie management uit van de aangeboden oplossing of ook van de genoemde logbronnen?	Logbronnen
124	Inhoud	Offerteaanvraag EU GGD HN SIEM SOC | DEEL: I OMSCHRIJVING OPDRACHT(GEVER) | I.1 INHOUD VAN DE OPDRACHT | Blz 7	'Er is behoefte om log- en systeeminformatie uit IT-systemen te verzamelen, te categoriseren en te correleren...' Kan de opdrachtgever inzicht geven om hoeveel data het gaat?	Nee
125	Inhoud	Offerteaanvraag EU GGD HN SIEM SOC | DEEL: I OMSCHRIJVING OPDRACHT(GEVER) | I.1 INHOUD VAN DE OPDRACHT | Blz 7	'Het aantal logbronnen die initieel opgenomen moeten worden in het systeem zijn rond de 200.' Kan opdrachtgever een overzicht beschikbaar stellen van de verschillende logbronnen?	Nee, niet in dit stadium
126	Inhoud	Offerteaanvraag EU GGD HN SIEM SOC | DEEL: I OMSCHRIJVING OPDRACHT(GEVER) | I.1 INHOUD VAN DE OPDRACHT | Blz 7	Kan opdrachtgever een overzicht beschikbaar stellen van de te monitoren SaaS applicaties?	Nee, niet in dit stadium

127	Inhoud	Offerteaanvraag EU GGD HN SIEM SOC | DEEL: I OMSCHRIJVING OPDRACHT(GEVER) | I.1 INHOUD VAN DE OPDRACHT | Blz 7	Kan opdrachtgever een grafische weergave beschikbaar stellen van haar infrastructuur/architectuur (waar draait wat)?	Nee, vertrouwelijke informatie
128	Inhoud	Offerteaanvraag EU GGD HN SIEM SOC | DEEL: I OMSCHRIJVING OPDRACHT(GEVER) | I.1 INHOUD VAN DE OPDRACHT | Blz 7	'Het resultaat van deze verzamelde gegevens moet inzicht kunnen verschaffen in potentiële IT incidenten…' Wat zijn de retentie eisen die opdrachtgever stelt aan de oplossing?	De retentietijd hangt af van prijs en risico.
129	Inhoud	Offerteaanvraag Europees openbare aanbesteding SIEM SOC GGD Hollands Noorden - Pagina 7	Op welke termijn (bijvoorbeeld x maand, x jaar etc) verwacht GGD HN zelf de signalen te interpreteren en op te volgen.	6 maanden
130	Inhoud	Offerteaanvraag Europees openbare aanbesteding SIEM SOC GGD Hollands Noorden - Pagina 7	Het aantal logbronnen die initieel opgenomen moeten worden in het systeem zijn rond de 200. Wat is uw definitie van een logbron? Is het mogelijk een overzicht te ontvangen van de betreffende logbronnen?	Vertrouwelijke informatie.
131	Juridisch	Offerteaanvraag Inhoud van de opdracht	Is er naast een Azure AD ook een Eigen AD en welke is leidend?	Ja, eigen AD is leidend
132	Inhoud	Offerteaanvraag Inhoud van de opdracht	De uitvoering van de opdracht is gepland vanaf het moment van inwerkingtreding van de overeenkomst, gepland van 1 maart 2022 tot en met 29 februari 2024. Kan Opdrachtgever aangeven per wanneer de dienst operationeel dient te zijn?	wordt nader bepaald
133	Inhoud	Offerteaanvraag Inhoud van de opdracht	Tot de opdracht hoort ook het leveren van de benodigde virtuele appliance in het externe datacenter van GGD HN. Kan Opdrachtgever de adresgegevens van bedoeld datacenter opgeven? Wat wordt bedoeld met leveren virtuele aplliance? Opdrachtgever doet de annname dat VM systemen waarop eventueel licenties gezet moeten worden beschikbaar worden gesteld door Opdrachtgever en dat Opdrachtnemer dan verantwoordelijk is voor leveren installeren, configureren en behren van genoemde licentie. Is die aanname correct?	Vertrouwelijke informatie v.w.b. datacenter Deze aanname is niet correct
134	Inhoud	Offerteaanvraag Inhoud van de opdracht	Een deel van de logbronnen zijn SaaS applicaties die ergens anders draaien, maar waar GGD HN wel verantwoordelijk voor is. Kan Opdrachtgever hier de type logbronnen en aantallen van geven? Inschrijver stelt deze vraag enerzijds om te kunnen bepalen of de gewenste type logbronnen technisch aan te sluiten zijn en anderzijds zijn deze gegevens nodig voor het bepalen van de prijs. Of is dit buiten scope?	kunnen we niet aangeven
135	Inhoud	Offerteaanvraag Inhoud van de opdracht	Het aantal logbronnen die initieel opgenomen moeten worden in het systeem zijn rond de 200. Mogelijk zal dat in de toekomst uitgebreid dienen te worden. Kan Opdrachtgever aangeven welke type en per type aantallen logbronnen aangesloten moeten gaan worden? Inschrijver stelt deze vraag enerzijds om te kunnen bepalen of de gewenste type logbronnen technisch aan te sluiten zijn en anderzijds zijn deze gegevens nodig voor het bepalen van de prijs.	kunnen we niet aangeven
136	Inhoud	Offerteaanvraag Inhoud van de opdracht	Inschrijver vraagt zich af of deze verkorte openbare procedure een SIEM/SOC oplossing voor GGDHN passend is. Dit omdat de kaders onduidelijk zijn en open uitwisselen van gevoelige informatie gevoelig ligt. Inschrijver vraagt GGD HN in overweging te nemen een andere aanpak te kiezen die binnen de wettelijke kaders sneller tot effectieve inperking van de risico's (als data lost preventie, discontinuiteit en verlies van (data) integriteit) leidt. Suggestie: na een voorselectie, over te gaan tot een niet-openbare procedure incl dialoog ronde.	Deze procedure is gekozen i.v.m. de urgentie om snel tot een oplossing te komen. De door u voorgestelde procedure heeft een doorlooptijd van minimaal 6 maanden.
137	Inhoud	Offerteaanvraag Inhoud van de opdracht	Graag krijgt inschrijver concreet zicht op de geplande ontwikkeling in het gebruik van cloud diensten IAAS/PAAS/SAAS vs Onpremise oplossingen. Kunt u dat inzicht geven?	kunnen we niet aangeven
138	Inhoud	Offerteaanvraag Inhoud van de opdracht	Is er een algemeen security plan /roadmap waar de SIEM/SOC oplossing in past?	Ja, maar niet beschikbaar.
139	Inhoud	Offerteaanvraag Inhoud van de opdracht	Graag krijgt inschrijver zicht op: Aantal gebruikers Azure AD? Aantal gebruikers van WINDOWS 7, 8, 10, MACOS EN MOBILE ENDPOINTS? Aantal gebruiker van MICROSOFT 365: EXCHANGE, TEAMS, SHAREPOINT EN ONEDRIVE? Aantal VM van AZURE WORKLOADS (IAAS & PAAS) EN HYBRIDE SERVERS? Aantal Web applicaties die naar het internet ontsloten worden? Aantal VM/Servers on prem waar MS Defender op draait?	Tijdens coronatijd 1800 medewerkers, normale situatie 700 medewerkers. Alleen kantoormedewerkers beschikken over een laptop 1200/700. Afhankelijk van de uitrusting E5 of F3 licentie
140	Inhoud	Offerteaanvraag Inhoud van de opdracht	Van welke Microsoft Cloud Services wordt gebruik gemaakt en welke soort end user licenties (Bijv E3/ E5) zijn er?	M365 E5 en F3
141	Inhoud	Offerteaanvraag Inhoud van de opdracht	Ondersteund het netwerk / FW ook de doorgifte van Span poorten en zijn in ook fysieke inkoppelingen mogelijk?	onbekend

142	Inhoud	Offerteaanvraag Inhoud van de opdracht	Indien het betreffende domein door een andere partij dan de ICT afdeling van GGD beheerd wordt kijgt inschrijver van daar graag inzicht over. Indien in dat domein logging noodzakelijk is, is dan de toegang of het plaatsen van logbronnen geborgd of is dat buiten scope? Bijvoorbeeld een exteren beheerd Lan en Firewall of een applicatie / storage cluster of een beheerde werkplek...	valt buiten de scope
143	Inhoud	Offerteaanvraag Inhoud van de opdracht	Graag krijgt inschijver specifieker inzicht in uw ICT architectuur waarbij zaken duidelijk moeten worden als: Opzet Lan , internet aansluitingen (en), Wan typologie, Firewalls intern/extern/DMZ, aanwezige IPS/IDS functies, proxi functies, DNS, Werkplek concept, # en type clients, aard omvang server / storage omgevingen / applicaties , inzicht in # locaties waar servers staan, security appliances - tooling als mail security oplossingen, eventueel aanwezige DLP oplossingen, NDR/EDR/XDR oplssingen etc die als logbron gebruikt kunnen worden. Graag van bovenstaande de nu aanwezige zaken en geplande zaken.	vertrouwelijk
144	Inhoud	Offerteaanvraag Inhoud van de opdracht	U schrijft dat het leveren van Virtuele Appliances in het externe DC van GGDHN tot de scope behoort. Kan er naast of in plaats van een viruele appliance ook een fysiek device geplaatst worden?	niet mogelijk
145	Inhoud	Offerteaanvraag Inhoud van de opdracht	U geeft aan dat het gaat om 200 logbronnen. Wat definieert u al een logbron. Kunt u aangeven om welke type logbronnen het gaat	EVT, Syslog
146	Inhoud	Offerteaanvraag Inhoud van de opdracht	U schrijft : "Er is behoefte om log- en systeeminformatie uit IT-systemen te verzamelen, te categoriseren en te correleren. Het resultaat van deze verzamelde gegevens moet inzicht kunnen verschaffen in potentiële IT incidenten en -onder voorwaarden- signalering afgeven, welke gebruikt kan worden om door de IT organisatie snel en adequaat te reageren op systeem- en beveiligingsincidenten." Nu staat deze behoefte heel breed gedefinieerd en zou inschrijver basis info moeten verzamelen die in het domein van het basaal ICT beheer hoort. Graag krijgt inschrijver de bevestiging dat het specifiek gaat om log en systeem informatie specifiek gericht op beveiligingsincidenten.	correct
147	Inhoud	Offerteaanvraag Inhoud van de opdracht	Vallen nu afwezige security logbronnen maar wel wenselijke logbronnen ook binnen de scope van de aanbesteding zonder dat deze nu in het beoordelingsmodel worden meegenomen?	ja
148	Inhoud	Offerteaanvraag Inhoud van de opdracht	U schrijft: Het doel van de aanbestedingsprocedure is het op een transparante wijze sluiten van een Overeenkomst tussen Opdrachtgever en Opdrachtnemer voor de levering van Netwerksecuritydiensten. Is de scope van het contract daarmee breeder dan de titel aanbesteding?	De scope in het PvE is leidend.
149	Inhoud	Office365 en de servers voorzien van beveiliging en detection and response functionaliteiten	Naast het meenemen van IDS/IPS functionaliteiten, wil GGD Hollands Noorden ook Office365 en de servers voorzien van beveiliging en detection and response functionaliteiten?	Ja (echter, MS 365 Defender is reeds in huis)
150	Inhoud	On-premise	Moet de verzamelde log en netwerkdata on-premise blijven van GGD HN?	Nee
151	Inhoud	On-premise, SaaS of hybride	Vereist GGD Hollands Noorden een on-premise, SaaS of hybride oplossing?	Hybride
152	Inhoud	Operating Systemen (leverancier en versie)	Wat zijn de Operating Systemen (leverancier en versie) van de werkplekken / servers in de omgeving van de Opdrachtgever ?	Windows 10/11, Windows Server 2012 R2 t/m 2022, Ubuntu Server 14 LTS
153	Inhoud	OT (Operationele Technologie)	Beschikt Opdrachtgever ook over OT (Operationele Technologie) systemen en dienen die ook meegenomen te worden ? Indien ja graag specificatie van deze systemen.	n.v.t.
154	Contract	Overeenkomst, art. 7	Kunt u aangeven wat de rangorde is van de Overeenkomst en de genoemde bijlagen?	1. overeenkomst, 2. Gibit 2020, 3. Nota van Inlichtingen, 4. offerteaanvraag met PvE, 5. Inschrijving
155	Proces	Beoordelingscommissie	Kunt u aangeven uit hoeveel personen en welke rollen de beoordelingscommissie voor G2.2 (Demo) bestaat?	Teamleider ICT, systeembeheer, technisch specialist, projectleider. Procesbegeleiding door inkoop.
156	Inhoud	Plafondprijs	Waar is de plafondprijs voor de jaarlijkse dienstverlening van 100.000 Euro op gebaseerd? Kunt u dit nader onderbouwen?	Betreft het beschikbare budget.
157	Inhoud	Plan van aanpak replacement van huidige vendoren	Is het mogelijk om in het plan van aanpak replacement van huidige vendoren mee te nemen om de hoogste efficiëntie en effectiviteit te behalen?	Nee, daarmee lopen andere verplichtingen.
158	Inhoud	Programma van Eisen	23. Use casus.Heeft GGD HN zelf reeds een idee bij business specifieke risico's en use casus? Waar dienen inschrijvers rekening mee houden?	nader te bepalen
159	Inhoud	Programma van Eisen	22: Vulnerability Scanner.Mogelijkheid om gegevens uit een Vulnerability Scanner mee te nemen in de SIEM, zodat opvolging gestandaardiseerd is. Kan Opdrachtgever de specificaties van de beoogde Vulnerability Scanner welke als logbron gebruik moet gaan worden opgeven?	nader te bepalen
160	Inhoud	Programma van Eisen	15 Siem 16 SOC Opvolging SOC Functie. Is het correct dat incident response niet onderdeel is de inschrijfprijs? Is ICT van GGD HN ook 7*24 bereikbaar en inzetbaar?	nader te bepalen
161	Inhoud	Programma van Eisen	14: Deteceteren Ongeautoriseerde IT assets.Kan Opdrachtgever aangeven welke logbron hiervoor wordt gebruikt en een omschrijving geven van de gewenste usecase?	MS Defender
162	Inhoud	Programma van Eisen	13: IDS/IPS functionaliteit.Kan Opdrachtgever aangeven welke logbron hiervoor wordt gebruikt en een omschrijving geven van de gewenste usecase?	meerdere bronnen, nader te bepalen

163	Inhoud	Programma van Eisen	12: Bescherming tegen Insider Threats.Kan Opdrachtgever aangeven welke logbron hiervoor wordt gebruikt en een omschrijving geven van de gewenste usecase?	meerdere bronnen, nader te bepalen
164	Inhoud	Programma van Eisen	10: Encryptie. Opdrachtgever stelt dat encryptie zowel voor data at rest als Data in Transit moet zijn gewaarborgd. Doelstelling is om data optimaal te beschermen. Is Opdrachtgever bereid deze eis te laten vervallen danwel anders te omschrijven? Voorstel Opdrachtnemer is verantwoordelijk voor de bescherming van de data, op een dusdanige manier dat een databreach wordt uitgesloten. Beschrijf hierbij hoe u aan deze eis voldoet.	akkoord
165	Inhoud	Programma van Eisen	08: AD/IAMDMogelijkheid tot integratie met bestaande identity providers, zoals Microsoft AD, Azure AD of IAM systemen. Kan Opdrachtgever de specificaties opgeven van "IAM"systemen? Deze vraag wordt gesteld om te kunnen bepalen of Opdrachtnemer het betreffende IAM systeem als logbron kan opnemen.	HelloID
166	Inhoud	Programma van Eisen	8 AD/IAMDMaakt GGDHN nu ook gebruik van PAM oplossingen, Zo ja welke en indien geplanned, wat wanneer?	nee
167	Inhoud	Programma van Eisen	6 Z-cert Aansluiting Z-cert - ZorgDectectie Netwerk: Er zijn landelijk maar weinig commerciele partijen "aangesloten". Hierdoor beperkt u het concurrentie speelveld en mogelijke aanbieders. Is dat wenselijk? Mag deze eis omgezet worden in een wens dan wel realisatie in eerste jaar van de dienst ipv bij aanvang? Kunt u "aansluiting" ook nader duiden?	De GGD wordt zelf aangesloten op Z-cert.
168	Inhoud	Programma van Eisen	3 Gedragslijk NVZ Kunt u dit concreet maken welke specifieke eisen u hier stelt?	Ja, zie gedragslijn NVZ.
169	Inhoud	Programma van Eisen	NEN7510 is grotendeels gebaseerd op de IS0 27001 en eigelijk specifiek voor de Zorg en patient gegevens verwerkende instelling zelf. Is een voor de SIEM/SOC aanbieder ISO 27001 niet afdoende?	Nee, patientgegevens worden ook verwerkt. Denk hierbij aan reizigersvaccinaties.
170	Inhoud	PVE - Eis 22	Kunt u aangeven wat wordt bedoeld met "zodat opvolging gestandaardiseerd is". Is het niet logischer om deze resultaten toe te voegen aan een Service Management Tool? Het is niet gebruikelijk dat de verantwoordelijken voor patchmanagement toegang hebben tot de SIEM.	Het resultaat van de SIEM oplossing kan input zijn voor een SMT
171	Inhoud	Programma van eisen eis 16	Kunt u nader toelichten wat u verwacht van de geëiste 24/7 dienstverlening?	24/7 monitoring in combinatie met consignatie/piketdienst
172	Inhoud	Programma van Eisen - Eis 22.	Wordt er verwacht vanuit de SIEM SOC oplossing een aanbieding te doen voor een alternatieve vulnerability management dienst?	Ja, maar is in deze out of scope
173	Inhoud	Programma van Eisen – Eis 22.	Welke vulnerability scanner wordt momenteel gebruikt door GGD HN?	Geen
174	Inhoud	Programma van Eisen - Eis 23.	Kunt u aangeven welke use-cases minimaal worden verwacht aanwezig te zijn in de bibliotheek?	Deze scope is onderdeel van de implementatie.
175		Programma van Eisen / Conformiteitenlijst. Punt 4	Kun u aangeven wat u exact van inschrijver verwacht op dit punt?	Hou het vooral praktisch en duidelijk.
176		Programma van Eisen / Conformiteitenlijst. Punt 6	Kun u aangeven wat u exact van inschrijver verwacht op dit punt? Z-cert geeft aangesloten zorginstellingen "Security Threat Intelligence". Ons eigen SOC maakt gebruik van diverse globaal erkende Threat Intell's, op basis waarvan wij acteren richting onze SOC klanten. Wat voegt hier de aansluiting op z-cert aan toe?	Aansluiting op Z-Cert regelt opdrachtgever zelf.
177	Juridisch	Bijlage 3	Kunt u bevestigen dat bijlage 3 in de definitieve verwerkersovereenkomst niet wordt opgenomen? Zo neen, welke bepalingen zullen in deze bijlage worden opgenomen?	Nee, dat kunnen wij niet bevestigen. Bij het afsluiten van de hoofdovereenkomst kunnen hier nadere afspraken over gemaakt worden.
178	Inhoud	V.2.1 van offerteaanvraag (pagina 26)	Kunt u bevestigen dat de kosten voor zowel Structurele kosten (G1.1), Implementatiekosten (G1.2) en Opleidingskosten (G1.3) realistisch moeten zijn en dat er derhalve dus niet strategisch en/of manipulatief ingeschreven mag worden met bijvoorbeeld een nulbedrag. Graag uw bevestiging.	Zie deel V van het aanbestedingsdocument.
179	Juridisch	Verwerkersovereenkomst	Kunt u bevestigen dat voor het aantonen van een passend niveau van beveiliging het afdoende is dat Leverancier ISO 27001 gecertificeerd is en een daartoe strekkend certificaat overhandigt?	Nee dat is niet afdoende, De eis is NEN 7510
180	Inhoud	Programma van Eisen, eis 6	Klopt onze aanname dat met deze eis wordt bedoeld dat Inschrijver de aansluiting op Z-cert ZorgDetectieNetwerk moet faciliteren? GGD HN is immers al deelnemer van Z-cert.	Aanname is correct
181	Inhoud	Proven technology	GGD Hollands Noorden schrijft over het gebruik van proven technology, is het belangrijk dat de technologie die gebruikt wordt meerdere jaren door onderzoeksbureaus erkend wordt als leider?	Ja
182	Uitvoering	PvE	Is de prijs inclusief licentiekosten van eventueel aangeleverde software?	Ja
183	Uitvoering	PvE	Het Programma van Eisen indiceert dat de dienstverlening remote dient plaats te vinden, klopt dit?	Ja
184	Uitvoering	PvE	PvE, Artikel 10: IDS/IPS functionaliteit bevindt zich doorgaans op apparatuur binnen een netwerkomgeving (dus bij opdrachtgever), is deze apparatuur reeds aanwezig of dient deze te worden aangeleverd?	Niet aanwezig
185	Uitvoering	PvE	Wat is de scope van de te monitoren omgeving?	ong. 200 logbronnen
186	Inhoud	Bijlage A - Programma van Eisen	Kunt u 'Bijlage A Programma van Eisen' beschikbaar stellen in Word zodat de conformiteitenlijst eenvoudig digitaal aangevinkt kan worden?	Is separaat toegevoegd.

187	Juridisch	Artikel 4.2 GIBIT	Leverancier kan in redelijkheid niet aan welke termijn dan ook – dus ook niet aan een fatale termijn – worden gehouden indien het overschrijden ervan verband houdt met de omstandigheid dat: i. GGD zelf niet of niet tijdig de noodzakelijke medewerking verleent aan de uitvoering van de overeenkomst, of ii. GDD zelf niet of niet alle door voor de uitvoering van de overeenkomst benodigde informatie verstrekt, of iii. GGD zelf de voor de voortgang van de werkzaamheden van Leverancier benodigde besluiten niet of niet tijdig neemt; of iv. Betrokken derden – waaronder een of meer van de leveranciers en/of dienstverleners van ICT – hun medewerking en/of benodigde informatie niet, niet tijdig of anderszins gebrekkig verlenen; of v. Sprake is van meerwerk of sprake is van wijziging van de opdracht door of op verzoek van GGD zelf; Bent u bereid deze redelijke nuancering van de in art. 4.2 GIBIT genoemde regel te aanvaarden?	De definitie in art 4.1 en 4.2 van de GIBIT 2020 is helder. Verdere nuancering achten wij niet nodig.
188	Inhoud	Data ingest	Om tot een juiste en vergelijkbare prijsstelling te komen is het noodzakelijk om te weten hoeveel hoeveel data het SIEM dient te verwerken (data ingest). Kunt u aangeven wat uw benodigde data ingest is?	Nee
189	Inhoud	realtime dashboard	Opdrachtgever spreekt over dagelijkse updates over bedreigingen en de status van de technische informatiebeveiliging richting IT-Beheer en CISO. Volstaat een realtime dashboard i.c.m. maandelijkse rapportages ook?	Ja
190	Inhoud	Retentie	Worden er eisen gesteld aan de retentie-periode voor Logs en Netwerk data? Zo ja, wat is de periode van retentie?	De retentietijd hangt af van prijs en risico.
191	Inhoud	Saas applicaties	– Hoeveel van de 200 systemen / SaaS applicaties zijn web-gebaseerd? (HTTP/HTTPS)	80%
192	Inhoud	SPAN/TAP/Netflow	Heeft GGD HN de mogelijkheid om SPAN/TAP/Netflow te sturen naar virtuele appliance(s)?	Ja
193	Inhoud	Storage	Wat voor soort storage is er beschikbaar voor de virtuele appliance?	Hypervisor is VMware
194	Inhoud	Support	2e/3e lijns support, wordt hierbij verwacht dat het 24/7 kan worden geleverd? Moet dit dan ook op locatie zijn?	Nee
195	Inhoud	Systemen	Is het mogelijk een specifieker overzicht te ontvangen van de type systemen die moeten worden gemonitord?	o.a. Windows 10/11, Windows Server, Datto AP's en switches, Cisco Routers
196	Inhoud	technische benodigdheden	• Eventuele voorkeuren of beperkingen op de SOC-locatie. Europe/US/ROW	EU
197	Inhoud	technische benodigdheden	Kunt u details delen over bestaande SIEM-tools voor het bewaken van kwetsbaarheden en het reageren op incidenten?	Geen
198	Inhoud	technische benodigdheden	Bevestig of de leverancier in een 'as-a-service'-model is.	Ja
199	Inhoud	technische benodigdheden	Gelieve te bevestigen of de leverancier nieuwe SIEM-oplossingen moet brengen?	Ja
200	Inhoud	technische benodigdheden	Bevestig a.u.b. als alleen Siem-SOC-services binnen het bereik vallen.	Ja
201	Inhoud	technische benodigdheden	Deel de lijst met vereisten voor nieuwe use-cases - Beveiliging / netwerkgerelateerd met daarnaast een overzicht van het aantal EPS (events per second)	Deze scope is onderdeel van de implementatie.
202	Inhoud	technische benodigdheden	Deel a.u.b. de lijst met vereisten voor nieuwe use-cases (gebruiksscenario's) - toepassingsgerelateerd	Deze scope is onderdeel van de implementatie.
203	Inhoud	technische benodigdheden	• Gelieve de inventarisgegevens van logbronnen te delen SAAS & On-premise?	Vertrouwelijke informatie.
204	Inhoud	technische benodigdheden	• Deel Applicatie's en beveiliging Asset's / device Inventory; hoeveelheid en naam enz.	Vertrouwelijke informatie.
205	Inhoud	technische benodigdheden	Wilt u details van bestaande Siem SOC-locaties delen?	n.v.t.
206	Inhoud	technische benodigdheden	Deel prijsvereisten voor het leveren van beveiligingsdiensten: vaste prijs of tijd en materiaal of eenheid van op werk gebaseerde prijzen enz.	Zie bijlage D prijzenblad
207	Inhoud	Threat Intelligence	Het de beschikking hebben over eigen Threat Intelligence is vaak een vereiste in SIEM/SOC trajecten, hoe kijkt GGD Hollands Noorden hier tegenaan ?	Zit niet de scope.
208	Inhoud	Logbronnen	Om tot een juiste en vergelijkbare prijsstelling te komen is het noodzakelijk om te weten welke logbronnen er initieel in scope zijn, hoeveel logging deze genereren en wat het type logging hiervan is. Kunt u dit gedetailleerd aangeven?	Actieve netwerkcomponenten en servers, SaaS en Azure
209	Inhoud	twedee vragenronde	Is het mogelijk om een tweede vragenronde te plannen?	Er is geen tweede vragenronde gepland om nadere vragen over de eerste Nota van Inlichtingen te kunnen stellen.
210	Inhoud	UBA/UEBA	Bedoeld GGD HN met "bescherming tegen insider threats" het gebruik van UBA/UEBA (User Behavior Analitics/ User Entity Behavior Analitics)?	Nee. Monitoring van verkeer on-premise (lateral movement)
211	Proces	V.3 van offerteaanvraag (pagina 27)	Onderdeel van het gunningscriterium Kwaliteit is de Demo (G2.2) waar de drie best scorende partijen voor worden uitgenodigd. Deze demo telt mee voor 10/50 te behalen punten op kwaliteit. Het is echter nog niet duidelijk wat er van de Demo wordt verwacht, hoe de beoordeling daarvan plaatsvindt en hoe de objectiviteit hierbij wordt geborgd. Graag uw gemotiveerde toelichting op dit gunningscriterium.	Van de demo wordt verwacht dat o.a. processen, procedures en werkwijze van de inschrijver duidelijk naar voren komt. Objectiviteit wordt geborgd door meerdere deskundige personen vanuit verschillende functies in het beoordelingsteam te laten plaatsnemen waarbij de inkoopadviseur het proces begeleidt.

212	Proces	Meerwaarde	Opdrachtgever hanteert bij de beoordeling de scores 0, 2, 6, 8 en 10, waarbij het voor een score 8 of 10 een voorwaarde is om (veel) meerwaarde te bieden. Kan Opdrachtgever verduidelijken waar men meerwaarde in ziet?	Binnen het beschikbare budget zo veel mogelijk waarde leveren.
213	Inhoud	Opvolging beveiligingsrisisco's	Titel van de aanbesteding is "Leveren en implementeren SIEM SOC oplossing en opvolging beveiligingsrisico's". Kunt u aangeven wat u verstaat onder "opvolging beveiligingsrisico's"? Het is op dit moment namelijk lastig in te schatten welke kosten hiermee gemoeid zijn.	Opvolging van de resultaten van de SIEM/SOC oplossing; dat het resulteert in een incident bij de juiste behandelaar, lees: eigen IT mensen en/of MSSP
214	Inhoud	SIEM on prem	U geeft aan "Tot de opdracht hoort ook het leveren van de benodigde virtuele appliance in het externe datacenter van GGD HN". Bedoelt u hiermee dat we de SIEM oplossing on prem in jullie externe datacenter laten draaien?	Ja
215	Inhoud	Vendor managed detection and response	Organisaties zien dat vendor managed services bewezen krachtig zijn door de inhouse kennis van de producten. Geeft GGD Hollands Noorden ook de voorkeur aan vendor managed detection and response?	Ja
216	Inhoud	Vendoren voor de beveiliging van endpoints, firewalls, servers, Office365	Om zeker te zijn van de mogelijke integraties is het belangrijk om te weten welke vendoren GGD Hollands Noorden momenteel gebruikt voor de beveiliging van endpoints, firewalls, servers, Office365. Is het mogelijk om hier informatie over te verschaffen?	Fortigate, MS Defender 365, mShield
217	Inhoud	verschillende lagen van security met punt oplossingen	Erkent GGD Hollands Noorden dat het hebben van verschillende lagen van security met punt oplossingen resulteert in een veelvoud on-gecorreleerde alerts?	Ja
218	Proces	III.2.3.1 - Kerncompetenties	U vraagt om referenties op te geven om daarmee de technische bekwaamheid en/of beroepsbekwaamheid middels de genoemde kerncompetenties te toetsen. Het is in de (cyber) security markt echter door het vertrouwelijke karakter niet gebruikelijk om referenties met naam en toenaam te noemen. Opdrachtnemer heeft een vertrouwensrelatie met haar klanten, waardoor het niet altijd mogelijk is om de naam van deze referenties te delen. Wij willen Opdrachtgever dan ook vragen om geanonimiseerde referenties toe te staan. Wij kunnen deze referenties op verzoek (bijvoorbeeld na selectie) aan u verifieren. Staat Opdrachtgever hiervoor open?	Geanonimiseerde referenties is toegestaan. Verificatie zal plaatsvinden voor de uitnodiging voor de presentatie.
219	Inhoud	Applicaties	Vallen er applicaties in deze scope die door meerdere GGD'en worden gebruikt?	In eerste instantie niet, wellicht in een vervolg
220	Juridisch	Artikel 10 GIBIT	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…'?	Nee, niet akkoord.
221	Contract	Verwerkersovereenkomst, art. 6.1	Leverancier is van mening dat deze bepaling vragen oproept over verminking en verlies van Persoonsgegevens. Wij stellen daarom voor de redactie van artikel 6.1 aan te vullen met: "In aanvulling daarop komen partijen overeen dat de aansprakelijkheid van de Verwerker voor verminking, verlies en vernietiging van Persoonsgegevens, in verband met deze Verwerkersovereenkomst is beperkt tot het vergoeden van aan de Verwerker toerekenbare directe schade. Kunt u hiermee akkoord gaan? Zo niet, kunt u motiveren waarom niet?	Nee, niet akkoord.
222	Juridisch	Artikel 5.5 GIBIT	Voorstel om te schrappen. Leverancier kan zich buiten de aanbestedingsstukken om geen beeld vormen de aan artikel 5.5 verbonden risico's	Niet akkoord.
223	Juridisch	7.3 GIBIT	Zie hierover onze eerdere vraag bij artikel 4.2 GIBIT. Hetgeen daar is opgemerkt geldt overeenkomstig voor art. 7.3 GIBIT. Bent u daarmee akkoord?	Zie ook het antwoord op die vraag. Aanvullend Het artikel bepaalt dat herstel van tijdens het testen geconstateerde gebreken niet mag leiden tot vertraging. Het is dus aan Leverancier – mede gelet op zijn rol als penvoerder van het aanbod (artikel 3), het implementatieplan (artikel 5) en/of het testprotocol (artikel 7.1) – om op voorhand een realistische planning te hanteren met voldoende ruimte voor herstel van eventueel geconstateerde gebreken.
224	Inhoud	vulnerability management oplossing	Wat is de huidige vulnerability management oplossing ?	Geen