

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
1.	Algemeen	Algemeen verzoek. Indien u naar aanleiding van de NvI wijzigingen doorvoert in documenten, wilt u deze dan middels track changes of 'gele highlight', duidelijk markeren?	Nee. De KB publiceert geen gewijzigde versies van de Aanbestedingsstukken, met uitzondering van Bijlage 5 Prijzenblad NvI 1 (zie het antwoord op vraag 187) en de Word-versies van Bijlage 7 en 8 (zie het antwoord op vraag 533), die bij deze Nota van Inlichtingen worden gepubliceerd. Eventuele wijzigingen van de Raamovereenkomst (inclusief het Programma van Eisen) naar aanleiding van de Nota's van Inlichtingen worden na gunning verwerkt in de definitieve Raamovereenkomst. De antwoorden in de Nota's van Inlichtingen prevaleren boven de eerder gepubliceerde Aanbestedingsstukken.
2.	Beschrijvend document – Bijlagen	In de bijlagen wordt bijlage nummer 6 gemist. Is dat een bewuste ommissie en, zo niet, kunt u bijlage 6 alsnog toevoegen en inschrijvers de gelegenheid daarover vragen te stellen?	Er is geen sprake van een ommissie. Bijlage 6 betreft het Uniform Europees Aanbestedingsdocument (UEA), dat Inschrijver via de UEA-wizard in TenderNed invult en ondertekent (zie hoofdstuk 4 en paragraaf 7.4 van het Beschrijvend document).
3.	Beschrijvend document – §2.1 en §2.2 Aanleiding en doelstellingen	Welke knelpunten of verbeterpunten heeft de KB ervaren in de samenwerking met eerdere leveranciers van pentestdiensten en welke verbeteringen verwacht de KB van de nieuwe opdrachtnemer?	De KB doet geen concrete uitspraken over ervaringen met eerdere leveranciers. De verwachtingen van de KB zijn verwerkt in de doelstellingen (paragraaf 2.2) en het Programma van Eisen.
4.	Beschrijvend document – §2.3 Opdrachtoomschrijving (scope)	Beschrijvend document, paragraaf 2.3. U beschrijft de scope van de opdracht, meer specifiek de term "penetratietesten". Kan u aangeven wat u zelf onder deze term verstaat?	Het zou voor partijen die onderhavige Opdracht kunnen uitvoeren niet nodig moeten zijn om de term 'penetratietesten' uit te leggen. De KB verstrekt daarom geen verdere definitie.
5.	Beschrijvend document – §2.3 Opdrachtoomschrijving (scope)	Beschrijvend document, paragraaf 2.3. U beschrijft de scope van de opdracht. Betreft de scope uitsluitend penetratietesten, of ook gerelateerde werkzaamheden zoals (geautomatiseerde) kwetsbaarheidsscans, broncode-onderzoeken, configuratie-onderzoeken en Red Teaming.	De scope omvat penetratietesten, maar kan als de situatie dat vraagt ook worden uitgebreid met een broncode- of configuratie-onderzoek. Red teaming en kwetsbaarheidsscans vallen buiten de scope van de Raamovereenkomst.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
6.	Beschrijvend document – §2.3 Opdrachtoomschrijving (scope)	Kan KB bevestigen of diensten zoals Red Teaming, social engineering of fysieke beveiligingstesten zoals mystery visit, wel of niet binnen de scope van de raamovereenkomst vallen?	Red teaming, social engineering en fysieke beveiligingstesten (zoals een mystery visit) vallen niet binnen de scope van de Raamovereenkomst. Zie ook het antwoord op vraag 5.
7.	Beschrijvend document – §2.3 Opdrachtoomschrijving (scope)	Vallen red teaming, social engineering, broncodereviews, tests van AI- en LLM-toepassingen en OT binnen 'alle (soorten) applicaties en omgevingen'? Zo ja, in welke mate?	Broncodereviews (als onderdeel van een pentest) en het testen van AI- en LLM-toepassingen vallen binnen de scope. Red teaming en social engineering vallen niet binnen de scope (zie het antwoord op vraag 6). OT-omgevingen zijn bij de KB op dit moment niet of nauwelijks van toepassing. Dit kan op een later moment worden uitgebreid. De KB kan geen indicatie geven van de mate waarin de verschillende soorten pentesten voorkomen.
8.	Beschrijvend document – §2.3 Opdrachtoomschrijving (scope)	Kunt u toelichten welke soort pentesten u verwacht onder deze overeenkomst uit te vragen?	De pentesten kunnen betrekking hebben op alle (soorten) applicaties en omgevingen van de KB, zoals webapplicaties, API's, mobiele applicaties, interne en externe infrastructuur, cloudomgevingen en identity-omgevingen (zoals Active Directory/Entra ID). De concrete scope wordt per Nadere Opdracht vastgesteld tijdens de inventarisatie (zie eis E18).
9.	Beschrijvend document – §2.3 Opdrachtoomschrijving (scope)	Het PvE noemt onder ander applicaties, platformen, systemen, netwerken en verschillende methodieken om te testen. Kan KB limitatief of indicatief aangeven welke type Security Assessments gedurende de looptijd verwacht worden, bijvoorbeeld webapplicaties, API's, mobiele applicaties, interne infrastructuur, externe infrastructuur, cloudomgevingen etc.?	Zie het antwoord op vraag 8. De KB geeft geen limitatieve opsomming.
10.	Beschrijvend document – §2.3 Opdrachtoomschrijving (scope)	Kunt u aangeven welke typen pentesten naar verwachting onder de Raamovereenkomst zullen worden uitgevoerd? Bijvoorbeeld aan webapplicaties, API's, mobiele applicaties, interne/externe	Zie het antwoord op vraag 8.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		infrastructuur, Active Directory/Entra ID, Microsoft 365, cloudomgevingen, netwerkcomponenten en configuratiereviews.	
11.	Beschrijvend document – §2.3 Opdrachtomschrijving (scope)	Indien verschillende typen pentesten worden verwacht, kan de KB een indicatieve procentuele verdeling geven van de verwachte opdrachten, bijvoorbeeld applicatie/API-pentesten versus infrastructuur-, identity- en cloudpentesten?	Nee. De KB kan geen procentuele verdeling geven. Het aantal en de soort pentesten zijn afhankelijk van de ontwikkelingen in het IT-landschap van de KB.
12.	Beschrijvend document – §2.3 Opdrachtomschrijving (scope)	Maakt het testen van cloudomgevingen onderdeel uit van de verwachte dienstverlening? Zo ja, van welke cloudplatformen maakt de KB hoofdzakelijk gebruik (bijvoorbeeld Microsoft Azure, AWS en/of Google Cloud) en kunnen ook configuratie- en IAM-assessments onderdeel zijn van een opdracht?	Ja, het testen van cloudomgevingen (zoals Azure) kan onderdeel uitmaken van de dienstverlening. Configuratie- en IAM-assessments kunnen onderdeel uitmaken van een pentest op een cloudomgeving.
13.	Beschrijvend document – §2.3 Opdrachtomschrijving (scope)	Kunnen pentesten op Active Directory en/of Entra ID onderdeel uitmaken van de Nadere Opdrachten? Zo ja, verwacht de KB daarbij uitsluitend aanvalsscenario's vanuit een bepaald startpunt of kunnen ook configuratie- en rechtenanalyses onderdeel van de scope zijn?	Ja, pentesten op Active Directory en/of Entra ID kunnen onderdeel uitmaken van de Nadere Opdrachten. De KB kan op voorhand geen uitspraken doen over het type test dat vereist is; de aanpak (waaronder eventuele configuratie- en rechtenanalyses) wordt per Nadere Opdracht vastgesteld tijdens de inventarisatie (eis E18).
14.	Beschrijvend document – §2.3 Opdrachtomschrijving (scope)	In het Programma van Eisen worden black-box-, grey-box- en white-boxmethodieken genoemd. Kan de KB aangeven welke testvorm naar verwachting het meest zal voorkomen en of hierbij bijvoorbeeld testaccounts, broncode, architectuurdocumentatie of configuratiegegevens beschikbaar worden gesteld?	De KB geeft per Nadere Opdracht aan welke methodiek (black-box, grey-box of white-box) gehanteerd moet worden (zie eis E31). De KB kan geen indicatie geven van de verdeling. Testaccounts, documentatie en (indien van toepassing) broncode worden per Nadere Opdracht beschikbaar gesteld, voor zover dit voor de gekozen methodiek noodzakelijk is.
15.	Beschrijvend document – §2.3 Opdrachtomschrijving (scope)	Kan de KB aangeven in welke mate de verschillende testvormen (black box, grey box, white box) naar verwachting voorkomen?	Zie het antwoord op vraag 14.
16.	Beschrijvend document – §2.3 Opdrachtomschrijving (scope)	Kan de KB nader specificeren welke typen applicaties (bijvoorbeeld web-, mobiele en desktopapplicaties) en omgevingen (bijvoorbeeld	Zie het antwoord op vraag 8.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		cloudomgevingen, interne netwerken, Active Directory-omgevingen en infrastructuurcomponenten) naar verwachting het grootste onderdeel zullen uitmaken van de af te nemen pentests, zodat inschrijvers hun aanpak, expertise en capaciteitsinzet hierop kunnen afstemmen?	
17.	Beschrijvend document – §2.3 Opdrachtomschrijving (scope)	Kan de KB een indicatieve verdeling geven van de verwachte opdrachten naar type omgeving, testvorm, omvang en locatie? Dit helpt Inschrijvers om capaciteit en het "all-in mandag tarief" realistisch vast te stellen.	Zie het antwoord op vraag 11. De KB kan ook geen verdeling naar omvang of locatie geven (zie ook het antwoord op vraag 344).
18.	Beschrijvend document – §2.3 Opdrachtomschrijving (scope)	Het Beschrijvend document vermeldt dat de pentesten betrekking kunnen hebben op alle soorten applicaties en omgevingen van de KB. De aanbestedingsstukken bevatten echter geen globale beschrijving van het huidige en verwachte IT-landschap. Kan de KB op hoofdlijnen aangeven welke categorieën testobjecten gedurende de raamovereenkomst worden verwacht? Wij verzoeken de KB daarbij, voor zover mogelijk, ook een indicatie te geven van de gebruikte technologieën, hostingvormen, voornaamste typen koppelvlakken en de verwachte aantallen of onderlinge verdeling van de pentesten. Gevoelige technische details zijn hiervoor niet nodig.	De KB deelt in het kader van deze Aanbesteding, mede om redenen van informatiebeveiliging, geen nadere informatie over haar IT-landschap. Dit zal verder besproken en doorgenomen worden na definitieve gunning van de Opdracht. Voor de soorten testobjecten, zie het antwoord op vraag 8. De benodigde informatie wordt per Nadere Opdracht verstrekt tijdens de inventarisatie (eis E18).
19.	Beschrijvend document – §2.3 Opdrachtomschrijving (scope)	Kan de KB op hoofdlijnen inzicht geven in het technische applicatielandschap waarop de pentesten naar verwachting betrekking hebben, waaronder veelgebruikte technologieën, hostingmodellen en architectuurvormen?	Zie het antwoord op vraag 18.
20.	Beschrijvend document – §2.3 Opdrachtomschrijving (scope)	Beschrijvend document, paragraaf 2.3. U benoemt "Het IT-landschap van de KB ontwikkelt zich". Kan voor ons een beeld schetsen hoe uw IT-landschap er uit ziet, bijvoorbeeld infrastructuur (on premise of cloud), applicaties (webapplicaties e.d.) en IT-organisatie? Ons verzoek is om een beeld te schetsen van de huidige situatie en van de toekomst op korte en middellange termijn.	Zie het antwoord op vraag 18.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
21.	Beschrijvend document – §2.3 Opdrachtschrijving (scope)	Beschrijvend document, paragraaf 2.3. U benoemt "Het IT-landschap van de KB ontwikkelt zich, onder andere door de integratie van mogelijkheden op het gebied van AI". Kan u aangeven welke toepassingen van AI de KB heeft en in de nabije toekomst voor zich ziet?	De KB doet geen uitspraken over (toekomstige) AI-toepassingen. Indien een AI-toepassing onderwerp is van een pentest, wordt dit in de betreffende Nadere Opdracht aangegeven.
22.	Beschrijvend document – §2.3 Opdrachtschrijving (scope)	Kan de KB een indicatie geven van de gebruikelijke omvang van infrastructuurpentesten, bijvoorbeeld in aantallen IP-adressen, hosts, subnetten of netwerksegmenten?	Nee. De omvang verschilt per pentest en wordt per Nadere Opdracht tijdens de inventarisatie vastgesteld.
23.	Beschrijvend document – §2.3 Opdrachtschrijving (scope)	Kan de KB een indicatie geven van de gemiddelde omvang/complexiteit van de te testen applicaties, bijvoorbeeld aantal gebruikersrollen, functionaliteiten, API-endpoints of applicatiecomponenten?	Zie het antwoord op vraag 22.
24.	Beschrijvend document – §2.5 Omvang van de Opdracht	§2.5 Omvang van de Opdracht Opdrachtgever raamt de gemiddelde jaarlijkse waarde van de Opdracht op €70.000 exclusief btw, zonder afname- of omzetgarantie, en noemt een maximale omvang van €500.000 voor de gehele looptijd. Kan Opdrachtgever, voor zover beschikbaar en eventueel in bandbreedtes, over de meest representatieve historische periode inzicht geven in het aantal pentesten per jaar, de typen testobjecten en de gemiddelde en maximale omvang per pentest in uren of mandagen?	De KB kan slechts beperkt informatie verstrekken over de historische omvang. In de periode vanaf september 2025 zijn ongeveer vijf pentesten uitgevoerd. Verdere historische informatie is niet beschikbaar. Over toekomstige pentesten kan de KB geen informatie verstrekken. De uitvoering van pentesten vindt immers plaats op basis van de behoefte van de interne organisatie.
25.	Beschrijvend document – §2.5 Omvang van de Opdracht	Kan de KB het aantal uitgevoerde pentesten en de gemiddelde omvang in mandagen over 2024 en 2025 delen, indien beschikbaar uitgesplitst naar type onderzoeksobject, zodat Inschrijvers capaciteit en tarief realistisch kunnen bepalen?	Zie het antwoord op vraag 24.
26.	Beschrijvend document – §2.5 Omvang van de Opdracht	Kan de KB inzicht geven in het aantal uitgevoerde pentesten per jaar gedurende de afgelopen twee of drie jaar, inclusief de gemiddelde en maximale omvang in mandagen per pentest?	Zie het antwoord op vraag 24.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
27.	Beschrijvend document – §2.5 Omvang van de Opdracht	Kunt u aangeven hoe de historische verdeling eruitziet qua omvang van pentesten (bijvoorbeeld klein, middelgroot, groot) zodat inschrijvers een beter beeld krijgen van de verwachte inzet onder de raamovereenkomst?	Zie het antwoord op vraag 24.
28.	Beschrijvend document – §2.5 Omvang van de Opdracht	Kunt u inzicht geven in het gemiddelde aantal pentesten per jaar over de afgelopen drie jaar, uitgesplitst naar bijvoorbeeld webapplicaties, API's, infrastructuur, cloudomgevingen en overige objecten?	Zie het antwoord op vraag 24.
29.	Beschrijvend document – §2.5 Omvang van de Opdracht	Kan de KB een indicatie geven van het verwachte aantal pentesten per jaar en de verdeling over bijvoorbeeld webapplicaties, infrastructuur, cloudomgevingen en mobiele applicaties, zodat Inschrijvers de benodigde capaciteit beter kunnen bepalen?	Zie het antwoord op vraag 24.
30.	Beschrijvend document – §2.5 Omvang van de Opdracht	Kan de Aanbestedende dienst een indicatie geven van het aantal pentesten dat jaarlijks wordt verwacht, de gemiddelde omvang van deze pentesten in mandagen en het maximaal verwachte aantal gelijktijdig lopende pentesten? Dit stelt Inschrijvers in staat om een passende capaciteits- en continuïteitsplanning op te stellen.	Zie het antwoord op vraag 24. De KB verwacht dat in de regel niet meer dan drie pentesten gelijktijdig worden uitgevoerd.
31.	Beschrijvend document – §2.5 Omvang van de Opdracht	Beschrijvend document, paragraaf 2.5. U benoemt de geraamde omvang van de opdracht. Kan u aangeven welk aantal penetratietesten en met welke gemiddelde omvang van elk u jaarlijks typisch afneemt?	Zie het antwoord op vraag 24.
32.	Beschrijvend document – §2.5 Omvang van de Opdracht	§2.5 Omvang van de Opdracht Kan Opdrachtgever een niet-bindende indicatie geven van het verwachte volume, de typen opdrachten en eventuele piekperioden gedurende de eerste twee contractjaren?	Zie het antwoord op vraag 24. De KB verwacht geen specifieke piekperioden.
33.	Beschrijvend document – §2.5 Omvang van de Opdracht	§2.5 Omvang van de Opdracht Kan Opdrachtgever, voor zover beschikbaar en eventueel in bandbreedtes, inzicht geven in het historische aandeel opdrachten op	Zie het antwoord op vraag 24.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		locatie, de gemiddelde doorlooptijd, het voorkomen en de duur van piekbelasting en het aandeel opdrachten waarvoor specialistische technische expertise vereist was?	
34.	Beschrijvend document – §2.5 Omvang van de Opdracht	§2.5 Omvang van de Opdracht Kan Opdrachtgever, voor zover beschikbaar en eventueel in bandbreedtes, inzicht geven in het historische aandeel black-box-, grey-box- en white-boxonderzoeken, de gebruikelijke complexiteit en het aantal hertesten?	Zie het antwoord op vraag 24.
35.	Beschrijvend document – §2.5 Omvang van de Opdracht	§2.5 Omvang van de Opdracht Kan Opdrachtgever, voor zover beschikbaar en eventueel in bandbreedtes, inzicht geven in de historische verdeling tussen webapplicaties, API's, mobiele toepassingen, infrastructuur, cloudomgevingen en overige omgevingen?	Zie het antwoord op vraag 24.
36.	Beschrijvend document – §2.5 Omvang van de Opdracht	§2.5 Omvang van de Opdracht Indien de gevraagde historische of verwachte informatie niet beschikbaar is, kan Opdrachtgever uniforme calculatieaannames verstrekken waarmee alle Inschrijvers capaciteit, personeelsmix en continuïteitsmaatregelen op dezelfde basis kunnen onderbouwen?	Nee. De KB verstrekt geen uniforme calculatieaannames; deze kan de KB niet vaststellen. Het gunningscriterium Prijs heeft uitsluitend betrekking op het all-in tarief per mandag (zie Bijlage 5). Zie verder het antwoord op vraag 24.
37.	Beschrijvend document – §2.5 Omvang / Raamovereenkomst art. 2.5	2.5 en §2.5 maximale waarde De Raamovereenkomst bepaalt dat Opdrachtgever bij het bereiken van de maximale waarde met onmiddellijke ingang mag opzeggen, terwijl het Beschrijvend document spreekt over een opzegtermijn van maximaal drie maanden. Kan Opdrachtgever verduidelijken welke regeling geldt? Kan tevens worden bevestigd dat het bereiken van de maximale waarde uitsluitend verhindert dat nieuwe Nadere Overeenkomsten worden gesloten en geen gevolgen heeft voor reeds gesloten Nadere Overeenkomsten, lopende pentesten, rapportageverplichtingen en de betaling daarvan?	De bepalingen zijn niet tegenstrijdig. De KB kan de Raamovereenkomst bij het bereiken van de maximale omvang opzeggen met een opzegtermijn van maximaal drie maanden; opzegging met onmiddellijke ingang valt daarbinnen. Het bereiken van de maximale omvang heeft geen gevolgen voor reeds gesloten Nadere Overeenkomsten; deze worden conform de gemaakte afspraken uitgevoerd en betaald.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
38.	Beschrijvend document – §2.5 Omvang / Raamovereenkomst art. 2.5	Het Beschrijvend document noemt bij het bereiken van de maximale omvang een opzegtermijn van maximaal drie maanden, terwijl artikel 2.5 onmiddellijke opzegging toestaat. Welke regeling geldt? Kunt u tevens bevestigen dat reeds gesloten Nadere Overeenkomsten in dat geval worden uitgevoerd en betaald conform de gemaakte afspraken?	Zie het antwoord op vraag 37.
39.	Beschrijvend document – §2.5 Omvang / Raamovereenkomst art. 2.5	Paragraaf 2.5 van het Beschrijvend document noemt bij het bereiken van de maximale omvang een opzegtermijn van maximaal 3 maanden. Artikel 2.5 van de concept Raamovereenkomst spreekt van opzegging met onmiddellijke ingang. Welke bepaling is van toepassing? Wij verzoeken de KB de opzegtermijn van 3 maanden in de Raamovereenkomst op te nemen.	Nee, dat is niet akkoord. Zie het antwoord op vraag 37.
40.	Beschrijvend document – §2.7 Raamovereenkomst	In de Aanbestedingsstukken wordt op meerdere plaatsen gesproken over meerdere partijen en over de winnende Inschrijver(s), terwijl elders wordt aangegeven dat de KB voornemens is een Raamovereenkomst met één Opdrachtnemer te sluiten. Kunt u bevestigen hoeveel Opdrachtnemers de KB voornemens is te contracteren?	De KB sluit de Raamovereenkomst met één Opdrachtnemer.
41.	Beschrijvend document – §2.8 Verwerkersovereenkomst	Kan de KB toelichten waarom in paragraaf 2.8 als uitgangspunt wordt gehanteerd dat een verwerkersovereenkomst wordt gesloten, terwijl eis E47 expliciet vermeldt dat momenteel niet vaststaat of gedurende de looptijd een verwerkersrelatie ontstaat? Wij zijn van mening dat de uitvoering van pentesten niet zonder meer leidt tot een verwerkersrelatie en dat geheimhouding, informatiebeveiliging en zorgvuldige omgang met eventueel aangetroffen persoonsgegevens contractueel kunnen worden geborgd. Op basis van welke criteria bepaalt de KB of een verwerkersovereenkomst noodzakelijk is?	De KB heeft de Verwerkersovereenkomst verstrekt voor het geval er wél een verwerkersrelatie ontstaat tussen Opdrachtnemer en de KB. Tijdens de implementatie zullen Partijen vaststellen of er sprake is van een verwerkersrelatie. Indien dit het geval is, wordt de Verwerkersovereenkomst alsnog gesloten.
42.	Beschrijvend document – §2.8 Verwerkersovereenkomst	Wij constateren dat de aanbestedingsdocumentatie voorziet in het sluiten van een verwerkersovereenkomst voor de dienstverlening. Wij vragen ons af of dit voor de uitvoering van penetratietesten in alle gevallen passend is. Bij een penetratietest verwerkt de leverancier	De KB kan dit niet op voorhand bevestigen. Zie het antwoord op vraag 41.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		persoonsgegevens niet ten behoeve van een door de opdrachtgever bepaald verwerkingsdoel, maar voert de leverancier, binnen de door de opdrachtgever geautoriseerde scope, beveiligingstests uit met als doel kwetsbaarheden in systemen, applicaties en infrastructuur te identificeren. Het enkele feit dat de leverancier daarbij mogelijk toegang krijgt tot persoonsgegevens, of dat persoonsgegevens zich bevinden in de systemen waarop de test wordt uitgevoerd, betekent naar onze mening niet zonder meer dat sprake is van verwerking van persoonsgegevens namens de opdrachtgever in de zin van artikel 4, onder 2 en 8, AVG. De eventuele toegang tot persoonsgegevens is immers niet het doel van de dienstverlening, maar een mogelijk en onvermijdelijk neveneffect van het testen van de betreffende systemen. De rol van de leverancier bij een penetratietest verschilt daarmee van die van een reguliere verwerker die persoonsgegevens namens de verwerkingsverantwoordelijke verwerkt voor een specifiek, door de verwerkingsverantwoordelijke bepaald doel. Vraag Kan de aanbestedende dienst bevestigen dat een leverancier die uitsluitend penetratietesten uitvoert, en daarbij binnen een vooraf overeengekomen en door de opdrachtgever geautoriseerde scope werkt, niet als verwerker wordt aangemerkt enkel vanwege de mogelijke incidentele toegang tot persoonsgegevens die zich in de geteste systemen bevinden? Indien de aanbestedende dienst van mening is dat voor de uitvoering van de pentestwerkzaamheden wél sprake is van een verwerkersrelatie, kan zij dan toelichten op basis van welke concrete verwerkingsactiviteiten en doeleinden zij tot die kwalificatie komt? Indien de aanbestedende dienst vasthoudt aan het gebruik van een verwerkersovereenkomst, verzoeken wij tevens te bevestigen dat deze uitsluitend betrekking heeft op daadwerkelijke verwerkingsactiviteiten die kwalificeren als verwerking namens de opdrachtgever en niet op de enkele mogelijkheid dat tijdens geautoriseerde security testing persoonsgegevens incidenteel kunnen worden ingezien.	

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
43.	Beschrijvend document – §2.8 Verwerkersovereenkomst	"Voor zover bij het verlenen van onze diensten persoonsgegevens worden verwerkt, beschouwt Opdrachtnemer zich als verwerkingsverantwoordelijke in de zin van de AVG. Dit betekent dat Opdrachtnemer geen verwerkersovereenkomsten sluit met klanten aangezien dat enkel vereist en passend is als Opdrachtnemer optreedt als verwerker. Achtergrond van dit standpunt is dat Opdrachtnemer door klanten wordt ingeschakeld vanwege zijn bijzondere expertise over het betreffende onderwerp en dus zijn diensten verleent als professioneel, onafhankelijk adviseur. Opdrachtnemer bepaalt volledig zelfstandig hoe zij haar werkzaamheden uit zal voeren, welke middelen zij daarbij gebruikt en welke persoonsgegevens daarvoor nodig zijn en stelt ook geheel zelfstandig haar adviezen op. Deze zelfstandigheid is essentieel voor Opdrachtnemer om de kwaliteit van haar dienstverlening te kunnen blijven waarborgen. De verplichting om aanwijzingen van de klant op te volgen t.a.v. welke persoonsgegevens we mogen verwerken en hoe wij dat precies mogen doen, zoals een verwerker dient te doen, doet inherent afbreuk aan de autonomie die Opdrachtnemer nodig heeft om kwalitatief goede diensten te kunnen leveren. Het verwerken van persoonsgegevens is ook niet de kern van onze diensten maar veeleer een noodzakelijke bijkomstigheid om onze diensten te kunnen leveren. Ten slotte; voor zover Opdrachtnemer instructies krijgt van cliënten zien die in principe op de gewenste output van onze dienstverlening en niet op de wijze waarop wij persoonsgegevens moeten verwerken. Gelet op het voorgaande zijn wij van mening dat het sluiten van een verwerkersovereenkomst niet passend is gezien de AVG-rol die wij feitelijk hebben (verantwoordelijke), noch noodzakelijk voor compliance met de AVG. Als verantwoordelijke zal Opdrachtnemer er zelf voor zorgen dat de noodzakelijke verwerkingen van persoonsgegevens voldoen aan de AVG. Opdrachtnemer is wèl bereid om afspraken te maken over de verwerking van persoonsgegevens die passen bij een situatie waarin sprake is van twee zelfstandige verwerkingsverantwoordelijken. Een instructierecht kan daarvan in ieder geval geen onderdeel uitmaken.	Nee, de KB deelt deze visie niet op voorhand. Of Opdrachtnemer als Verwerker kwalificeert, wordt tijdens de implementatie vastgesteld (zie het antwoord op vraag 41).

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		Deelt u onze visie dat, nu Opdrachtnemer als verwerkingsverantwoordelijke geen instructies van Opdrachtgever zal krijgen inzake de verwerking van persoonsgegevens, in het kader van voorliggende opdracht geen verwerkingsovereenkomst zoals bedoeld in art 14.2 ARBIT-2022 tot stand zal komen. Zo nee, waarom niet?"	
44.	Beschrijvend document – §2.8 Verwerkersovereenkomst	Door de aard van de opdracht kwalificeren wij, net als u, als zelfstandig verwerkingsverantwoordelijke bij de werkzaamheden die wij voor u verrichten. In de verhouding ‘opdrachtgever’ en ‘opdrachtnemer’ is van belang of de opdrachtnemer overeenkomstig de instructies van de opdrachtgever en onder (uitdrukkelijke) verantwoordelijkheid van de opdrachtgever persoonsgegevens verwerkt. Dergelijke instructies en verantwoordelijkheid zijn essentieel om vast te stellen of een partij verwerkingsverantwoordelijke dan wel verwerker is. Aangezien u aan ons een opdracht verstrekt die niet primair gericht is op het verwerken van persoonsgegevens, wij die opdracht onafhankelijk uitvoeren en u ons inschakelt in verband met onze professionele deskundigheid, is van dergelijke instructies en verantwoordelijkheid geen sprake. Wij bepalen immers welke stukken nodig zijn om onze werkzaamheden te verrichten, wat wij met die stukken doen en welke instrumenten (zoals software) wij daarbij gebruiken. Daarmee kwalificeren wij als verwerkingsverantwoordelijke en hoeft er geen verwerkersovereenkomst gesloten te worden. Kunt u op basis van het voorgaande bevestigen dat beide partijen als zelfstandig verwerkingsverantwoordelijke kwalificeren en dat de verwerkersovereenkomst buiten toepassing wordt verklaard?	De KB kan dit niet op voorhand bevestigen. Zie het antwoord op vraag 41.
45.	Beschrijvend document – §2.8 Verwerkersovereenkomst	Verwacht u dat in het kader van de opdracht (mogelijk) persoonsgegevens door Opdrachtnemer worden verwerkt? Opdrachtnemer stelt voor om art. 18 ARBIT buiten toepassing te laten en in plaats daarvan een verwerkersovereenkomst nader overeen te komen.	Zie het antwoord op vraag 41. De KB wil de ARBIT op dit onderdeel niet aanpassen.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		Kunt u dat bevestigen? Zo niet, dan verzoeken wij u dat duidelijk te motiveren.	
46.	Beschrijvend document – §2.8 Verwerkersovereenkomst	Merkt de KB Opdrachtnemer bij de uitvoering van pentesten aan als verwerker? Wordt de Verwerkersovereenkomst eenmalig bij aanvang van de Raamovereenkomst gesloten of per Nadere Opdracht?	Zie het antwoord op vraag 41. De Verwerkersovereenkomst wordt eenmalig gesloten, maar de daarbij behorende bijlagen kunnen worden aangepast.
47.	Beschrijvend document – §2.9 Herzieningsclausule	§2.9 herzieningsclausule De herzieningsclausule maakt aanvullende opdrachten mogelijk tot 10% van de maximale raming. Kan Opdrachtgever bevestigen dat deze bepaling uitsluitend een aanbestedingsrechtelijke mogelijkheid biedt en Opdrachtnemer niet verplicht aanvullende of gewijzigde diensten zonder voorafgaande schriftelijke overeenstemming over scope, planning, risico's en vergoeding uit te voeren?	Ja, dat wordt bevestigd. Daarbij wordt opgemerkt dat een wijziging van de scope van de Raamovereenkomst niet mogelijk is; de herzieningsclausule biedt uitsluitend ruimte voor aanvullende opdrachten die nauw verband houden met de Opdracht (paragraaf 2.9 van het Beschrijvend document).
48.	Beschrijvend document – §2.9 Herzieningsclausule	Kunt u bevestigen dat uitbreiding van de overeengekomen testscope, bijvoorbeeld door toevoeging van systemen, applicaties, gebruikersrollen, interfaces of testdoelstellingen, wordt behandeld als een wijziging van de betreffende Nadere Overeenkomst?	Ja. Een uitbreiding van de scope van een lopende Nadere Opdracht wordt behandeld conform eis E56.
49.	Beschrijvend document – §3.1 Planning	In de planning sluiten de tweede vragenronde op maandag 26 oktober om 10.00 uur. Hierdoor ligt de feitelijke interne afronding voor inschrijvers op de voorafgaande vrijdag 23 oktober, wat voor de tweede vragenronde kort is aangezien de nvi 1 gepubliceerd wordt op maandag 19 oktober. Daarnaast valt het einde van de bezwaartermijn op zondag 27 december 2026 en omvat deze termijn de kerstdagen. Wij verzoeken de KB de planning meer aan te laten sluiten op reguliere werkdagen, bijvoorbeeld door de vragenronden op een dinsdag of woensdag te laten sluiten. Wilt u daarnaast bevestigen dat de bezwaartermijn, overeenkomstig de geldende termijnregels, niet eindigt op zondag 27 december maar op de eerstvolgende werkdag? Wilt u overwegen de bezwaartermijn vanwege de kerstperiode ruimer vast te stellen?	Nee, de sluitingsdata van de vragenrondes worden niet gewijzigd. De planning biedt naar het oordeel van de KB voldoende tijd. De einddatum van de bezwaartermijn in de planning (paragraaf 3.1 van het Beschrijvend document) wordt aangepast naar 28 december 2026; dit betreft inderdaad een omissie. De KB ziet geen aanleiding de bezwaartermijn verder te verruimen.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
50.	Beschrijvend document – §4 Controleverklaring	Indien Inschrijver of een Derde een recent opgerichte vennootschap is waarvan nog geen boekjaar is afgesloten, en er dus nog geen controle-, beoordelings- of samenstellingsverklaring bestaat, welk bewijsmiddel accepteert de KB dan ter voldoening aan deze Geschiktheidseis?	In dat geval kan Inschrijver een beroep doen op de financiële en economische draagkracht van een Derde (bijvoorbeeld de moedermaatschappij) door middel van Bijlage 7. Indien dat niet mogelijk is, kan Inschrijver na voorlopige gunning een ander vergelijkbaar bewijsstuk overleggen, zoals een door een accountant afgegeven verklaring bij de openingsbalans. Het is daarbij van belang dat de continuïteit van de onderneming daadwerkelijk aangetoond wordt.
51.	Beschrijvend document – §4 Verzekering	Verlangt de KB naast de bedrijfsaansprakelijkheidsverzekering (AVB) ook een afzonderlijke beroepsaansprakelijkheidsverzekering? Zo ja, welke minimale dekking geldt daarvoor?	Ja. Inschrijver hoeft deze verzekering echter niet aan te tonen in het kader van de Geschiktheidseisen. Op grond van artikel 52 ARBIT-2022 dient Opdrachtnemer passend verzekerd te zijn tegen beroepsaansprakelijkheid. De KB hanteert hiervoor een minimale dekking van € 1.250.000,- per aanspraak en € 2.500.000,- per verzekeringsjaar (overeenkomstig de systematiek van artikel 29.2 ARBIT-2022).
52.	Beschrijvend document – §4 Verzekering	Artikel 29.2 ARBIT-2022 noemt een minimale dekking van € 1.250.000 per aanspraak voor de aansprakelijkheidsverzekering voor bedrijven. Voor de beroepsaansprakelijkheidsverzekering (artikel 52 ARBIT-2022) wordt geen minimumbedrag genoemd. Welk minimum verzekerd bedrag hanteert de KB voor de beroepsaansprakelijkheidsverzekering?	Zie het antwoord op vraag 51.
53.	Beschrijvend document – §4 Verzekering	Verlangt de KB naast een aansprakelijkheidsverzekering voor bedrijven en een beroepsaansprakelijkheidsverzekering ook een cyberverzekering? Zo ja, met welke minimale dekking?	Nee. De KB verlangt geen afzonderlijke cyberverzekering. Voor de beroepsaansprakelijkheidsverzekering, zie het antwoord op vraag 51.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
54.	Beschrijvend document – §4 Verzekering	Kan de KB bevestigen dat een polis waarop een eigen risico is vermeld niet tot uitsluiting leidt, mits Opdrachtnemer dit eigen risico niet met de KB verrekent?	Ja, dat wordt bevestigd.
55.	Beschrijvend document – §4 Verzekering	Accepteert de KB een verzekeringscertificaat van een groepspolis van de moedermaatschappij, waarop Inschrijver als (mede)verzekerde is vermeld?	Ja, mits Inschrijver op het verzekeringscertificaat als (mede)verzekerde is vermeld en de minimaal verzekerde bedragen worden gehaald.
56.	Beschrijvend document – §4 Referenties, kerncompetentie 1	Moeten de minimaal vier verschillende pentesten betrekking hebben op vier verschillende applicaties of platformen, of kunnen ook afzonderlijke pentesten met verschillende scopes of onderzoeksobjecten (applicaties, API's, koppelvlakken, beheervoorzieningen) binnen één samenhangend bedrijfskritiek platform meetellen?	De vier pentesten hoeven geen betrekking te hebben op vier verschillende applicaties of platformen. Ook afzonderlijke pentesten met een eigen scope, uitvoering en rapportage op verschillende onderdelen (zoals applicaties, API's, koppelvlakken of beheervoorzieningen) binnen één bedrijfskritiek platform tellen mee. Een hertest die uitsluitend dient ter verificatie van eerder gevonden kwetsbaarheden telt niet als afzonderlijke pentest.
57.	Beschrijvend document – §4 Referenties, kerncompetentie 1	Kan de KB bevestigen dat voor kerncompetentie 1 vier afzonderlijke pentestopdrachten binnen één klantrelatie of raamovereenkomst volstaan, mits deze binnen een aaneengesloten periode van twaalf maanden zijn uitgevoerd?	Ja, dat wordt bevestigd.
58.	Beschrijvend document – §4 Referenties, kerncompetentie 1	Mogen de vier pentesten bestaan uit meerdere afzonderlijke opdrachten bij dezelfde opdrachtgever, of moeten zij onder één overeenkomst zijn uitgevoerd?	De vier pentesten mogen bestaan uit meerdere afzonderlijke opdrachten bij dezelfde opdrachtgever. Zie ook het antwoord op vraag 57.
59.	Beschrijvend document – §4 Referenties, kerncompetentie 1	Is het toegestaan dat de vier pentesten zijn uitgevoerd op verschillende applicaties of platformen van dezelfde opdrachtgever, binnen één (raam)overeenkomst? Dient de aaneengesloten periode van 12 maanden volledig binnen de termijn van drie jaar voor de uiterste indieningsdatum te vallen?	Ja, dat is toegestaan. De aaneengesloten periode van twaalf maanden dient volledig binnen de periode van drie jaar voorafgaand aan de uiterste datum van indiening van de Inschrijving te vallen.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
60.	Beschrijvend document – §4 Referenties, kerncompetentie 1	Mag de aaneengesloten periode van twaalf maanden iedere periode zijn die binnen de toegestane referentieperiode valt, dus elke periode van twaalf maanden waarvan de einddatum niet meer dan drie jaar vóór de sluitingsdatum van de inschrijving ligt?	Zie het antwoord op vraag 59.
61.	Beschrijvend document – §4 Referenties, kerncompetentie 1	Tellen periodieke pentesten van hetzelfde platform als verschillende pentesten wanneer iedere test een afzonderlijke scope, uitvoering en eindrapportage heeft? Telt een hertest die uitsluitend dient ter verificatie van eerder gevonden kwetsbaarheden daarbij als een afzonderlijke pentest?	Periodieke pentesten van hetzelfde platform tellen als verschillende pentesten, mits iedere pentest een eigen scope, uitvoering en eindrapportage heeft. Een hertest telt niet als afzonderlijke pentest (zie het antwoord op vraag 56).
62.	Beschrijvend document – §4 Referenties, kerncompetentie 1	Wat verstaat de KB onder 'bedrijfskritisch' en 'meerdere koppelvlakken'? Moeten de vier pentests vier verschillende applicaties betreffen, of volstaan vier opdrachten (ook hertests of onderdelen van hetzelfde platform)?	Onder bedrijfskritisch verstaat de KB een applicatie of platform dat essentieel is voor de primaire processen of dienstverlening van de opdrachtgever, waarbij uitval of compromittering een aanzienlijke impact heeft. Onder koppelvlakken verstaat de KB de interfaces waarmee de applicatie of het platform gegevens uitwisselt met andere systemen, applicaties of partijen (zoals API's en integraties). Voor de vier pentesten, zie de antwoorden op de vragen 56 en 61.
63.	Beschrijvend document – §4 Referenties, kerncompetentie 1	Opdrachtgever stelt bij kerncompetentie 1 het volgende: "Inschrijver heeft aantoonbare ervaring met de uitvoering van pentesten van bedrijfskritieke applicaties/platformen waarbij er sprake is van meerdere koppelvlakken." Kunt u aangeven wat de Koninklijke Bibliotheek in deze context onder koppelvlakken verstaat?	Zie het antwoord op vraag 62.
64.	Beschrijvend document – §4 Referenties, kerncompetentie 2	Kerncompetentie 2 vereist ervaring met een pentest bij "een publieke instelling (overheidsinstelling)". (a) Welke objectief toetsbare criteria hanteert de KB voor dit begrip? Is vereist dat de referent een aanbestedende dienst of publiekrechtelijke instelling in de zin van	a. De in de vraag genoemde voorbeelden van organisaties mogen eveneens worden ingezet om de kerncompetentie aan te tonen.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		artikel 1.1 Aanbestedingswet 2012 is, of vallen hieronder ook organisaties die volledig eigendom zijn van de Staat en op grond van een wet een publieke taak uitvoeren (zoals bij wet aangewezen nationale instituten met een private rechtsvorm), alsmede semipublieke organisaties zoals zorginstellingen, onderwijsinstellingen en woningcorporaties? (b) De competentie die de KB met KC2 beoogt te toetsen, is het uitvoeren van een pentest binnen een omgeving met publieke normenkaders (zoals BIO, NCSC-richtlijnen, DigiD-normenkader). Die competentie is niet afhankelijk van de rechtsvorm van de opdrachtgever. Een eis die uitsluitend ervaring bij een overheidsinstelling accepteert, sluit gekwalificeerde inschrijvers uit en beperkt de mededinging, terwijl voorschrift 3.5G van de Gids Proportionaliteit voorschrijft dat referentie-eisen worden geformuleerd als kerncompetenties en niet als ervaring bij een bepaald type organisatie. Is de KB bereid KC2 te herformuleren tot: "Inschrijver heeft aantoonbare ervaring met de uitvoering van een pentest van een applicatie en/of platform die is getoetst aan een of meer publieke normenkaders (bijvoorbeeld BIO, NCSC ICT-beveiligingsrichtlijnen voor webapplicaties, DigiD-normenkader), bij een publieke, semipublieke of private organisatie"? (c) Indien de KB KC2 ongewijzigd laat: accepteert de KB dan een pentest bij een private organisatie die DigiD-aansluitingen of andere overheidsdiensten exploiteert en daarvoor aan het DigiD-normenkader of de BIO is getoetst?	b. Nee, de KB is het niet met Inschrijver eens dat de door de KB gestelde kerncompetentie in strijd is met het proportionaliteitsbeginsel. Zie de uitbreiding zoals gegeven bij onderdeel a. c. Nee, tenzij de betreffende organisatie kwalificeert als organisatie met een publieke taak (zie onderdeel a en het antwoord op vraag 65). Het enkele feit dat een private organisatie DigiD-aansluitingen exploiteert of aan het DigiD-normenkader of de BIO is getoetst, volstaat niet.
65.	Beschrijvend document – §4 Referenties, kerncompetentie 2	Inschrijver verzoekt om voor kerncompetentie 2 onder “publieke instelling (overheidsinstelling)” ook te verstaan: een zelfstandig bestuursorgaan, decentrale overheid, onderwijsinstelling, publiekrechtelijke organisatie, semioverheidsorganisatie en/of andere organisatie met een publieke taak? Wij stellen deze aanpassing voor, omdat de gevraagde ervaring en competenties ook bij dergelijke organisaties in vergelijkbare mate kunnen worden opgedaan. Een beperking tot uitsluitend overheidsinstellingen lijkt de kring van geschikte referenties onnodig te beperken, terwijl de relevante ervaring, complexiteit en	Ja, dat is akkoord. Dit is reeds de insteek van de KB geweest met de geformuleerde kerncompetentie.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		vergelijkbaarheid van de opdracht ook bij semipublieke organisaties aanwezig kunnen zijn. Wij nemen bij dit voorstel ook het uitgangspunt uit de Gids Proportionaliteit mee dat geschiktheidseisen in redelijke verhouding dienen te staan tot het voorwerp van de opdracht en voldoende ruimte moeten bieden aan ondernemingen die de vereiste deskundigheid op gelijkwaardige wijze kunnen aantonen.	
66.	Beschrijvend document – §4 Referenties, kerncompetentie 2	Wat verstaat de KB onder 'publieke instelling (overheidsinstelling)'? Vallen ook zelfstandige bestuursorganen, gemeenten, provincies, waterschappen, publiekrechtelijke instellingen in onderwijs, zorg en cultuur, vitale infrastructuur en overheden van andere EU-lidstaten daaronder?	Zie de antwoorden op de vragen 64 en 65.
67.	Beschrijvend document – §4 Referenties, kerncompetentie 2	Bij kerncompetentie 2 wordt gevraagd: "Inschrijver heeft aantoonbare ervaring met de uitvoering van een pentest van een applicatie en/of platform van een publieke instelling (overheidsinstelling)". Kunt u aangeven wat de reden is waarom dit specifiek voor een publieke instelling/overheidsinstelling moet zijn uitgevoerd?	Zie de antwoorden op de vragen 64 en 65. Aanvullend: de KB acht deze ervaring van cruciaal belang voor de uitvoering van de Opdracht.
68.	Beschrijvend document – §4 Referenties, kerncompetentie 2	Beschrijvend document, Hoofdstuk 4. U benoemt op pagina 16 en verder de Geschiktheidseisen technische en beroepsbekwaamheid. Wij wijzen u er op dat de drempels voor de kerncompetenties in vergelijking met andere aanbestedingen zeer laag zijn. De ervaring met andere aanbestedingen leert dat een aanbesteding met dergelijke lage drempels op geschiktheid veel Gegadigden aantrekt, in eerdere aanbestedingen zelfs tientallen. Staat u er voor pen om de Geschiktheidseisen significant aan te scherpen?	Nee. De kerncompetenties zijn gebaseerd op de omvang van de Opdracht en conform de uitgangspunten van de Gids Proportionaliteit. De KB ziet geen aanleiding de kerncompetenties aan te scherpen.
69.	Beschrijvend document – §4 Referenties (algemeen)	Inschrijver neemt aan dat één referentie beide kerncompetenties mag afdekken, klopt dat ?	Ja, dat is correct (zie hoofdstuk 4 van het Beschrijvend document).
70.	Beschrijvend document – §4 Referenties (algemeen)	Indien een organisatie tijdens de referentieperiode uitsluitend haar handelsnaam wijzigt maar dezelfde rechtspersoon en hetzelfde KvK-nummer behoudt, worden opdrachten onder de oude en de nieuwe	Ja, dat wordt bevestigd.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		handelsnaam dan beschouwd als uitgevoerd voor dezelfde opdrachtgever?	
71.	Beschrijvend document – §4 Referenties (algemeen)	Mag Inschrijver voor het aantonen van de kerncompetenties gebruikmaken van referentieopdrachten die door de aangeboden (senior) pentester vanuit een detacheringsconstructie zijn uitgevoerd, mits deze pentester daadwerkelijk voor de uitvoering van de onderhavige Opdracht beschikbaar wordt gesteld?	Een referentie moet betrekking hebben op een opdracht die door Inschrijver zelf (dan wel een Derde waarop Inschrijver een beroep doet) is uitgevoerd. Indien de pentester vanuit Inschrijver is gedetacheerd en de pentesten in dat kader heeft uitgevoerd, is dat toegestaan. Ervaring die een individuele medewerker bij een andere onderneming heeft opgedaan telt niet mee.
72.	Beschrijvend document – §4 Referenties (algemeen)	Inschrijver neemt aan dat een referentie geaccepteerd als de einddatum binnen 3 jaar voor inschrijving ligt, maar de opdracht langer geleden is gestart, is dat correct ?	Ja, dat is correct. Let op: de aaneengesloten periode van twaalf maanden uit kerncompetentie 1 moet wel volledig binnen de periode van drie jaar voorafgaand aan de uiterste datum van indiening vallen (zie het antwoord op vraag 59).
73.	Beschrijvend document – §4 Referenties (algemeen)	Bevestigt de KB dat bij een lopende raamovereenkomst alleen de reeds gerealiseerde pentesten hoeven te worden beschreven, ook wanneer de raamovereenkomst zelf eerder dan drie jaar geleden is gestart?	Ja, dat wordt bevestigd. Bij een lopende opdracht tellen uitsluitend de reeds gerealiseerde pentesten mee.
74.	Beschrijvend document – §4 Referenties (algemeen)	Bevestigt de KB dat een nog lopende opdracht als referentie mag worden gebruikt wanneer de voor de kerncompetentie benodigde werkzaamheden en resultaten reeds zijn gerealiseerd?	Ja. Zie het antwoord op vraag 73.
75.	Beschrijvend document – §4 Referenties (algemeen)	Kwalificeert een privaatrechtelijke stichting zonder winstoogmerk, die op grond van een wettelijke regeling een publieke taak uitvoert, daarover rapporteert aan de Rijksoverheid en onder toezicht staat van een rijksinspectie, als "publieke instelling (overheidsinstelling)" in de zin van Kerncompetentie 2? Zo nee, welke kenmerken ontbreken dan volgens de KB?	Ja, een dergelijke organisatie voldoet.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
76.	Beschrijvend document – §4 Referenties (algemeen)	Indien bij een referentieopdracht de ene groepsmaatschappij formeel contractpartij van de opdrachtgever was en een andere groepsmaatschappij (verbonden in de zin van artikel 2:24b BW) de technische pentestwerkzaamheden feitelijk heeft uitgevoerd, mag de Inschrijver dan voor de technische en beroepsbekwaamheid (Kerncompetentie 1 en/of 2) een beroep doen op de uitvoerende groepsmaatschappij als Derde? Bevestigt de KB dat in dat geval een afzonderlijk UEA van de Derde en Bijlage 8 volstaan, en dat de Derde tijdens de uitvoering van de Raamovereenkomst daadwerkelijk moet worden ingezet voor de werkzaamheden waarvoor een beroep op haar wordt gedaan?	Ja, dat is toegestaan, mits uit de referentieverklaring (Bijlage 2) blijkt dat de Derde de pentestwerkzaamheden feitelijk heeft uitgevoerd. De Derde vult een eigen UEA in (Deel II A en B en Deel III) en Inschrijver voegt Bijlage 8 direct bij de Inschrijving, ondertekend door Inschrijver en de Derde (paragraaf 7.14 van het Beschrijvend document). Inschrijver is verplicht de Derde bij de uitvoering van de Raamovereenkomst daadwerkelijk in te zetten voor de werkzaamheden waarvoor een beroep op de Derde is gedaan. Daarnaast levert de Derde na voorlopige gunning dezelfde bewijsstukken met betrekking tot de Uitsluitingsgronden aan als Inschrijver (hoofdstuk 4).
77.	Beschrijvend document – §4 Vereiste standaarden (ISO 9001 / CCV)	In de aanbestedingsstukken worden zowel ISO 27001 als ISO 9001 als eis gesteld. Kunt u toelichten waarom naast ISO 27001 specifiek ook ISO 9001 noodzakelijk wordt geacht voor de uitvoering van deze opdracht? Gezien de aard van de gevraagde pentestwerkzaamheden lijkt een keurmerk dat specifiek toeziet op de kwaliteit en uitvoering van penetratietesten, zoals het CCV Keurmerk Pentesten, inhoudelijk directer aan te sluiten op de opdracht dan een algemeen kwaliteitsmanagementcertificaat als ISO 9001. Kan de aanbestedende dienst toelichten waarom ISO 9001 als eis is opgenomen en het CCV Keurmerk Pentesten niet? Tevens vernemen wij graag of het CCV Keurmerk Pentesten, in combinatie met de reeds vereiste ISO 27001-certificering, als gelijkwaardig alternatief voor ISO 9001 kan worden geaccepteerd.	Ja. Het CCV Keurmerk Pentesten wordt door de KB geaccepteerd als gelijkwaardig bewijs voor ISO 9001:2015. De eis ten aanzien van ISO 27001 blijft onverkort van toepassing.
78.	Beschrijvend document – §4 Vereiste standaarden (ISO 9001 / CCV)	Beschouwt de KB een geldige certificering volgens het CCV-certificatieschema Cyber Security Pen Test (uitgegeven door een geaccrediteerde certificerende instelling), dat eisen stelt aan procesbeheersing, competentiebeheer, kwaliteitsborging en	Ja. Zie het antwoord op vraag 77.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		klachtafhandeling van pentestdienstverlening, als gelijkwaardig aan ISO 9001:2015 voor de uitvoering van deze Opdracht? Zo nee, welk bewijs verwacht de KB van een Inschrijver die geen ISO 9001-certificaat heeft?	
79.	Beschrijvend document – §4 Vereiste standaarden (ISO 9001 / CCV)	De KB stelt in de aanbestedingsstukken eisen aan het kwaliteits- en informatiebeveiligingsmanagementsysteem van Opdrachtnemer en in PvE-eis E27 aan de certificeringen van individuele pentesters. Deze eisen tonen echter niet aan dat ook het volledige proces voor het voorbereiden, uitvoeren, controleren en rapporteren van pentesten onafhankelijk is getoetst. Het CCV-keurmerk Pentesten stelt specifieke eisen aan onder meer de kwalificaties en integriteit van de pentestorganisatie, de voorbereiding en vastlegging van het testplan, de uitvoering van de pentest, de verantwoordelijkheden binnen het testproces, de controle van de resultaten en de inhoud en kwaliteit van de rapportage. Gezien de toegang die pentesters krijgen tot mogelijk kwetsbare applicaties, omgevingen en informatie over beveiligingsrisico's, verzoekt Inschrijver de KB om het beschikken over het CCV-keurmerk Pentesten als eis op te nemen. Kan de KB hiermee instemmen en aangeven op welk moment het bewijs moet worden overgelegd? Indien de KB hiermee niet instemt, kan zij dan toelichten op welke wijze zij onafhankelijk vaststelt dat het volledige pentestproces van Opdrachtnemer voldoet aan aantoonbare eisen ten aanzien van kwaliteit, betrouwbaarheid, integriteit en reproduceerbaarheid?	Dit wordt niet als nieuwe geschiktheidseis opgenomen. Zie wel het antwoord op vraag 77.
80.	Beschrijvend document – §4 Vereiste standaarden (ISO 9001 / CCV)	Dank voor uw heldere aanbesteding. Eén vraag/suggestie: veel van de eisen die u terecht stelt (bijvoorbeeld certificering van pentesters, de structuur van de rapportage, kwaliteitsmanagementsysteem, ...) worden afgedekt door het Keurmerk Pentesten van het CCV, een breed gedragen keurmerk in de markt. Is het een optie om de aanbesteding te vereenvoudigen door deze eisen simpelweg te vervangen door een geldig Keurmerk te vereisen?	Zie de antwoorden op de vragen 77 en 79.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
81.	Beschrijvend document – §4 Vereiste standaarden (ISO 27001)	In paragraaf 4.3.3 van het Beschrijvend Document wordt als vereiste standaard ISO 27001:2017 of gelijkwaardig genoemd. De norm NEN-EN-ISO/IEC 27001:2017 is inmiddels ingetrokken en vervangen. Kan de KB bevestigen dat de eis betrekking heeft op de actuele norm ISO/IEC 27001:2022, dan wel NEN-EN-ISO/IEC 27001:2023, of aantoonbaar gelijkwaardig, en de verwijzing in de aanbestedingsstukken hierop aanpassen? Kan de KB tevens bevestigen dat een certificaat dat uitsluitend betrekking heeft op de ingetrokken versie uit 2017 en niet tijdig is omgezet naar de actuele norm, niet als geldig bewijs wordt geaccepteerd?	Ja. De eis wordt aangepast naar ISO/IEC 27001:2022 (NEN-EN-ISO/IEC 27001:2023) of gelijkwaardig. Een certificaat dat uitsluitend betrekking heeft op een eerdere versie en niet tijdig is omgezet, is niet langer geldig en wordt niet als bewijs geaccepteerd.
82.	Beschrijvend document – §4 Vereiste standaarden (ISO 27001)	Accepteert de KB een geldig ISO/IEC 27001:2022-certificaat (inclusief Amd1:2024) als voldoening aan de eis "ISO 27001:2017"?	Ja. Zie het antwoord op vraag 81.
83.	Beschrijvend document – §4 Vereiste standaarden (ISO 27001)	In de geschiktheidseisen wordt verwezen naar ISO 27001:2017. Inmiddels is de actuele norm ISO/IEC 27001:2022. Bevestigt de KB dat certificering conform ISO/IEC 27001:2022 voldoet aan de gestelde eis?	Ja. Zie het antwoord op vraag 81.
84.	Beschrijvend document – §4 Vereiste standaarden (ISO 27001)	De gevraagde norm ISO 27001:2017 is opgevolgd door ISO/IEC 27001:2022. Kan de KB bevestigen dat een geldig certificaat conform ISO/IEC 27001:2022 voldoet aan deze Geschiktheidseis?	Ja. Zie het antwoord op vraag 81.
85.	Beschrijvend document – §4 Vereiste standaarden (ISO 27001)	Kan Opdrachtgever bevestigen dat een geldige SOC 2 Type II-rapportage met een Verklaring van Toepasselijkheid (SoA) die de SOC/MDR-dienstverlening expliciet omvat, als gelijkwaardig bewijs wordt geaccepteerd?	Nee. Een SOC 2 Type II-rapportage toont naar het oordeel van de KB niet aan dat Inschrijver beschikt over een informatiebeveiligingsmanagementsysteem conform ISO 27001.
86.	Beschrijvend document – §4 Vereiste standaarden (scope en aanlevering)	Moet de scope van de ISO 9001- en ISO 27001-certificering expliciet penetratietesten of cybersecurity noemen, of volstaat een scope die de voor deze Opdracht toegepaste kwaliteits- en informatiebeveiligingsprocessen omvat?	Een scope die de voor deze Opdracht toegepaste kwaliteits- en informatiebeveiligingsprocessen omvat, volstaat.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
87.	Beschrijvend document – §4 Vereiste standaarden (scope en aanlevering)	Volstaan ISO 9001- en ISO 27001-certificaten op naam van de moedermaatschappij van Inschrijver, dan wel een deelcertificaat van Inschrijver dat onderdeel is van het hoofdcertificaat van de moedermaatschappij, indien aantoonbaar is dat het gecertificeerde managementsysteem ook de Inschrijver en de uitvoering van deze Opdracht omvat?	Ja, mits uit het certificaat aantoonbaar blijkt dat Inschrijver en de uitvoering van deze Opdracht onder de scope van het gecertificeerde managementsysteem vallen. Indien het certificaat op naam van de moedermaatschappij staat, doet Inschrijver een beroep op de moedermaatschappij als Derde (Bijlage 8).
88.	Beschrijvend document – §4 Vereiste standaarden (scope en aanlevering)	In de paragraaf “Vereiste standaarden” staat dat Inschrijver op de dag van Inschrijving moet voldoen aan ISO 9001 en ISO 27001 of daaraan gelijkwaardige normen. In paragraaf 7.5 zijn de certificaten of gelijkwaardige bewijsstukken opgenomen in de checklist van bewijsstukken die na voorlopige gunning moeten worden aangeleverd. Deze bewijsstukken staan niet in de checklist bij Inschrijving van paragraaf 7.4. Bevestigt de KB dat Inschrijver op de uiterste inschrijfdatum aan beide vereiste standaarden moet voldoen, maar de certificaten of gelijkwaardige bewijsstukken pas na voorlopige gunning hoeft aan te leveren?	Ja, dat wordt bevestigd.
89.	Beschrijvend document – §5.1 Gunningscriteria (weging)	Beschrijvend document, paragraaf 5.1. U benoemt de verdeling van punten over gunningscriteria Kwaliteit en Prijs. Deze verdeling van punten is nu 60/40. Het is onze ervaring dat deze verhouding in verdeling, waarbij een prijs een relatief groot aandeel heeft, het startschot is voor een 'race naar de bodem' op prijs. Dit te meer omdat de elementen G1-G3 van het Gunningscriterium Kwaliteit relatief weinig ruimte te bieden voor Gegadigde om zich te onderscheiden op kwaliteit. Dit zijn namelijk elementen die in elke aanbesteding terugkomen, en elke Gegadigde heeft geperfectioneerd in de uitwerking. Uw nadeel is dat deze verdeling met name Gegadigden aantrekt die zeer lage prijzen aanbieden maar in de uitvoering een zeer uitgekleden dienstverlening aanbieden, niet passend voor de doelstellingen van de Aanbesteding die u in uw Beschrijvend Document benoemt.	Nee, dat is niet akkoord. De KB heeft bewust gekozen voor de huidige verhouding tussen kwaliteit en prijs. De weging wordt niet gewijzigd.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		Het is in aanbestedingen gangbaarder om een andere verdeling in kwaliteit/prijs te kiezen, bijvoorbeeld 90/10 of 80/20. Staat u er voor open om de puntenverdeling aan te passen?	
90.	Beschrijvend document – §5.1 Gunningscriteria (weging)	§5.1 Gunningscriteria, G1.1 Uitvoering van pentesten G1.1 Uitvoering van pentesten en G1.2 Rapportering hebben rechtstreeks betrekking op de kwaliteit en bruikbaarheid van de te leveren pentestdienst en vertegenwoordigen gezamenlijk 45 van de 60 beschikbare kwaliteitspunten. Is Opdrachtgever bereid voor G1.1 een minimale kwaliteitsscore vast te stellen?	Nee, dat is niet akkoord. De KB hanteert geen minimale kwaliteitsscore.
91.	Beschrijvend document – §5.1 Gunningscriteria (weging)	§5.1 Gunningscriteria, G1.2 Rapportering Is Opdrachtgever bereid voor G1.2 een minimale kwaliteitsscore vast te stellen?	Nee. Zie het antwoord op vraag 90.
92.	Beschrijvend document – §5.1 Gunningscriteria (weging)	§5.1 Gunningscriteria, G1.1 Uitvoering van pentesten, G1.2 Rapportering Indien Opdrachtgever geen afzonderlijke drempel per criterium wil hanteren, is Opdrachtgever dan bereid een minimale gezamenlijke score voor G1.1 en G1.2 vast te stellen, zodat een ontoereikende testuitvoering of rapportagekwaliteit niet volledig door een lage prijs kan worden gecompenseerd?	Nee. Zie het antwoord op vraag 90.
93.	Beschrijvend document – §5.1 Gunningscriteria (weging)	§5.1 Gunningscriteria, G1.1 Uitvoering van pentesten, G1.2 Rapportering Kan Opdrachtgever bepalen dat een Inschrijving die op G1.1 of G1.2 als “Matig” of “Onvoldoende” wordt beoordeeld niet voor gunning in aanmerking komt, ongeacht de met prijs behaalde score?	Nee. Zie het antwoord op vraag 90.
94.	Beschrijvend document – §5.1.1 Beoordelingssystematiek	In paragraaf 5.1.1 zijn voor de beoordeling van de open vragen vijf scoremogelijkheden opgenomen: 100%, 75%, 50%, 25% en 0%. Bevestigt de KB dat een individuele beoordelaar uitsluitend één van deze vijf percentages kan toekennen en dus geen tussenliggende score, zoals 60%, 80% of 90%? Bevestigt de KB tevens dat een	Ja, dat wordt bevestigd.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		tussenliggende score uitsluitend kan ontstaan door het middelen van de definitieve individuele scores van de beoordelaars?	
95.	Beschrijvend document – §5.1.1 Beoordelingssystematiek	In paragraaf 5.1.1 zijn per open vraag vijf scoremogelijkheden opgenomen: 100%, 75%, 50%, 25% en 0%. In paragraaf 6.1 staat dat iedere beoordelaar individueel een score geeft en dat de definitieve individuele scores vervolgens worden opgeteld en gedeeld door het aantal beoordelaars. Begrijpen wij correct dat hierdoor ook tussenliggende percentages en puntenscores kunnen ontstaan? Kan de KB dit bevestigen en de berekeningswijze toelichten, bijvoorbeeld wanneer drie beoordelaars voor G1.1 respectievelijk 100%, 75% en 75% toekennen?	Ja, dat is correct. In het genoemde voorbeeld bedraagt de score $(100\% + 75\% + 75\%) / 3 = 83,33\%$ van de maximaal te behalen 25 punten, oftewel 20,83 punten.
96.	Beschrijvend document – §5.1.1 Beoordelingssystematiek	Binnen het beoordelingskader levert een goede beantwoording een “positieve bijdrage” aan de dienstverlening en een uitstekende beantwoording een “zeer positieve bijdrage”. Ook wordt onderscheid gemaakt tussen “op onderdelen meerwaarde” en “uitstekende meerwaarde”. Kan de KB toelichten aan de hand van welke onderscheidende, zoveel mogelijk objectief verifieerbare kenmerken de beoordelingscommissie bepaalt of sprake is van een positieve dan wel zeer positieve bijdrage en van meerwaarde dan wel uitstekende meerwaarde? Hoe waarborgt de KB dat de beoordelaars deze begrippen onderling consistent toepassen?	De beoordelingscommissie beoordeelt iedere open vraag integraal aan de hand van de vraagstelling, de doelstellingen van de KB (paragraaf 2.2), de eisen uit de Aanbestedingsstukken en de omschrijvingen in de scoretabel. De KB geeft geen nadere invulling aan de begrippen uit de scoretabel en stelt geen aanvullende beoordelingsaspecten, minimumniveaus of voorbeelden van meerwaarde vast. Het is aan Inschrijver om concreet en onderbouwd aan te tonen op welke wijze zijn aanbod bijdraagt aan de vraagstelling van de KB. De betrokken inkoopadviseur ziet erop toe dat de beoordelingscommissie het beoordelingskader consistent toepast.
97.	Beschrijvend document – §5.1.1 Beoordelingssystematiek	Voor de beoordeling “Uitstekend” moet de beantwoording de verwachtingen van de KB overtreffen en/of uitstekende meerwaarde bieden. De concrete verwachtingen en de wijze waarop meerwaarde wordt vastgesteld, zijn niet afzonderlijk beschreven. Kan de KB aangeven welke verwachtingen zij hierbij als referentiekader hanteert en welke vormen van meerwaarde binnen	Zie het antwoord op vraag 96. Het Programma van Eisen vormt daarbij de minimale uitgangspunten.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		G1.1, G1.2 en G1.3 relevant zijn? Bevestigt de KB dat het Programma van Eisen en de bij het betreffende gunningscriterium beschreven doelstellingen, vraagstelling en aandachtspunten gezamenlijk het inhoudelijke ijkpunt vormen voor de beoordeling?	
98.	Beschrijvend document – §5.1.1 Beoordelingssystematiek	Kunt u toelichten welke kenmerken volgens de KB onderscheidende meerwaarde vormen bij de beantwoording van de kwaliteitscriteria G1.1, G1.2 en G1.3?	Zie het antwoord op vraag 96.
99.	Beschrijvend document – §5.1.1 Open vragen (omvang en opmaak)	De beantwoording van de kwalitatieve gunningscriteria moet in één document worden opgenomen, waarbij voor ieder subgunningscriterium een afzonderlijke paginalimiet geldt. Kan de KB bevestigen dat Inschrijver binnen de beantwoording van een subgunningscriterium mag verwijzen naar informatie die bij een ander subgunningscriterium is opgenomen en dat de beoordelingscommissie deze informatie bij de beoordeling van het verwijzende subgunningscriterium betreft? We vragen dit om herhaling in tekst te voorkomen en de beschikbare A4 optimaal in te vullen. Of dient ieder subgunningscriterium volledig zelfstandig leesbaar te zijn en moet relevante informatie zo nodig binnen meerdere antwoorden worden herhaald?	Nee. Iedere open vraag wordt zelfstandig beoordeeld. Informatie die bij een andere open vraag is opgenomen, wordt niet bij de beoordeling van de betreffende vraag betrokken.
100.	Beschrijvend document – §5.1.1 Open vragen (omvang en opmaak)	Wij verzoeken de KB om op de paginalimiet van G1.1 aanvullend maximaal één pagina A4 met uitsluitend visualisaties toe te voegen, bijvoorbeeld een processchema en communicatiematrix. Deze pagina bevat dan geen zelfstandige inhoudelijke beantwoording, maar ondersteunt de binnen de pagina's beschreven werkwijze. Stemt de KB hiermee in en kan zij bevestigen dat deze aanvullende pagina volledig bij de beoordeling wordt betrokken?	Akkoord. Voor G1.1 mag Inschrijver één extra pagina A4 toevoegen die uitsluitend visualisaties bevat (zoals een processchema of communicatiematrix). Deze pagina wordt bij de beoordeling betrokken. Het maximale aantal pagina's voor de overige open vragen wordt niet gewijzigd.
101.	Beschrijvend document – §5.1.1 Open vragen (omvang en opmaak)	G1.1 bestaat uit vijf deelvragen, waarbij deelvraag 2 vijf afzonderlijke elementen bevat. Inschrijver moet onder meer ingaan op het team, de volledige aanpak, technieken en methoden, het gebruik van AI,	Nee, dat is niet akkoord. Zie het antwoord op vraag 100.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		communicatie, kwaliteitsborging, continuïteit en marktconforme urenbegrotingen. Voor deze beantwoording zijn maximaal drie pagina's beschikbaar. Vanwege de omvang en diversiteit van de gevraagde informatie verzoeken wij de KB de maximale omvang van G1.1 te verhogen van drie naar vier pagina's A4. Stemt de KB hiermee in?	
102.	Beschrijvend document – §5.1.1 Open vragen (omvang en opmaak)	G1.1 Uitvoering van pentesten bestaat uit 5 vragen waarvan 1 vraag 5 subvragen bevat. Bent u bereid om het aantal pagina's van 3 naar 5 te verhogen?	Nee, dat is niet akkoord. Zie het antwoord op vraag 100.
103.	Beschrijvend document – §5.1.1 Open vragen (omvang en opmaak)	Beschrijvend document, paragraaf 5.1.1, G.1.1. U geeft 3 pagina's A4 ter uitwerking. Tegelijkertijd vraagt u om 5 punten uit te werken, waarbij punt 2 (aanpak) ook een aantal subpunten kent. Dit geeft relatief weinig ruimte per uit te werken punt. Staat u er voor open om meer pagina's A4 ter beschikking te stellen, bijvoorbeeld 6 pagina's A4. Uw voordeel is dat de meer uitgebreide uitwerking u in staat stelt om de kwaliteit van de uitwerkingen van Gegadigden beter te beoordelen.	Nee, dat is niet akkoord. Zie het antwoord op vraag 100.
104.	Beschrijvend document – §5.1.1 Open vragen (omvang en opmaak)	De huidige maximale paginaomvang bedraagt drie pagina's voor G1.1, twee pagina's voor G1.2 en één pagina voor G1.3. Gezien het aantal deelvragen en de gevraagde onderbouwing verzoeken wij u deze maxima te verhogen naar respectievelijk vijf, vier en twee pagina's. Bent u hiertoe bereid, zodat inschrijvers voldoende ruimte hebben voor inhoudelijke diepgang, concrete onderbouwing en het aantonen van onderscheidend vermogen?	Nee, dat is niet akkoord. Zie het antwoord op vraag 100.
105.	Beschrijvend document – §5.1.1 Open vragen (omvang en opmaak)	In par. 5.1.1 is per open vraag (G1.1, G1.2, G1.3) een maximaal aantal pagina's A4 vastgesteld, waarbij het voorblad en de inhoudsopgave expliciet zijn uitgesloten van dit maximum. Namens de gezamenlijke Inschrijvers vragen wij of de KB kan bevestigen dat, naast het voorblad en de inhoudsopgave, ook een eventueel tussenblad tussen de	Ja, mits deze pagina's geen inhoudelijke beantwoording bevatten. Een eventuele aanbiedingsbrief wordt niet bij de beoordeling betrokken.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		beantwoording van de afzonderlijke open vragen en een begeleidende aanbestedingsbrief niet meetellen voor het maximale aantal pagina's?	
106.	Beschrijvend document – §5.1.1 Open vragen (omvang en opmaak)	Bij de beantwoording van de kwalitatieve gunningscriteria willen wij een voorpagina en colofon toevoegen. Kunt u bevestigen dat zowel de voorpagina als het colofon buiten de maximale paginaomvang vallen, mits deze uitsluitend administratieve gegevens bevatten en geen inhoudelijke beantwoording van de gunningscriteria?	Ja. Zie het antwoord op vraag 105.
107.	Beschrijvend document – §5.1.1 Open vragen (omvang en opmaak)	In de checklist bij Inschrijving (par. 7.4) worden geen CV's van het in te zetten team gevraagd. Namens de gezamenlijke Inschrijvers vragen wij of het is toegestaan om, ter onderbouwing van de in G1.1 gevraagde teambeschrijving, de CV's van de voorgestelde teamleden als aparte bijlage toe te voegen aan de Inschrijving, zonder dat deze CV's meetellen voor het maximale aantal pagina's van G1.1? Zo nee, graag een toelichting waarom dit niet mogelijk is.	Inschrijver mag cv's van het team ter informatie verstrekken. Deze worden niet bij de beoordeling van de Inschrijvingen betrokken en niet aan de beoordelingscommissie verstrekt.
108.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 Uitvoering van pentesten, beoordelingssystematiek Uitstekend/Goed/Voldoende Kan Opdrachtgever de nadere beoordelingsaspecten van G1.1 vooraf publiceren, zodat alle Inschrijvers hun beantwoording op dezelfde prioriteiten en verwachtingen kunnen richten?	Zie het antwoord op vraag 96.
109.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 Uitvoering van pentesten, beoordelingssystematiek Uitstekend/Goed/Voldoende Kan Opdrachtgever verduidelijken hoe een algemene procesbeschrijving wordt onderscheiden van een operationeel geborgd en controleerbaar uitvoeringsmodel?	Zie het antwoord op vraag 96.
110.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 Uitvoering van pentesten, beoordelingssystematiek Uitstekend/Goed/Voldoende Kan Opdrachtgever verduidelijken hoe de haalbaarheid van de aangeboden maatregelen binnen de aangeboden prijs, personeelsmix en beschikbare capaciteit wordt beoordeeld?	Alle maatregelen die Inschrijver aanbiedt, dienen te zijn opgenomen in de aangeboden prijsstelling (zie paragraaf 5.1). Zie verder het antwoord op vraag 96.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
111.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 Uitvoering van pentesten, beoordelingssystematiek Uitstekend/Goed/Voldoende Kan Opdrachtgever verduidelijken hoe de concreetheid, meetbaarheid, aantoonbaarheid en verifieerbaarheid van aangeboden maatregelen binnen G1.1 worden beoordeeld?	Zie het antwoord op vraag 96.
112.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 Uitvoering van pentesten, beoordelingssystematiek Uitstekend/Goed/Voldoende Kan Opdrachtgever verduidelijken welke aangeboden maatregelen binnen G1.1 als minimumniveau worden beschouwd en welke maatregelen als aantoonbare meerwaarde worden gewaardeerd?	Zie het antwoord op vraag 96.
113.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 Uitvoering van pentesten, beoordelingssystematiek Uitstekend/Goed/Voldoende Kan Opdrachtgever verduidelijken welke concrete, criteriumspecifieke kenmerken binnen G1.1 leiden tot de beoordelingen “Voldoende”, “Goed” en “Uitstekend”?	Zie het antwoord op vraag 96.
114.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 Uitvoering van pentesten, beoordelingssystematiek Uitstekend/Goed/Voldoende Kan Opdrachtgever aangeven of het ontbreken of onvoldoende beantwoorden van één deelvraag de maximaal te behalen score op G1.1 begrenst?	Er is sprake van een integrale beoordeling van de open vraag. Het ontbreken of onvoldoende beantwoorden van een deelvraag is wel van invloed op de score (zie de scoretabel).
115.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 Uitvoering van pentesten, beoordelingssystematiek Uitstekend/Goed/Voldoende G1.1 omvat verschillende inhoudelijke onderwerpen, waaronder teamsamenstelling, ervaring, inventarisatie, testaanpak, methoden, AI-gebruik, communicatie, nauwkeurigheid, betrouwbaarheid, continuïteit en marktconforme urenbegrotingen. Voor de beantwoording van al deze onderwerpen geldt gezamenlijk een maximum van drie pagina’s. Kan Opdrachtgever inzichtelijk maken	Er wordt geen afzonderlijke weging toegepast op de deelvragen of onderwerpen. Zie het antwoord op vraag 114.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		welk relatief belang aan de afzonderlijke deelvragen en onderwerpen van G1.1 wordt toegekend?	
116.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 Uitvoering van pentesten, E26 Betrokkenheid Senior Pentesters, E27 Kwalificaties Pentesters Kan Opdrachtgever bepalen dat Inschrijvers in G1.1 de beoogde personeelsmix beschrijven, inclusief de rol van de senior, de rol van overige pentesters, de rol van de reviewer, de verantwoordelijkheidsverdeling en de indicatieve verhouding tussen technische uitvoering, senior review en kwaliteitscontrole?	Nee. Het is aan Inschrijver om te bepalen op welke wijze hij het team omschrijft (deelvraag 1). Zie ook het antwoord op vraag 96.
117.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 Uitvoering van pentesten, G1.2 Rapportering, E32 Activiteiten, E33 Bespreken pentesten, E35 Vierogen-principe, E43 Inhoud rapportage De Aanbestedingsstukken bevatten eisen aan afzonderlijke uitvoeringsactiviteiten en onderdelen van de rapportage. Om te waarborgen dat alle Inschrijvers dezelfde minimale prestatie begroten en dat uitvoering op het aangeboden kwaliteitsniveau controleerbaar is, is Opdrachtgever bereid per Nadere Opdracht een minimale, toetsbare uitvoerings- en opleverset vast te stellen?	Nee. De minimale eisen aan de uitvoering en rapportage zijn opgenomen in het Programma van Eisen (onder andere E32, E33, E35 en E43). De verdere invulling wordt per Nadere Opdracht vastgelegd in de offerte (E20).
118.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 Uitvoering van pentesten, G1.2 Rapportering, E32 Activiteiten, E33 Bespreken pentesten, E35 Vierogen-principe, E43 Inhoud rapportage Kan Opdrachtgever bevestigen dat een Inschrijver geen hogere kwaliteitsscore ontvangt voor maatregelen die niet aantoonbaar in de aangeboden prijs, personeelsmix en uitvoeringscapaciteit zijn geborgd?	Zie het antwoord op vraag 110.
119.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 Uitvoering van pentesten, G1.2 Rapportering, E32 Activiteiten, E33 Bespreken pentesten, E35 Vierogen-principe, E43 Inhoud rapportage	Zie het antwoord op vraag 96.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		Kan Opdrachtgever bevestigen dat de aantoonbare volledigheid, controleerbaarheid en reproduceerbaarheid van de aangeboden uitvoering worden betrokken bij de beoordeling van G1.1?	
120.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 Uitvoering van pentesten, G1.2 Rapportering, E32 Activiteiten, E33 Bespreken pentesten, E35 Vierogen-principe, E43 Inhoud rapportage Kan Opdrachtgever bevestigen dat Inschrijvers in G1.1 moeten toelichten hoe zij aantoonbaar borgen dat de minimale uitvoerings- en opleverset bij iedere pentest wordt geleverd?	Zie het antwoord op vraag 96.
121.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 Uitvoering van pentesten, G1.2 Rapportering, E32 Activiteiten, E33 Bespreken pentesten, E35 Vierogen-principe, E43 Inhoud rapportage Kan Opdrachtgever bevestigen dat iedere urenbegroting voldoende ruimte moet bieden om de minimale uitvoerings- en opleverset volledig uit te voeren?	Ja, dat wordt bevestigd. De urenbegroting biedt ruimte voor alle activiteiten die noodzakelijk zijn voor de uitvoering van de pentest; de vaste aanneemsom omvat al deze activiteiten (E32 en E55).
122.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 Uitvoering van pentesten, G1.2 Rapportering, E32 Activiteiten, E33 Bespreken pentesten, E35 Vierogen-principe, E43 Inhoud rapportage Kan Opdrachtgever bevestigen dat de minimale uitvoerings- en opleverset, voor zover passend bij de betreffende pentest, bestaat uit een overzicht van niet-geteste onderdelen en resterende onzekerheden, bespreking en toelichting van de resultaten en, indien van toepassing, een afzonderlijk hertestresultaat?	Zie het antwoord op vraag 117.
123.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 Uitvoering van pentesten, G1.2 Rapportering, E32 Activiteiten, E33 Bespreken pentesten, E35 Vierogen-principe, E43 Inhoud rapportage Kan Opdrachtgever bevestigen dat de minimale uitvoerings- en opleverset, voor zover passend bij de betreffende pentest, bestaat uit technische validatie van kritieke en hoge bevindingen, vastlegging dat	Zie het antwoord op vraag 117.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		de vierogencontrole is uitgevoerd en de volledige rapportage volgens E43?	
124.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 Uitvoering van pentesten, G1.2 Rapportering, E32 Activiteiten, E33 Bespreken pentesten, E35 Vierogen-principe, E43 Inhoud rapportage Kan Opdrachtgever bevestigen dat de minimale uitvoerings- en opleverset, voor zover passend bij de betreffende pentest, bestaat uit de vastlegging van beperkingen, uitsluitingen en aannames, een overzicht van de feitelijk ingezette rollen en verantwoordelijkheden en aantoonbare betrokkenheid van de senior functionaris?	Zie het antwoord op vraag 117.
125.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 Uitvoering van pentesten, G1.2 Rapportering, E32 Activiteiten, E33 Bespreken pentesten, E35 Vierogen-principe, E43 Inhoud rapportage Kan Opdrachtgever bevestigen dat de minimale uitvoerings- en opleverset, voor zover passend bij de betreffende pentest, ten minste bestaat uit een schriftelijk vastgelegde scope, testdoelstelling en set uitgangspunten, een testplan of vastgelegde testaanpak, een overzicht van uitgevoerde testactiviteiten en een overzicht van toegepaste methoden en toetsingskaders?	Zie het antwoord op vraag 117.
126.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	In deelvraag 4 van G1.1 vraagt de KB welke maatregelen Inschrijver neemt ter borging van “de continuïteit van de algehele dienstverlening”. Doelt de KB hiermee op de continuïteit tijdens de uitvoering van een afzonderlijke pentest, op de beschikbaarheid en vervangbaarheid van medewerkers gedurende de gehele looptijd van de Raamovereenkomst of op de bedrijfscontinuïteit van de organisatie van Opdrachtnemer? Wij verzoeken de KB vriendelijk de bedoelde reikwijdte van deze deelvraag te verduidelijken.	De KB doelt op de continuïteit van de dienstverlening gedurende de gehele looptijd van de Raamovereenkomst, waaronder de beschikbaarheid van voldoende gekwalificeerde capaciteit, de vervangbaarheid van medewerkers en de borging van kennis. Het is aan Inschrijver om te bepalen welke maatregelen hij daarbij beschrijft.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
127.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	Welke aspecten van continuïteit weegt de KB zwaar mee bij beoordeling van G1.1, bijvoorbeeld beschikbaarheid van capaciteit, vervangbaarheid van sleutelpersonen, kennisborging of opschaalbaarheid?	Zie het antwoord op vraag 126. De KB kent geen afzonderlijke weging toe aan deze aspecten.
128.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 deelvraag 4 Continuïteit, E6 Capaciteit en expertise G1.1 vraagt welke maatregelen Inschrijver neemt om de continuïteit van de algehele dienstverlening te borgen. Kan Opdrachtgever verduidelijken welke concrete en meetbare continuïteitsaspecten bij dit onderdeel worden beoordeeld?	Zie het antwoord op vraag 126.
129.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 deelvraag 4 Continuïteit, E6 Capaciteit en expertise Kan Opdrachtgever bevestigen dat een algemene verklaring over beschikbare capaciteit niet gelijk wordt gewaardeerd aan een concreet continuïteitsmodel met rollen, vervangingscapaciteit, overdrachtsmaatregelen, termijnen en aantoonbare borging?	Zie het antwoord op vraag 96.
130.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 deelvraag 4 Continuïteit, E6 Capaciteit en expertise Kan Opdrachtgever verduidelijken welke kenmerken van continuïteitsborging leiden tot de beoordelingen “Voldoende”, “Goed” en “Uitstekend”?	Zie het antwoord op vraag 96.
131.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 deelvraag 4 Continuïteit, E6 Capaciteit en expertise Kan Opdrachtgever aangeven welke bewijsvoering of prestatie-indicatoren mogen worden gebruikt om de aangeboden continuïteitsmaatregelen te onderbouwen?	Zie het antwoord op vraag 126. Inschrijver is vrij in de wijze van onderbouwing.
132.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 deelvraag 4 Continuïteit, E6 Capaciteit en expertise Kan Opdrachtgever aangeven welke continuïteitsmaatregelen als minimumniveau worden beschouwd en welke maatregelen aantoonbare meerwaarde opleveren?	Zie het antwoord op vraag 96.
133.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 deelvraag 4 Continuïteit, E6 Capaciteit en expertise Kan Opdrachtgever bevestigen dat bij de beoordeling van continuïteit wordt gekeken naar de continuïteit van beveiligde opslag,	Zie het antwoord op vraag 126.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		communicatie en rapportage, de herstelvoorzieningen voor gebruikte systemen en tooling en de escalatie, communicatie en besluitvorming bij een continuïteitsincident?	
134.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 deelvraag 4 Continuïteit, E6 Capaciteit en expertise Kan Opdrachtgever bevestigen dat bij de beoordeling van continuïteit wordt gekeken naar de borging bij ziekte, uitval en vertrek van sleutelfunctionarissen, de beschikbare capaciteit tijdens piekperioden en de beschikbaarheid van senior review en vierogencontrole?	Zie het antwoord op vraag 126.
135.	Beschrijvend document – §5.1.1 G1.1 Uitvoering van pentesten	G1.1 deelvraag 4 Continuïteit, E6 Capaciteit en expertise Kan Opdrachtgever bevestigen dat bij de beoordeling van continuïteit wordt gekeken naar de beschikbaarheid van gekwalificeerde vervanging, de maximale termijn waarbinnen vervanging beschikbaar is, de overdraagbaarheid en actualiteit van opdrachtinformatie en de spreiding van technische en specialistische kennis?	Zie het antwoord op vraag 126.
136.	Beschrijvend document – §5.1.1 G1.2 Rapportering	Welke elementen maken een rapportage volgens de KB daadwerkelijk onderscheidend ten opzichte van de minimumeisen uit het Programma van Eisen?	Zie het antwoord op vraag 96.
137.	Beschrijvend document – §5.1.1 G1.2 Rapportering	Bij G1.2, deelvraag 1, moet Inschrijver motiveren waarom de rapportages tegemoetkomen aan de behoeften van de KB. In paragraaf 2.2 noemt de KB als doelstelling dat rapportages goed gestructureerd moeten zijn en het gewenste inzicht moeten bieden om verbeteringen door te voeren. Kan de KB deze behoefte nader concretiseren? Aan welke gebruikersgroepen moeten de rapportages primair ondersteuning bieden, welk onderscheid verwacht de KB tussen technische en bestuurlijke informatie en welke informatie is minimaal nodig om kwetsbaarheden gericht te kunnen prioriteren en opvolgen?	De rapportages moeten zowel het management (onder andere de CISO) als de technisch verantwoordelijken (beheerders en ontwikkelaars) van de KB ondersteunen. De KB verwacht een duidelijk onderscheid tussen bestuurlijke informatie (managementsamenvatting) en technische informatie. De minimaal benodigde informatie is opgenomen in eis E43.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
138.	Beschrijvend document – §5.1.1 G1.2 Rapportering	Bij G1.2, deelvraag 2, vraagt de KB welke mogelijkheden Inschrijver biedt voor het verwerken van wensen van de KB met betrekking tot de opbouw van de rapportage. Kan de KB voorbeelden geven van de wensen die zij hierbij verwacht? Betreft dit wensen die voorafgaand aan iedere Nadere Opdracht kunnen verschillen?	Het is de verwachting van de KB dat het in de praktijk om het doorvoeren van minimale aanpassingen van een standaard template zal gaan, bijvoorbeeld meer of minder details. Verdere concrete voorbeelden kan de KB op dit moment niet benoemen.
139.	Beschrijvend document – §5.1.1 G1.2 Rapportering	E34 Specifiek advies, E37 Ernstige kwetsbaarheden, E43 Rapportage, G1.2 Rapportering Opdrachtgever verlangt dat adviezen specifiek zijn gericht op de situatie van Opdrachtgever en dat rapportages per kwetsbaarheid onder meer een impactanalyse, risicobeschrijving, prioritering en hersteladvies bevatten. Kan Opdrachtgever verduidelijken hoe de diepgang, contextgerichtheid en praktische bruikbaarheid hiervan binnen G1.2 worden beoordeeld?	Zie het antwoord op vraag 96.
140.	Beschrijvend document – §5.1.1 G1.2 Rapportering	E34 Specifiek advies, E37 Ernstige kwetsbaarheden, E43 Rapportage, G1.2 Rapportering Kan Opdrachtgever verduidelijken welke kenmerken van de contextuele risico- en impactduiding en hersteladviezen leiden tot de beoordelingen “Voldoende”, “Goed” en “Uitstekend”?	Zie het antwoord op vraag 96.
141.	Beschrijvend document – §5.1.1 G1.2 Rapportering	E34 Specifiek advies, E37 Ernstige kwetsbaarheden, E43 Rapportage, G1.2 Rapportering Kan Opdrachtgever bevestigen dat de mate waarin de voorbeeldrapportage contextuele, geprioriteerde en praktisch uitvoerbare advisering aantoonbaar bevat, expliciet wordt betrokken bij de beoordeling van G1.2?	Zie het antwoord op vraag 96.
142.	Beschrijvend document – §5.1.1 G1.2 Rapportering	E34 Specifiek advies, E37 Ernstige kwetsbaarheden, E43 Rapportage, G1.2 Rapportering Kan Opdrachtgever bevestigen dat een hoogwaardige rapportage, voor zover relevant, inzicht geeft in relevante afhankelijkheden, mogelijke neveneffecten en de wijze waarop herstel kan worden gevalideerd?	Zie het antwoord op vraag 96.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
143.	Beschrijvend document – §5.1.1 G1.2 Rapportering	E34 Specifiek advies, E37 Ernstige kwetsbaarheden, E43 Rapportage, G1.2 Rapportering Kan Opdrachtgever bevestigen dat een hoogwaardige rapportage, voor zover relevant, onderscheid maakt tussen een direct toepasbare risicobeperkende maatregel, een structurele oplossing en een compenserende maatregel wanneer direct herstel niet mogelijk is?	Zie het antwoord op vraag 96.
144.	Beschrijvend document – §5.1.1 G1.2 Rapportering	E34 Specifiek advies, E37 Ernstige kwetsbaarheden, E43 Rapportage, G1.2 Rapportering Kan Opdrachtgever bevestigen dat een hoogwaardige rapportage, voor zover relevant, afzonderlijk inzicht geeft in de mogelijke impact op de dienstverlening en doelstellingen van Opdrachtgever en de herstellprioriteit?	Zie het antwoord op vraag 96.
145.	Beschrijvend document – §5.1.1 G1.2 Rapportering	E34 Specifiek advies, E37 Ernstige kwetsbaarheden, E43 Rapportage, G1.2 Rapportering Kan Opdrachtgever bevestigen dat een hoogwaardige rapportage, voor zover relevant, afzonderlijk inzicht geeft in de mogelijke impact op de dienstverlening en doelstellingen van Opdrachtgever en de herstellprioriteit?	Zie het antwoord op vraag 96.
146.	Beschrijvend document – §5.1.1 G1.2 Rapportering	E34 Specifiek advies, E37 Ernstige kwetsbaarheden, E43 Rapportage, G1.2 Rapportering Kan Opdrachtgever bevestigen dat een hoogwaardige rapportage, voor zover relevant, afzonderlijk inzicht geeft in de technische ernst, praktische exploitatiebaarheid, blootstelling van het betreffende systeem, aanwezige beheersmaatregelen en gevoeligheid van betrokken gegevens en functionaliteit?	Zie het antwoord op vraag 96.
147.	Beschrijvend document – §5.1.1 G1.2 Voorbeeldrapportage	Bij G1.2 staat dat Inschrijver een voorbeeldrapportage als bijlage “mag” toevoegen. In de checklist bij Inschrijving in paragraaf 7.4 staat daarentegen “Antwoorden open vragen (in één bestand) + voorbeeld rapportage”. Bovendien staat boven deze checklist dat het ontbreken	Zoals aangegeven bij open vraag G1.2 mag de voorbeeldrapportage ter ondersteuning worden aangeleverd. De KB adviseert Inschrijver dit te doen,

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		van één of meerdere documenten ertoe leidt dat de Inschrijving terzijde wordt gelegd. Bevestigt de KB dat de voorbeeldrapportage facultatief is en dat het niet toevoegen ervan niet leidt tot ongeldigheid of terzijdelegging van de Inschrijving? Wij verzoeken de KB de checklist in paragraaf 7.4 hierop aan te passen.	aangezien dit document wordt betrokken bij de beoordeling van open vraag G1.2. Het niet aanleveren van een voorbeeldrapportage leidt niet tot ongeldigheid of terzijdelegging van de Inschrijving, maar kan wel van invloed zijn op de score voor open vraag G1.2. De checklist in paragraaf 7.4 van het Beschrijvend document dient in die zin te worden gelezen.
148.	Beschrijvend document – §5.1.1 G1.2 Voorbeeldrapportage	Bij G1.2 staat dat Inschrijver ter ondersteuning van de beantwoording een voorbeeldrapportage als bijlage mag toevoegen en dat deze niet meetelt voor het maximale aantal A4. 1. Kan de KB toelichten hoe de voorbeeldrapportage bij de beoordeling wordt betrokken? 2. Wordt deze door de beoordelingscommissie volledig gelezen en inhoudelijk meegewogen? 3. Mag Inschrijver in de beantwoording van G1.2 expliciet verwijzen naar onderdelen van de voorbeeldrapportage? 4. Wordt informatie die uitsluitend in de voorbeeldrapportage staat ook bij de beoordeling betrokken of moet alle te beoordelen informatie binnen de twee pagina's van G1.2 zijn opgenomen? Graag uw verduidelijking op alle vier de elementen. Dank u!	1. De voorbeeldrapportage dient ter ondersteuning van de beantwoording van G1.2 en wordt bij de integrale beoordeling van G1.2 betrokken. De voorbeeldrapportage dient uitsluitend als voorbeeld van een rapportage van Inschrijver (een bestaande, geanonimiseerde rapportage of een fictief voorbeeld; zie het antwoord op vraag 158) en mag geen antwoorden bevatten op de deelvragen van de KB. 2. Ja. 3. Ja. 4. De beoordeling vindt plaats op basis van de beantwoording binnen de twee pagina's, met de voorbeeldrapportage daarbij ter ondersteuning. De voorbeeldrapportage mag dus geen antwoorden bevatten op deelvragen 1 t/m 3.
149.	Beschrijvend document – §5.1.1 G1.2 Voorbeeldrapportage	Uit het woord “mag” bij G1.2 leiden wij af dat het toevoegen van een voorbeeldrapportage facultatief is. Bevestigt de KB dat het niet indienen van een voorbeeldrapportage op zichzelf geen negatieve invloed heeft op de geldigheid of beoordeling	Zie het antwoord op vraag 147.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		van de Inschrijving, mits de beantwoording van G1.2 voldoende inzicht biedt in de gevraagde rapportering?	
150.	Beschrijvend document – §5.1.1 G1.2 Voorbeeldrapportage	G1.2 Rapportering Bij G1.2 mag een voorbeeldrapportage als bijlage worden toegevoegd. Kan Opdrachtgever verduidelijken op welke wijze en op welke onderdelen deze voorbeeldrapportage in de beoordeling van G1.2 wordt betrokken?	Zie het antwoord op vraag 148.
151.	Beschrijvend document – §5.1.1 G1.2 Voorbeeldrapportage	Beschrijvend document, paragraaf 5.1.1, G.1.2. U benoemt "Inschrijver mag ter ondersteuning van de beantwoording van deze vragen een voorbeeldrapportage als bijlage bijvoegen". De vrijblijvendheid "mag" doet vermoeden dat de voorbeeldrapportage niet meetelt in de beoordeling van dit subgunningscriterium. Is deze aanname correct?	Nee, die aanname is niet correct. Zie het antwoord op vraag 148.
152.	Beschrijvend document – §5.1.1 G1.2 Voorbeeldrapportage	G1.2 Rapportering Kan Opdrachtgever bevestigen dat aantoonbaar in de voorbeeldrapportage zichtbare kwaliteit zwaarder wordt gewaardeerd dan een algemene beschrijving die niet zichtbaar door het voorbeeld wordt ondersteund?	Zie het antwoord op vraag 148.
153.	Beschrijvend document – §5.1.1 G1.2 Voorbeeldrapportage	G1.2 Rapportering Kan Opdrachtgever bevestigen dat de voorbeeldrapportage wordt gebruikt om de expliciete claims uit de beantwoording van G1.2 te verifiëren ten aanzien van de concreetheid en uitvoerbaarheid van hersteladviezen, de opvolgbaarheid en wijze van hervalidatie en de interne consistentie en aantoonbare kwaliteitscontrole?	Zie het antwoord op vraag 148.
154.	Beschrijvend document – §5.1.1 G1.2 Voorbeeldrapportage	G1.2 Rapportering Kan Opdrachtgever bevestigen dat de voorbeeldrapportage wordt gebruikt om de expliciete claims uit de beantwoording van G1.2 te verifiëren ten aanzien van de reproduceerbaarheid van bevindingen,	Zie het antwoord op vraag 148.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		het onderscheid tussen technische ernst en contextuele impact en de prioritering van bevindingen?	
155.	Beschrijvend document – §5.1.1 G1.2 Voorbeeldrapportage	G1.2 Rapportering Kan Opdrachtgever bevestigen dat de voorbeeldrapportage wordt gebruikt om de expliciete claims uit de beantwoording van G1.2 te verifiëren ten aanzien van de helderheid voor technische en niet-technische doelgroepen, de volledigheid van de scope- en methodologiebeschrijving en de kwaliteit en navolgbaarheid van technisch bewijs?	Zie het antwoord op vraag 148.
156.	Beschrijvend document – §5.1.1 G1.2 Voorbeeldrapportage	G1.2 Rapportering Kan Opdrachtgever aangeven hoe verschillen in onderwerp, complexiteit, omvang en ernst van de door Inschrijvers gekozen voorbeeldrapportages bij de beoordeling worden genormaliseerd?	De voorbeeldrapportages worden niet genormaliseerd. Zie het antwoord op vraag 148.
157.	Beschrijvend document – §5.1.1 G1.2 Voorbeeldrapportage	Mag de voorbeeldrapportage worden geanonimiseerd, inclusief systeemnamen, IP-adressen, screenshots, broncodefragmenten en contactpersonen? Geldt voor de voorbeeldrapportage een maximale omvang, en dient deze in het Nederlands te zijn opgesteld?	Ja, de voorbeeldrapportage mag (volledig) geanonimiseerd worden. Er geldt geen maximale omvang. De voorbeeldrapportage dient in het Nederlands te zijn opgesteld.
158.	Beschrijvend document – §5.1.1 G1.2 Voorbeeldrapportage	Mag de voorbeeldrapportage een geanonimiseerde bestaande rapportage zijn, of dient het een fictief voorbeeld te betreffen? Gelden voor de voorbeeldrapportage een maximaal aantal pagina's of opmaakeisen?	Beide zijn toegestaan. Er geldt geen maximaal aantal pagina's en er gelden geen opmaakeisen. Zie ook het antwoord op vraag 157.
159.	Beschrijvend document – §5.1.1 G1.2 Voorbeeldrapportage	Inschrijver neemt aan dat de voorbeeldrapportage kan afwijken van het gevraagde format volgen, indien alle onderwerpen aan bod komen, is dat juist?	Ja, dat is juist.
160.	Beschrijvend document – §5.1.1 G1.2 Voorbeeldrapportage	G1.2 Rapportering Om de kwaliteit en bruikbaarheid van rapportages op een gelijke en objectief vergelijkbare basis te beoordelen, is Opdrachtgever bereid	Nee, de KB kan dit niet verstrekken. Er is geen sprake van de beantwoording van een fictieve kwetsbaarheidsclusus.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		een korte, fictieve kwetsbaarheidscasus beschikbaar te stellen die iedere Inschrijver volgens dezelfde instructie uitwerkt?	
161.	Beschrijvend document – §5.1.1 G1.2 Voorbeeldrapportage	G1.2 Rapportering Indien Opdrachtgever geen uniforme kwetsbaarheidscasus wil opnemen, kan Opdrachtgever dan motiveren hoe de rapportagekwaliteit van verschillende Inschrijvers objectief wordt vergeleken wanneer iedere Inschrijver zelf het onderwerp, de complexiteit en de inhoud van zijn voorbeeldrapportage bepaalt?	Zie het antwoord op vraag 148.
162.	Beschrijvend document – §5.1.1 G1.2 Voorbeeldrapportage	G1.2 Rapportering Kan de uniforme uitwerking van de kwetsbaarheidscasus als vast onderdeel van G1.2 worden beoordeeld?	Zie het antwoord op vraag 160.
163.	Beschrijvend document – §5.1.1 G1.2 Voorbeeldrapportage	G1.2 Rapportering Kan Opdrachtgever voor de uniforme kwetsbaarheidscasus een vast format, een maximale omvang en expliciete beoordelingsaspecten vaststellen voor herstellprioriteit, een directe risicobeperkende maatregel, een structurele oplossing, een eventuele compenserende maatregel en de wijze van hervalidatie?	Zie het antwoord op vraag 160.
164.	Beschrijvend document – §5.1.1 G1.2 Voorbeeldrapportage	G1.2 Rapportering Kan Opdrachtgever voor de uniforme kwetsbaarheidscasus een vast format, een maximale omvang en expliciete beoordelingsaspecten vaststellen voor managementduiding, technische beschrijving, bewijs en reproductiestappen, technische ernst, praktische exploitatiebaarheid en contextuele impact?	Zie het antwoord op vraag 160.
165.	Beschrijvend document – §5.1.1 G1.3 Duurzaamheid	Bij G1.3 vermeldt de KB dat zij diverse maatregelen neemt om de impact van haar eigen bedrijfsvoering op het milieu te minimaliseren en dat de Opdrachtnemer moet bijdragen aan de ambities van de KB. Kan de KB aangeven welke concrete maatregelen en duurzaamheidsambities voor deze Opdracht relevant zijn? Kan zij daarbij tevens aangeven aan welke milieuthema's en onderdelen van	De KB hanteert geen specifiek kader en geeft geen voorkeur voor bepaalde thema's. Inschrijver kan alle maatregelen beschrijven die bijdragen aan het verduurzamen van de dienstverlening voor de KB, zowel op het gebied van milieu als sociaal ondernemerschap.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		sociaal ondernemerschap zij binnen G1.3 de meeste waarde hecht, zodat Inschrijvers hun maatregelen gericht op deze ambities kunnen laten aansluiten?	
166.	Beschrijvend document – §5.1.1 G1.3 Duurzaamheid	Bij G1.3 staat dat de maatregelen daadwerkelijk betrekking moeten hebben op de uitvoering van de Opdracht voor de KB. De uitvoering van pentesten en de daarvoor benodigde bedrijfsactiviteiten hoeven niet uitsluitend op een locatie van de KB plaats te vinden. Begrijpen wij correct dat ook duurzaamheidsmaatregelen die buiten de locaties van de KB worden uitgevoerd mogen worden beschreven, mits deze aantoonbaar, meetbaar en rechtstreeks zijn toe te rekenen aan de uitvoering van de Opdracht voor de KB? Zo nee, welke geografische of organisatorische afbakening hanteert de KB?	Ja, dat is correct.
167.	Beschrijvend document – §5.1.1 G1.3 Duurzaamheid	Bij G1.3 vermeldt de KB dat duurzaamheid betrekking heeft op zowel milieu als sociaal ondernemerschap en dat de maatregelen daadwerkelijk betrekking moeten hebben op de uitvoering van de Opdracht voor de KB. Staat de KB ervoor open dat bij de uitvoering van de Opdracht personen met een afstand tot de arbeidsmarkt, starters of andere sociaal-maatschappelijke doelgroepen worden ingezet, mits zij voldoen aan alle gestelde eisen op het gebied van deskundigheid, screening, vertrouwelijkheid en informatiebeveiliging? Kan de KB tevens aangeven of dergelijke inzet op locatie van de KB mogelijk is?	Ja, mits deze personen voldoen aan alle gestelde eisen (waaronder E26 tot en met E28). Inzet op locatie van de KB is daarbij mogelijk.
168.	Beschrijvend document – §5.1.1 Nakoming Inschrijving	G1.1 Uitvoering van pentesten, G1.2 Rapportering, E3 Correctheid gegevens, E6 Capaciteit en expertise, E26 Betrokkenheid Senior Pentesters, E27 Kwalificaties Pentesters Kan Opdrachtgever bevestigen dat de personele, methodologische en kwaliteitskenmerken die binnen G1.1 en G1.2 worden aangeboden gedurende de uitvoering aantoonbaar moeten worden toegepast en nagekomen?	Ja. De Inschrijving maakt onderdeel uit van de Raamovereenkomst (artikel 1.3 van de Raamovereenkomst). Opdrachtnemer is gehouden de aangeboden werkwijze en maatregelen gedurende de looptijd toe te passen. De KB kan de naleving toetsen via de overlegmomenten (E16), de managementinformatie (E17) en een audit (E50).

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
169.	Beschrijvend document – §5.1.1 Nakoming Inschrijving	G1.1 Uitvoering van pentesten, G1.2 Rapportering, E3 Correctheid gegevens, E6 Capaciteit en expertise, E26 Betrokkenheid Senior Pentesters, E27 Kwalificaties Pentesters Kan Opdrachtgever aangeven hoe de naleving van de bij de gunning gewaardeerde personele, methodologische en kwaliteitskenmerken gedurende de looptijd wordt gemonitord?	Zie het antwoord op vraag 168.
170.	Beschrijvend document – §5.1.1 Nakoming Inschrijving	G1.1 Uitvoering van pentesten, G1.2 Rapportering, E3 Correctheid gegevens, E6 Capaciteit en expertise, E26 Betrokkenheid Senior Pentesters, E27 Kwalificaties Pentesters Kan Opdrachtgever bevestigen dat gedurende de uitvoering met passende bewijsstukken moet kunnen worden aangetoond dat de aangeboden kwaliteitsmaatregelen daadwerkelijk zijn toegepast?	Ja. Zie het antwoord op vraag 168.
171.	Beschrijvend document – §5.1.1 Nakoming Inschrijving	G1.1 Uitvoering van pentesten, G1.2 Rapportering, E3 Correctheid gegevens, E6 Capaciteit en expertise, E26 Betrokkenheid Senior Pentesters, E27 Kwalificaties Pentesters Kan Opdrachtgever bevestigen dat een wijziging van personeelsmix, senioriteitsniveau, testdiepgang, reviewmodel of kwaliteitsborging niet mag leiden tot een lager kwaliteitsniveau dan waarop de Inschrijving is beoordeeld?	Ja. Zie het antwoord op vraag 168.
172.	Beschrijvend document – §5.1.1 Nakoming Inschrijving	G1.1 Uitvoering van pentesten, G1.2 Rapportering, E3 Correctheid gegevens, E6 Capaciteit en expertise, E26 Betrokkenheid Senior Pentesters, E27 Kwalificaties Pentesters Kan Opdrachtgever bevestigen dat vervanging uitsluitend plaatsvindt door aantoonbaar gelijkwaardige of betere capaciteit en dat gelijkwaardigheid wordt beoordeeld op relevante ervaring, certificeringen, technische specialisatie, senioriteitsniveau en verantwoordelijkheid binnen het kwaliteitsproces?	Ja. Zie het antwoord op vraag 168 en artikel 22.4 ARBIT-2022.
173.	Beschrijvend document – §5.1.1 Nakoming Inschrijving	G1.1 Uitvoering van pentesten, G1.2 Rapportering, E3 Correctheid gegevens, E6 Capaciteit en expertise, E26 Betrokkenheid Senior Pentesters, E27 Kwalificaties Pentesters	Ja. Zie het antwoord op vraag 168.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		Kan Opdrachtgever bevestigen dat de aangeboden test-, validatie-, review- en rapportageprocessen aantoonbaar worden uitgevoerd?	
174.	Beschrijvend document – §5.1.1 Nakoming Inschrijving	G1.1 Uitvoering van pentesten, G1.2 Rapportering, E3 Correctheid gegevens, E6 Capaciteit en expertise, E26 Betrokkenheid Senior Pentesters, E27 Kwalificaties Pentesters Kan Opdrachtgever bevestigen dat de aangeboden sleutelrollen daadwerkelijk bij de relevante werkzaamheden worden betrokken en dat de aangeboden personeelsmix en verantwoordelijkheidsverdeling tijdens de uitvoering worden toegepast?	Ja. Zie het antwoord op vraag 168.
175.	Beschrijvend document – §5.1.1 Nakoming Inschrijving	Kwaliteitsantwoorden als contractuele verplichtingen Kan Opdrachtgever bevestigen dat de antwoorden op de kwalitatieve gunningscriteria uitsluitend bindend zijn voor zover daarin concreet aangeboden Diensten en resultaten zijn beschreven en dat toelichtingen, voorbeelden, ambities, verwachtingen en beschrijvingen van gebruikelijke werkwijzen niet als afzonderlijke garanties of resultaatsverplichtingen worden aangemerkt?	Nee, dat wordt niet bevestigd. De Inschrijving maakt integraal onderdeel uit van de Raamovereenkomst. Zie het antwoord op vraag 168.
176.	Beschrijvend document – §5.1.2 Gunningscriterium Prijs	Het Beschrijvend Document spreekt over beoordeling van een totaalprijs, terwijl het Prijzenblad alleen een mandagtarief bevat. Kan de KB bevestigen dat het ingevulde mandagtarief rechtstreeks als Xlev (zie paragraaf 5.1.2) in de prijsformule wordt gebruikt?	Ja, dat wordt bevestigd.
177.	Beschrijvend document – §5.1.2 Gunningscriterium Prijs	Kan de KB toelichten waarom ervoor is gekozen om uitsluitend een dagtarief te beoordelen, terwijl de uiteindelijke kosten van een Nadere Opdracht worden bepaald door zowel het dagtarief als het geoffreerde aantal mandagen? Hoe waarborgt de KB dat de gekozen beoordelingsmethodiek niet leidt tot strategische onderbieding op het dagtarief en compensatie via hogere inspanningsinschattingen bij Nadere Opdrachten?	De inhoud en omvang van de Nadere Opdrachten zijn vooraf niet bekend. Het tarief per mandag is daarom het objectief vergelijkbare prijsonderdeel. De KB borgt realistische urenbegrotingen via eis E21 (marktconformiteit) en G1.1 deelvraag 5. De prijsbeoordeling wordt niet gewijzigd.
178.	Beschrijvend document – §5.1.2 Gunningscriterium Prijs	Kan KB overwegen de prijsbeoordeling te baseren op één of meerdere representatieve pentestcasussen, waarbij de totale inschrijfprijs	Nee, dat is niet akkoord. Zie het antwoord op vraag 177.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		wordt bepaald door de geoffreerde inspanning vermenigvuldigd met het dagtarief? Hierdoor wordt niet uitsluitend het dagtarief beoordeeld, maar de verwachte totale kosten van de dienstverlening.	
179.	Beschrijvend document – §5.1.2 Gunningscriterium Prijs	§5.1.2 Gunningscriterium Prijs, Bijlage 5 Prijzenblad De prijs voor een concrete pentest wordt na inventarisatie bepaald op basis van het aangeboden mandagtarief en de voor de Nadere Opdracht begrote inzet. Hierdoor vergelijkt het huidige prijscriterium primair tarieven en niet noodzakelijk de totale prijs en inhoud van de prestatie die Inschrijvers voor een vergelijkbare pentest aanbieden. Is Opdrachtgever bereid het Prijzenblad uit te breiden met één of meer representatieve referentieopdrachten waarvoor iedere Inschrijver op basis van een identieke scope, complexiteit, testmethodiek, uitgangspunten en deliverables een totaalprijs opgeeft?	Nee, dat is niet akkoord. Zie het antwoord op vraag 177.
180.	Beschrijvend document – §5.1.2 Gunningscriterium Prijs	§5.1.1 G1.1 Uitvoering van pentesten Indien Opdrachtgever het Prijzenblad niet wil aanpassen, is Opdrachtgever dan bereid een representatieve casus op te nemen bij G1.1, waarbij Inschrijvers op basis van dezelfde uitgangspunten de noodzakelijke activiteiten, personeelsmix, kwaliteitscontroles en inzet beschrijven?	Nee, dat is niet akkoord. Zie het antwoord op vraag 177.
181.	Beschrijvend document – §5.1.2 Gunningscriterium Prijs	§5.1.2 Gunningscriterium Prijs, Bijlage 5 Prijzenblad Kan Opdrachtgever de totale vaste aanneemsom van de representatieve referentieopdracht of referentieopdrachten geheel of gedeeltelijk betrekken bij het Gunningscriterium Prijs, zodat Inschrijvingen worden vergeleken op basis van een gelijkwaardige totale prestatie en niet uitsluitend op basis van het aangeboden mandagtarief?	Nee, dat is niet akkoord. Zie het antwoord op vraag 177.
182.	Beschrijvend document – §5.1.2 Gunningscriterium Prijs	§5.1.2 Gunningscriterium Prijs, Bijlage 5 Prijzenblad Is Opdrachtgever bereid Inschrijvers voor de representatieve referentieopdracht afzonderlijk inzicht te laten geven in de inzet voor inventarisatie en voorbereiding, technische testuitvoering, analyse en	Nee, dat is niet akkoord. Zie het antwoord op vraag 177.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		validatie, risico- en impactbepaling, kwaliteits- en vierogencontrole, rapportage en bespreking en een eventuele hertest?	
183.	Beschrijvend document – §5.1.2 Gunningscriterium Prijs	§5.1.2 Gunningscriterium Prijs, Bijlage 5 Prijzenblad Is Opdrachtgever bereid Inschrijvers voor de representatieve referentieopdracht inzicht te laten geven in de voorgestelde personeelsmix en de inzet per rol en senioriteitsniveau?	Nee, dat is niet akkoord. Zie het antwoord op vraag 177.
184.	Beschrijvend document – §5.1.2 Gunningscriterium Prijs	Op basis van welke fictieve volumes of weging wordt de totaalprijs berekend? Kan de KB een indicatie geven van het verwachte aantal pentesten per jaar, de soorten (bijvoorbeeld webapplicatie, API, infrastructuur, cloud, mobiel, AI-toepassingen) en de gemiddelde omvang in mandagen?	De prijsbeoordeling vindt uitsluitend plaats op basis van het tarief per mandag; er worden geen fictieve volumes of wegingen toegepast. Voor de omvang, zie het antwoord op vraag 24.
185.	Beschrijvend document – §5.1.2 Gunningscriterium Prijs	Heeft KB overwogen een maximale marktconforme tariefgrens vast te stellen, waarbij alle tarieven tot deze grens de maximale score behalen en de beoordeling vervolgens primair plaatsvindt op kwaliteit? Hiermee wordt voorkomen dat inschrijvers strategisch inschrijven met een zeer laag dagtarief, terwijl de werkelijke kosten van een Nadere Opdracht mede worden bepaald door de benodigde inspanning in mandagen.	Nee. De KB hanteert geen bovengrens voor het tarief per mandag. Wel hanteert de KB een ondergrens van € 1.000,- per mandag (zie het antwoord op vraag 187).
186.	Beschrijvend document – §5.1.2 Gunningscriterium Prijs	Hanteert de KB een bandbreedte of een specifieke toets voor abnormaal lage tarieven, en zo ja welke?	Ja. De KB hanteert een ondergrens van € 1.000,- per mandag (zie het antwoord op vraag 187).
187.	Beschrijvend document – §5.1.2 Gunningscriterium Prijs	U schrijft dat de KB het recht heeft om de marktconformiteit van de door Opdrachtnemer aangeboden uren/mandagen te (laten) beoordelen. Bent u bereid om tevens een marktconforme ondergrens voor de prijsstelling te hanteren, zodat wordt geborgd dat inschrijvingen realistisch en uitvoerbaar zijn en de gevraagde kwaliteit van de dienstverlening kan worden gewaarborgd?	Ja, dat is akkoord. De KB hanteert een ondergrens van € 1.000,- (exclusief btw) voor het aan te bieden all-in tarief per mandag. Een Inschrijving met een tarief onder deze ondergrens is ongeldig. De ondergrens is verwerkt in Bijlage 5 Prijzenblad Nvl 1, die gelijktijdig met deze Nota van Inlichtingen via TenderNed wordt gepubliceerd. Inschrijver dient

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
			uitsluitend gebruik te maken van dit gewijzigde Prijzenblad.
188.	Beschrijvend document – §5.1.2 Gunningscriterium Prijs	Prijs heeft met een weging van 40% een substantiële invloed op de uiteindelijke gunning. Tegelijkertijd vraagt Opdrachtgever om specialistische dienstverlening, en inzet van senior pentesters, waarbij kwaliteit, deskundigheid, continuïteit en actuele kennis van aanvalstechnieken essentieel zijn. Kan Opdrachtgever aangeven vanaf welk prijsniveau of op basis van welke objectieve criteria zij een aangeboden dagtarief als mogelijk niet-marktconform of abnormaal laag beschouwt en nader zal onderzoeken? En is Opdrachtgever bereid om, ter voorkoming van inschrijvingen waarbij het aangeboden prijsniveau niet in verhouding staat tot de gevraagde kwaliteit, vooraf een marktconforme ondergrens of referentieprijs in het prijzenblad op te nemen?	Zie het antwoord op vraag 186. Voor een ondergrens, zie het antwoord op vraag 187.
189.	Beschrijvend document – §5.1.2 Gunningscriterium Prijs	Prijs weegt voor 40% mee in de beoordeling. Wij begrijpen dat Opdrachtgever hiermee belang hecht aan een scherpe en competitieve prijsstelling. Tegelijkertijd zien wij dat in het prijzenblad geen ondergrens is opgenomen voor het dagtarief voor pentesten. Bij specialistische cybersecuritydienstverlening bestaat hierdoor het risico dat inschrijvers een zeer laag tarief aanbieden om een maximaal prijsvoordeel te behalen. Een dergelijk prijsniveau hoeft niet noodzakelijkerwijs representatief te zijn voor het tarief waartegen de dienstverlening gedurende de looptijd duurzaam en op het gevraagde kwaliteitsniveau kan worden uitgevoerd. Een kwalitatief hoogwaardige pentestdienstverlening, en inzet van senior pentesters, vraagt immers structurele investeringen in onder meer ervaren en gecertificeerde pentesters, opleiding en kennisontwikkeling, kwaliteitsborging, tooling, onderzoek naar nieuwe aanvalstechnieken en het behouden van schaarse specialistische medewerkers.	Ja. Zie het antwoord op vraag 187.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		Wij zijn daarom van mening dat zowel Opdrachtgever als Opdrachtnemer gebaat zijn bij een goede balans tussen een scherpe inkoopprijs enerzijds en een prijsniveau dat duurzame, kwalitatief hoogwaardige dienstverlening gedurende de looptijd mogelijk maakt anderzijds. Daarmee blijft prijs een relevant gunningscriterium, maar wordt voorkomen dat de prijsbeoordeling vooral een prikkel vormt om tarieven aan te bieden die niet passen bij het gewenste kwaliteitsniveau. Bent u bereid een marktconforme minimumdagprijs van 1.000 EUR te hanteren, zodat prijsconcurrentie plaatsvindt binnen een bandbreedte waarin aantoonbaar ruimte blijft voor de door u verlangde kwaliteit, deskundigheid, continuïteit en kennisontwikkeling?	
190.	Beschrijvend document – §5.1.2 Gunningscriterium Prijs	§5.1.2 Gunningscriterium Prijs, §6.1 Beoordeling Inschrijving, irreële of manipulatieve inschrijving In het Beschrijvend document is opgenomen dat een irreële of manipulatieve Inschrijving tot uitsluiting kan leiden. Kan Opdrachtgever verduidelijken welke objectieve omstandigheden aanleiding geven tot een nadere verificatie van de prijsstelling en de uitvoerbaarheid van de Inschrijving?	De KB beoordeelt dit per geval. Zie het antwoord op vraag 186.
191.	Beschrijvend document – §5.1.2 Gunningscriterium Prijs	§5.1.2 Gunningscriterium Prijs, §6.1 Beoordeling Inschrijving, irreële of manipulatieve inschrijving Kan Opdrachtgever bevestigen dat bij gerede twijfel over de realiteitswaarde of uitvoerbaarheid van een Inschrijving een schriftelijke en controleerbare onderbouwing kan worden gevraagd van de prijsopbouw, personeelsmix, beschikbare uitvoeringscapaciteit, kwaliteitsborging en de wijze waarop alle eisen en aangeboden maatregelen binnen de prijs daadwerkelijk worden geleverd?	Ja, dat wordt bevestigd.
192.	Beschrijvend document – §5.1.2 Gunningscriterium Prijs	§5.1.2 Gunningscriterium Prijs, §6.1 Beoordeling Inschrijving, irreële of manipulatieve inschrijving	Zie het antwoord op vraag 190.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		Kan Opdrachtgever bevestigen dat een Inschrijving niet als realistisch wordt beschouwd wanneer de aangeboden prijs en uitvoeringsopzet redelijkerwijs onvoldoende ruimte bieden om de volledige gevraagde en aangeboden dienstverlening uit te voeren?	
193.	Beschrijvend document – §5.1.2 Gunningscriterium Prijs	§5.1.2 Gunningscriterium Prijs, §6.1 Beoordeling Inschrijving, irreële of manipulatieve inschrijving Kan Opdrachtgever bevestigen dat bij de verificatie mede wordt gekeken naar de aannames die aan de prijsstelling ten grondslag liggen, de personeelsmix en senioriteitsverdeling, de vereiste ervaring en certificeringen, de inzet voor inventarisatie, voorbereiding, testuitvoering, analyse, validatie, vierogencontrole, rapportage, bespreking, opvolging, continuïteit en overige activiteiten die binnen de aangeboden prijs moeten worden uitgevoerd?	Zie het antwoord op vraag 190.
194.	Beschrijvend document – §5.1.2 Gunningscriterium Prijs	§5.1.2 Gunningscriterium Prijs, §6.1 Beoordeling Inschrijving, irreële of manipulatieve inschrijving Kan Opdrachtgever bevestigen dat bij de verificatie niet uitsluitend naar het aangeboden mandagtarief wordt gekeken, maar naar de samenhang tussen prijs, inzet en aangeboden prestatie?	Ja. Zie het antwoord op vraag 190.
195.	Beschrijvend document – §6.1 Verificatiegesprek	Kunt u aangeven welke aspecten tijdens een eventueel verificatiegesprek nader worden beoordeeld en of daarbij uitsluitend verificatie plaatsvindt of ook inhoudelijke herbeoordeling?	Tijdens een verificatiegesprek wordt geverifieerd of de Inschrijving voldoet aan de gestelde eisen en worden de gemaakte aannames en toezeggingen gecontroleerd. Er vindt geen herbeoordeling van de scores plaats.
196.	Beschrijvend document – §6.1 Verificatiegesprek	Betreft punt 9. Hoelang van tevoren wordt de uitnodiging voor het verificatiegesprek verstuurd? OF Op welke dagen vinden de verificatiegesprekken plaats? Dan kan inschrijver daarmee maximaal rekening houden.	Een eventueel verificatiegesprek vindt plaats in de periode tussen de sluiting van de Inschrijving en de voorlopige gunning. De KB nodigt Inschrijver minimaal vijf werkdagen van tevoren uit.
197.	Beschrijvend document – §6.2 Beoordelingscommissie	In paragraaf 6.2 staat dat de beoordelingscommissie uit maximaal drie deskundige medewerkers van de KB bestaat.	a. De beoordelingscommissie bestaat uit drie personen.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		Kan de KB aangeven: a. uit hoeveel personen de beoordelingscommissie naar verwachting bestaat; b. welke functies, vakgebieden of deskundigheden binnen deze commissie zijn vertegenwoordigd; c. of alle leden alle drie de kwalitatieve gunningscriteria beoordelen; d. of voor alle Inschrijvingen dezelfde beoordelaars worden ingezet? Kan de KB tevens bevestigen dat ieder kwalitatief gunningscriterium door ten minste twee beoordelaars wordt beoordeeld? De formulering “maximaal drie personen” sluit momenteel niet uit dat de beoordeling door slechts één persoon wordt uitgevoerd.	b. CISO, Technical Information Security Officer en Security Specialist. De KB behoudt zich het recht voor om de beoordelingscommissie bij onvoorziene omstandigheden te wijzigen. c. Ja, alle leden beoordelen alle drie de kwalitatieve gunningscriteria. d. Ja. Alle Inschrijvingen worden door dezelfde beoordelingscommissie beoordeeld. De beoordeling wordt door drie personen uitgevoerd.
198.	Beschrijvend document – §7.2 Inschrijving	Bevestigt de KB dat een groepsmaatschappij van Inschrijver (verbonden in de zin van artikel 2:24b BW) binnen dezelfde Inschrijving als Derde en/of Onderaannemer mag optreden, zonder dat dit wordt aangemerkt als een tweede Inschrijving?	Ja, dat wordt bevestigd, mits de betreffende groepsmaatschappij niet zelfstandig of via een andere Inschrijver inschrijft.
199.	Beschrijvend document – §7.3 Vormvereisten Inschrijving	Wordt een digitale handtekening op het Prijzenblad en referentieverklaring geaccepteerd?	Ja, een digitale handtekening wordt geaccepteerd. De referentieverklaring hoeft niet te worden ondertekend.
200.	Beschrijvend document – §7.14 Inschrijven met andere ondernemingen	Kan de KB bevestigen dat wanneer een Onderaannemer wordt opgegeven in Deel II D van het UEA, maar Inschrijver geen beroep doet op de financiële draagkracht of technische beroepsbekwaamheid van deze Onderaannemer om aan de Geschiktheidseisen te voldoen, voor deze Onderaannemer geen afzonderlijk UEA en geen Bijlage 8 hoeft te worden ingediend?	Ja, dat wordt bevestigd. De Onderaannemer dient wel te worden vermeld in het UEA en de Inschrijving (paragraaf 7.14).
201.	Programma van Eisen – E2 Akkoordverklaring	Klopt het dat nummer 1 in de opsomming ontbreekt en is dit onjuiste nummering of is hier een punt weggevalven/vergeten? Kunt u dit herstellen/verduidelijken?	De nummering van de opsomming in eis E2 is onjuist; er ontbreekt geen tekst. De opsomming dient te worden gelezen als 1 tot en met 4.
202.	Programma van Eisen – E5 en E12 Nederlandse taal	Kunt u bevestigen dat de eis ten aanzien van de Nederlandse taal uitsluitend betrekking heeft op de communicatie en op te leveren documenten richting de KB, en dat interne communicatie en interne	Ja, dat wordt bevestigd. Alle communicatie met de KB (waaronder offertes, rapportages en besprekingen) vindt in het Nederlands plaats.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		werkdokumentatie van Opdrachtnemer, waaronder communicatie tussen pentesters, technische notities en tooling, in het Engels mogen plaatsvinden, mits dit geen invloed heeft op de Nederlandstalige dienstverlening en communicatie richting de KB?	
203.	Programma van Eisen – E5 en E12 Nederlandse taal	Binnen het Programma van Eisen wordt in E12 gespecificeerd dat "communicatie, documenten en correspondentie in het kader van deze Opdracht en de Nadere Overeenkomsten" in het Nederlandse taal gevoerd en/of opgesteld dient te worden. Kan de KB bevestigen dat deze eis ziet op de communicatie richting de KB en de op te leveren documentatie, en niet betekent dat alle ingezette pentesters Nederlandstalig moeten zijn, waarbij de communicatie met opdrachtgever wordt verzorgd door één of meerdere Nederlandstalige teamleden?	Ja. Zie het antwoord op vraag 202.
204.	Programma van Eisen – E5 en E12 Nederlandse taal	Mag een individuele pentester met Engels als werktal worden ingezet, mits alle communicatie, offertes, rapportages en besprekingen met de KB in het Nederlands plaatsvinden en een Nederlandstalige senior pentester eindverantwoordelijk is?	Ja. Zie het antwoord op vraag 202.
205.	Programma van Eisen – E5 en E12 Nederlandse taal	Wordt er een specifiek Nederlands taalvaardigheidsniveau (bijvoorbeeld B2 of C1 volgens het ERK) vereist voor de in te zetten pentesters, of volstaat het dat zij mondeling en schriftelijk professioneel in het Nederlands kunnen communiceren?	De KB hanteert geen specifiek taalniveau. Zie het antwoord op vraag 202.
206.	Programma van Eisen – E5 en E12 Nederlandse taal	Is de KB bereid als eis of sterke voorkeur op te nemen dat alle uitvoerende pentesters beschikken over aantoonbare professionele beheersing van de Nederlandse taal op minimaal C1-niveau zodat technische bevindingen direct met stakeholders kunnen worden afgestemd?	Nee, dat is niet akkoord. Zie het antwoord op vraag 205.
207.	Programma van Eisen – E5 en E12 Nederlandse taal	Is het toegestaan technisch bewijsmateriaal in de rapportage, zoals tooloutput, screenshots en CVE-omschrijvingen, in het Engels op te nemen?	Ja. Technisch bewijsmateriaal zoals tooloutput, schermafbeeldingen en CVE-omschrijvingen mag in de oorspronkelijke taal worden opgenomen. De overige

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
			onderdelen van de rapportage worden in het Nederlands opgesteld.
208.	Programma van Eisen – E6 Garantie (capaciteit)	E6 bepaalt dat Opdrachtnemer gedurende de gehele looptijd over voldoende capaciteit en expertise moet beschikken. De KB geeft geen indicatie van het aantal gelijktijdige pentesten, de gewenste starttermijn of de verwachte spreiding van de opdrachten. Kan de KB aangeven: a. hoeveel pentesten naar verwachting per jaar worden uitgevoerd; b. hoeveel pentesten naar verwachting gelijktijdig kunnen lopen; c. welke minimale termijn doorgaans ligt tussen opdrachtverstrekking en de gewenste startdatum; d. binnen welke termijn Opdrachtnemer een pentest beschikbaar moet kunnen inplannen?	a. Zie het antwoord op vraag 24. b. Zie het antwoord op vraag 30. c. en d. Dit verschilt per Nadere Opdracht. De gewenste startdatum wordt in de offerteaanvraag aangegeven en in overleg vastgesteld.
209.	Programma van Eisen – E6 Garantie (capaciteit)	Geldt er een minimaal aantal aan te bieden pentesters?	Nee. Opdrachtnemer garandeert wel voldoende capaciteit en expertise gedurende de gehele looptijd (E6).
210.	Programma van Eisen – E8 Exclusiviteit	Volgens E8 mag de KB pentesten buiten de Raamovereenkomst inkopen wanneer Opdrachtnemer op enig moment niet aan de overeengekomen verplichtingen kan voldoen. Kan de KB toelichten wanneer hiervan sprake is? Bevestigt de KB dat zij Opdrachtnemer, behoudens aantoonbare spoedeisende omstandigheden, eerst schriftelijk in gebreke stelt en een redelijke termijn biedt om alsnog aan de verplichtingen te voldoen voordat een pentest buiten de Raamovereenkomst wordt ingekocht?	Hiervan is sprake indien Opdrachtnemer een Nadere Opdracht niet, niet tijdig of niet conform de gestelde eisen kan uitvoeren, bijvoorbeeld wanneer Opdrachtnemer niet binnen de termijn van E19 een offerte uitbrengt of niet binnen de door de KB gewenste periode capaciteit beschikbaar heeft. Er is geen sprake van een ingebrekestelling; de KB informeert Opdrachtnemer wel vooraf.
211.	Programma van Eisen – E8 Exclusiviteit	Wanneer is er sprake van een situatie waarin Opdrachtnemer 'niet aan de overeengekomen verplichtingen kan voldoen', zodat de KB pentesten buiten de Raamovereenkomst mag inkopen? Welke doorlooptijd verwacht de KB tussen ondertekening van de offerte en de start van de pentest?	Zie het antwoord op vraag 210. De doorlooptijd wordt per Nadere Opdracht in overleg vastgesteld.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
212.	Programma van Eisen – E9 en E10 Wet- en regelgeving en normen	E9 en E10 verplichten Opdrachtnemer om gedurende de looptijd steeds te voldoen aan nieuwe wet- en regelgeving en opvolgende versies van normen. Bevestigt de KB dat Opdrachtnemer een redelijke implementatietermijn krijgt wanneer wetgeving of een norm gedurende de looptijd wijzigt? Bevestigt de KB tevens dat Partijen in overleg treden over de financiële en operationele gevolgen wanneer een wijziging aantoonbaar leidt tot aanvullende werkzaamheden of kosten die bij Inschrijving redelijkerwijs niet konden worden voorzien?	Ja, dat wordt bevestigd.
213.	Programma van Eisen – E9 en E10 Wet- en regelgeving en normen	Kunt u bevestigen dat nieuwe security-, compliance-, audit- of rapportageverplichtingen die na contractsluiting worden geïntroduceerd en leiden tot aanvullende werkzaamheden of kosten, worden behandeld via de wijzigingsprocedure?	Zie het antwoord op vraag 212.
214.	Programma van Eisen – E11 Schade	E11 van het Programma van Eisen bepaalt dat Opdrachtnemer aansprakelijk is voor alle schade die aan Opdrachtnemer is toe te rekenen. In artikel 26.2 en 26.3 ARBIT 2022 is de aansprakelijkheid, behoudens de uitzonderingen van artikel 26.4, per gebeurtenis begrensd. Op grond van artikel 1.3 van de Raamovereenkomst staat het Beschrijvend document inclusief het Programma van Eisen hoger in rang dan ARBIT 2022. Bevestigt de KB dat E11 geen afwijking vormt van de aansprakelijkheidsbeperkingen van artikel 26.2 en 26.3 ARBIT 2022 en dat deze beperkingen onverkort van toepassing zijn op aansprakelijkheid die voortvloeit uit E11? Bevestigt de KB tevens dat onder “de Vergoeding” als bedoeld in artikel 26.3 ARBIT 2022 wordt verstaan: de totale overeengekomen prijs van de Nadere Overeenkomst waarop de schadeveroorzakende gebeurtenis betrekking heeft? Zo nee, verzoeken wij de KB de toepasselijke aansprakelijkheidsbegrenzing en de berekeningsgrondslag te verduidelijken.	Ja. Eis E11 vormt geen afwijking van de aansprakelijkheidsbeperkingen van artikel 26 ARBIT-2022. Ja, dat wordt bevestigd. Onder de Vergoeding als bedoeld in artikel 26.3 ARBIT-2022 wordt verstaan de totale overeengekomen prijs van de Nadere Overeenkomst waarop de schadeveroorzakende gebeurtenis betrekking heeft.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
215.	Programma van Eisen – E11 Schade	Kunt u bevestigen dat E11 niet beoogt af te wijken van de aansprakelijkheidsregeling zoals opgenomen in ARBIT 2022 en uitsluitend ziet op schade waarvoor Opdrachtnemer op grond van de overeengekomen aansprakelijkheidsregeling aansprakelijk is?	Ja. Zie het antwoord op vraag 214.
216.	Programma van Eisen – E11 Schade	E11 i.c.m. ARBIT art. 26 en BD §7.13 Volgens E11 is Opdrachtnemer aansprakelijk voor 'alle schade' die aan hem toe te rekenen is, zonder beperking. Gelet op de rangorde in §7.13 van het Beschrijvend document gaat het Programma van Eisen boven ARBIT-2022. Kan de KB bevestigen dat de aansprakelijkheidsbeperkingen van artikel 26.2 en 26.3 ARBIT-2022 onverkort van toepassing zijn op de aansprakelijkheid uit E11? Zo niet, is de KB bereid E11 in die zin aan te passen?	Ja. Zie het antwoord op vraag 214.
217.	Programma van Eisen – E11 Schade	U noemt hier dat de opdrachtnemer aansprakelijk is voor alle schade die toe te rekenen is aan de opdrachtnemer. Als ervaren pentestpartner voor vele NL-organisaties (ook in de publieke sector) vergelijkbaar met de KB, zien wij de gebruikelijke aansprakelijkheid beperkt is tot directe schade. Wilt u deze eis daartoe beperken en zo in verhouding brengen tot de opdracht?	Nee, dat is niet akkoord. De KB maakt geen onderscheid tussen directe en indirecte schade. Zie verder het antwoord op vraag 214.
218.	Programma van Eisen – E11 Schade	Bijlage 1 – Programma van Eisen, Eis 11. U stelt dat de Opdrachtnemer aansprakelijk is voor "alle toe te rekenen schade". In onze beroepsgroep is het gebruikelijk de aansprakelijkheid te beperken waarbij de maximum aansprakelijkheid in redelijke verhouding staat tot het met de Overeenkomst gemoeide honorarium. Wij wijzen in dit kader naar Voorschrift 3.9 D van de Gids Proportionaliteit, 3e herziening d.d. 1 januari 2022 door het Ministerie van Economische Zaken, Landbouw en Innovatie is uitgebracht. Dit Voorschrift 3.9 D bepaalt dat de aansprakelijkheid van de opdrachtnemer gelimiteerd dient te zijn, waarbij de aansprakelijkheidsbeperking die in de betreffende branche gebruikelijk is in acht dient te worden genomen. De formulering inzake aansprakelijkheid als thans opgenomen in Eis 11 sluit hier niet bij aan.	Nee, dat is niet akkoord. Zie het antwoord op vraag 217.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		Kunt u akkoord gaan met het aanpassen van de aansprakelijkheid conform vorenstaande en artikel 18.5 als volgt aanpassen: “De totale aansprakelijkheid van opdrachtnemer jegens opdrachtgever voor eventuele fouten die bij zorgvuldig handelen door opdrachtnemer zouden zijn vermeden, is beperkt tot maximaal driemaal het bedrag van het honorarium dat opdrachtgever heeft betaald en/of nog verschuldigd is voor de onder de opdracht verrichte specifieke werkzaamheden waaruit de fouten voortvloeien. Indien de opdracht een langere doorlooptijd heeft dan twaalf maanden, dan is de totale aansprakelijkheid in het kader van de opdracht beperkt tot maximaal driemaal het bedrag van het honorarium dat opdrachtgever aan opdrachtnemer heeft betaald en/of nog verschuldigd is over de laatste twaalf maanden voor de onder de opdracht verrichte specifieke werkzaamheden waaruit de fouten voortvloeien. Samenhangende fouten worden daarbij aangemerkt als één fout.”	
219.	Programma van Eisen – E14 Bereikbaarheid	Kan de KB aangeven in welke mate werkzaamheden buiten reguliere kantooruren of in weekenden worden verwacht? Indien dit wordt verlangd, moet dit dan volledig binnen het aangeboden all in mandag tarief worden uitgevoerd?	Werkzaamheden buiten reguliere kantooruren of in het weekend worden alleen in uitzonderlijke gevallen gevraagd en worden in dat geval vooraf in de offerteaanvraag aangegeven. Mocht hier sprake van zijn dan komen Partijen vooraf een (marktconforme) toeslag overeen.
220.	Programma van Eisen – E17 Managementinformatie	Betreft "Informatie met betrekking tot uitgevoerde pentesten". Welke informatie en met welk detailniveau, verwacht de opdrachtgever hier precies? Mogen wij als ervaren pentestpartner voor vele met KB vergelijkbare organisaties een suggestie hierin doen?	De KB verwacht een overzicht van de uitgevoerde pentesten (onderwerp, periode, status, ureninzet en kosten). Opdrachtnemer mag hiervoor een voorstel doen. De definitieve inhoud wordt in overleg vastgesteld.
221.	Programma van Eisen – E17 Managementinformatie	Betreft "Bevindingen (laag, midden en hoog)". Verwacht de opdrachtgever hier enkel een aantal per risicoscore, of een meer gedetailleerd overzicht? Zoja, welk detailniveau is gewenst?	Een overzicht van het aantal bevindingen per risicoclassificatie per pentest volstaat. Zie ook het antwoord op vraag 220.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
222.	Programma van Eisen – E18 Nadere overeenkomst (inventarisatie)	Volgens E18 mag Opdrachtnemer voor de inventarisatie en het volledige proces tot aan het sluiten van de Nadere Overeenkomst geen kosten in rekening brengen. De omvang van deze inventarisatie is niet begreind. Kan de KB aangeven welke werkzaamheden en maximale tijdsbesteding zij onder de kosteloze inventarisatie verstaat? Bevestigt de KB dat aanvullende technische onderzoeken, workshops, locatiebezoeken, architectuuranalyses en het inrichten van een testomgeving geen onderdeel zijn van de kosteloze inventarisatie, tenzij dit vooraf uitdrukkelijk is overeengekomen?	Onder de inventarisatie verstaat de KB alle werkzaamheden die nodig zijn om tot een passende offerte te komen, zoals het voeren van (intake)gesprekken, het bestuderen van beschikbare documentatie en het vaststellen van de scope, aanpak en planning. De KB hanteert geen maximale tijdsbesteding. Werkzaamheden die onderdeel zijn van de uitvoering van de pentest (zoals het inrichten van een testomgeving) vallen onder de Nadere Opdracht.
223.	Programma van Eisen – E18 Nadere overeenkomst (inventarisatie)	De inventarisatie/intake vormt een noodzakelijk onderdeel van de voorbereiding op een Nadere Opdracht. Kunt u bevestigen dat de hiervoor benodigde uren mogen worden meegenomen in de vaste aanneemsom voor de betreffende Nadere Opdracht?	Nee. De inventarisatie tot aan het sluiten van de Nadere Overeenkomst is kosteloos (E18) en mag niet in de vaste aanneemsom worden verwerkt. De voorbereiding van de uitvoering (E32) maakt wel onderdeel uit van de aanneemsom.
224.	Programma van Eisen – E18 Nadere overeenkomst (inventarisatie)	Kunt u bevestigen dat voor iedere Nadere Overeenkomst vooraf schriftelijk wordt vastgelegd: de scope van de pentest, de te testen systemen en omgevingen, de beoogde testmethodiek, de deliverables en eventuele beperkingen en randvoorwaarden?	Ja, dit wordt vastgelegd in de offerte (E20) die na ondertekening door de KB de Nadere Overeenkomst vormt (E22).
225.	Programma van Eisen – E18 Nadere overeenkomst (inventarisatie)	E18 Nadere Overeenkomst, E19 Reactietermijn, E20 Offerte Is Opdrachtgever bereid voor iedere Offerteaanvraag een minimale dataset te hanteren die, voor zover relevant, informatie bevat over het doel en de achtergrond van de pentest, de testobjecten, de expliciete in-scope- en out-of-scopeonderdelen, de architectuur en de gebruikte technologieën, versies en koppelingen?	De KB begrijpt niet geheel wat Inschrijver bedoelt met een 'minimale dataset'. Mogelijk doelt Inschrijver op een vragenlijst voor de inventarisatie die de KB vooraf beantwoordt. De KB verzoekt Inschrijver de vraag in de tweede vragenronde te verduidelijken.
226.	Programma van Eisen – E18 Nadere overeenkomst (inventarisatie)	E18 Nadere Overeenkomst, E19 Reactietermijn, E20 Offerte Is Opdrachtgever bereid in de minimale dataset, voor zover relevant, locatievereisten, rapportage- en hertestverwachtingen, de gewenste start- en opleverdatum, contactpersonen en de escalatieprocedure op te nemen?	Zie het antwoord op vraag 225.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
227.	Programma van Eisen – E18 Nadere overeenkomst (inventarisatie)	E18 Nadere Overeenkomst, E19 Reactietermijn, E20 Offerte Is Opdrachtgever bereid in de minimale dataset, voor zover relevant, de gewenste testmethodiek en toetsingskaders, toegestane en uitgesloten testtechnieken, productiebeperkingen en testvensters, afhankelijkheden en betrokken derden op te nemen?	Zie het antwoord op vraag 225.
228.	Programma van Eisen – E18 Nadere overeenkomst (inventarisatie)	E18 Nadere Overeenkomst, E19 Reactietermijn, E20 Offerte Is Opdrachtgever bereid in de minimale dataset, voor zover relevant, de URL's, domeinen, IP-adressen en API's, gebruikersrollen, testaccounts en autorisatieniveaus, beschikbare documentatie, testomgeving en testdata op te nemen?	Zie het antwoord op vraag 225.
229.	Programma van Eisen – E18 Nadere overeenkomst (inventarisatie)	Kunt u toelichten op basis van welke uitgangspunten Nadere Overeenkomsten worden uitgevraagd en gegund aan de gecontracteerde leveranciers, waaronder de toe te passen beoordelingscriteria, weging en gunningsmethodiek?	De KB sluit de Raamovereenkomst met één Opdrachtnemer (zie het antwoord op vraag 40). Nadere Opdrachten worden rechtstreeks aan Opdrachtnemer verstrekt; er is geen sprake van een minicompetitie.
230.	Programma van Eisen – E19 Reactietermijn	E19 bepaalt dat Opdrachtnemer binnen maximaal tien werkdagen een offerte verstrekt. Vanaf welk moment gaat deze termijn lopen? Bevestigt de KB dat de termijn aanvangt nadat de inventarisatie is afgerond en Opdrachtnemer alle informatie heeft ontvangen die nodig is om scope, aanpak, planning en urenbegroting verantwoord vast te stellen?	De termijn van tien werkdagen gaat lopen op het moment dat de inventarisatie (het gesprek met de aanvrager vanuit de KB) heeft plaatsgevonden en Opdrachtnemer de daarbij afgesproken informatie heeft ontvangen.
231.	Programma van Eisen – E19 Reactietermijn	E18 Nadere Overeenkomst, E19 Reactietermijn, E20 Offerte Kan Opdrachtgever bevestigen dat de termijn van maximaal tien werkdagen voor het uitbrengen van een offerte aanvangt nadat Opdrachtnemer beschikt over de informatie die redelijkerwijs noodzakelijk is om scope, aanpak, planning, personeelsinzet, kwaliteitsborging en urenbegroting verantwoord vast te stellen?	Zie het antwoord op vraag 230.
232.	Programma van Eisen – E19 Reactietermijn	E18 Nadere Overeenkomst, E19 Reactietermijn, E20 Offerte	Zie het antwoord op vraag 230.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		Kan Opdrachtgever bevestigen dat ontbrekende essentiële informatie wordt aangevuld voordat de offertetermijn aanvangt, of dat Partijen in dat geval een passende afwijkende offertetermijn overeenkomen?	
233.	Programma van Eisen – E21 Marktconformiteit	Volgens E21 mag de KB de aangeboden uren of mandagen op marktconformiteit laten beoordelen. Kan de KB aangeven op basis van welke objectieve maatstaven, referentiegegevens en deskundigheid de marktconformiteit wordt beoordeeld? Worden daarbij de aard, scope, complexiteit, testmethodiek, vereiste expertise, rapportageverplichtingen en risicoklasse van de betreffende pentest betrokken? Krijgt Opdrachtnemer inzage in de onderbouwing van het oordeel en gelegenheid daarop te reageren?	De KB kan de marktconformiteit beoordelen aan de hand van vergelijkbare pentesten of laten beoordelen door een onafhankelijke deskundige. Daarbij worden onder andere de scope, complexiteit, testmethodiek en vereiste expertise van de betreffende pentest betrokken. Opdrachtnemer krijgt inzage in de onderbouwing van het oordeel en de gelegenheid daarop te reageren (zie het overleg zoals opgenomen in E21).
234.	Programma van Eisen – E21 Marktconformiteit	Welke objectieve criteria hanteert de KB bij de beoordeling van de marktconformiteit van urenbegrotingen en offertes?	Zie het antwoord op vraag 233.
235.	Programma van Eisen – E21 Marktconformiteit	Kan de KB toelichten aan de hand van welke objectieve criteria wordt beoordeeld of een ureninschatting of mandagenbegroting marktconform is? Is de KB bereid vast te leggen dat bij deze beoordeling rekening wordt gehouden met onder meer de complexiteit van de omgeving, testdiepgang, scope, beschikbaar gestelde informatie, benodigde expertise en gevraagde methodiek?	Ja. Zie het antwoord op vraag 233.
236.	Programma van Eisen – E21 Marktconformiteit	Wie beoordeelt de marktconformiteit van de aangeboden uren/mandagen, aan de hand van welke criteria of benchmark, en wie draagt de kosten van deze beoordeling? Wat gebeurt er indien partijen na overleg geen overeenstemming bereiken?	Zie het antwoord op vraag 233. De kosten van de beoordeling zijn voor rekening van de KB. Indien Partijen na overleg geen overeenstemming bereiken, is de KB gerechtigd de betreffende Nadere Opdracht niet aan Opdrachtnemer te verstrekken.
237.	Programma van Eisen – E21 Marktconformiteit	Marktconformiteit urenbegroting Opdrachtnemer moet marktconforme urenbegrotingen garanderen en Opdrachtgever heeft het recht offertes daarop te laten beoordelen. Kan Opdrachtgever verduidelijken op basis van welke objectieve	Zie het antwoord op vraag 233. De beoordeling heeft betrekking op het aantal uren/mandagen; het aangeboden tarief per mandag staat vast. Inzage in

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		criteria, benchmark en vergelijkbare scope marktconformiteit wordt bepaald? Kan tevens worden bevestigd dat een onderzoek geen toegang geeft tot kostprijzen, marges, salarissen, gegevens van andere klanten of andere bedrijfsvertrouwelijke informatie en dat verschil van inzicht over marktconformiteit geen grond vormt voor eenzijdige prijsaanpassing?	kostprijzen, marges en salarissen is hiervoor niet vereist.
238.	Programma van Eisen – E21 Marktconformiteit	E21 Marktconformiteit, E32 Activiteiten, E33 Bespreken pentesten, E35 Vierogen-principe Kan Opdrachtgever bevestigen dat iedere uren- of mandagenbegroting aantoonbaar voldoende ruimte moet bieden voor de volledige uitvoering van alle voor de betreffende pentest noodzakelijke activiteiten?	Ja. Zie het antwoord op vraag 121.
239.	Programma van Eisen – E21 Marktconformiteit	E21 Marktconformiteit, E32 Activiteiten, E33 Bespreken pentesten, E35 Vierogen-principe Kan Opdrachtgever bevestigen dat een uren- of mandagenbegroting ten minste ruimte moet bieden voor intake en scopebepaling, voorbereiding, technische testuitvoering, analyse van resultaten, validatie en uitsluiting van false positives, risico- en impactbepaling, praktisch toepasbare hersteladviezen, technische en redactionele kwaliteitscontrole, vierogencontrole, de volledige rapportage, bespreking en toelichting van de resultaten en noodzakelijke communicatie en escalatie gedurende de opdracht?	Ja, met uitzondering van de inventarisatie (intake en scopebepaling) tot aan het sluiten van de Nadere Overeenkomst; deze is op grond van eis E18 kosteloos en wordt niet in de vaste aanneemsom verwerkt (zie het antwoord op vraag 223). Zie verder het antwoord op vraag 121.
240.	Programma van Eisen – E21 Marktconformiteit	E21 Marktconformiteit, E32 Activiteiten, E33 Bespreken pentesten, E35 Vierogen-principe Kan Opdrachtgever bevestigen dat de beoordeling van een urenbegroting niet uitsluitend is gericht op de vraag of het aantal uren niet te hoog is, maar ook op de vraag of de aangeboden inzet voldoende en realistisch is om de overeengekomen scope, alle verplichte activiteiten en het aangeboden kwaliteitsniveau volledig uit te voeren?	Ja. Zie het antwoord op vraag 121.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
241.	Programma van Eisen – E21 Marktconformiteit	E21 Marktconformiteit, E32 Activiteiten, E33 Bespreken pentesten, E35 Vierogen-principe Kan Opdrachtgever bevestigen dat een begroting die redelijkerwijs onvoldoende ruimte biedt voor de verplichte activiteiten niet als een passende of marktconforme begroting wordt beschouwd?	Ja. Zie het antwoord op vraag 121.
242.	Programma van Eisen – E21 Marktconformiteit	E21 Marktconformiteit, E32 Activiteiten, E33 Bespreken pentesten, E35 Vierogen-principe Kan Opdrachtgever aangeven op welke wijze tijdens de offertebeoordeling en uitvoering wordt vastgesteld dat de volledige aangeboden dienstverlening daadwerkelijk in de begroting is opgenomen?	Dit blijkt uit de offerte (E20) en de daarin opgenomen urenbegroting. De KB kan daarnaast een nadere specificatie opvragen. Zie ook het antwoord op vraag 121.
243.	Programma van Eisen – E23 Annuleren Nadere Opdracht	23 bepaalt dat een Nadere Opdracht tot maximaal twee weken voor uitvoering kosteloos kan worden geannuleerd. 1. Bedoelt de KB dat een Nadere Opdracht tot veertien kalenderdagen vóór de overeengekomen startdatum kosteloos kan worden geannuleerd? 2. Bevestigt de KB dat bij annulering binnen veertien kalenderdagen de aantoonbaar gemaakte kosten én de reeds gereserveerde, redelijkerwijs niet meer inzetbare capaciteit in rekening mogen worden gebracht?	1. Ja, dat is correct. 2. Nee. Onder de reeds gemaakte kosten verstaat de KB uitsluitend de kosten van aantoonbaar reeds verrichte werkzaamheden (zoals voorbereiding) en aantoonbare externe kosten. Gereserveerde capaciteit valt hier niet onder.
244.	Programma van Eisen – E23 Annuleren Nadere Opdracht	Omvatten de reeds gemaakte kosten uit E23 ook aantoonbaar gereserveerde specialistische capaciteit en niet annuleerbare verplichtingen jegens goedgekeurde onderaannemers?	Nee. Zie het antwoord op vraag 243.
245.	Programma van Eisen – E23 Annuleren Nadere Opdracht	Kunt u bevestigen dat wanneer een Nadere Opdracht minder dan twee weken voor de geplande uitvoeringsdatum wordt geannuleerd, onder "reeds gemaakte kosten" tevens de kosten vallen van reeds ingeplande en gereserveerde capaciteit die als gevolg van de annulering redelijkerwijs niet meer voor andere opdrachten kan worden ingezet?	Nee. Zie het antwoord op vraag 243.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
246.	Programma van Eisen – E23 Annuleren Nadere Opdracht	Vallen onder 'reeds gemaakte kosten' bij annulering binnen 2 weken voor uitvoering ook de gereserveerde en niet meer inzetbare capaciteit? Is de KB bereid een staffel te hanteren, bijvoorbeeld 50% van de aanneemsom bij annulering binnen 5 werkdagen voor aanvang?	Nee, zie het antwoord op vraag 243. De KB hanteert geen staffel.
247.	Programma van Eisen – E23 Annuleren Nadere Opdracht	Bijlage 1 – Programma van Eisen, Eis 23. U geeft aan dat opdrachtnemer er mee in stemt dat een nadere opdracht maximaal 2 weken voor start kosteloos geannuleerd kan worden. Aangezien onze capaciteit op deze termijn mogelijk niet opnieuw ingepland kan worden stellen wij voor om deze termijn te verlengen naar 3 weken.	Nee, dat is niet akkoord.
248.	Programma van Eisen – E23 Annuleren Nadere Opdracht	Bijlage 1 – Programma van Eisen, Eis 23. U geeft aan dat opdrachtnemer er mee in stemt dat bij annulering Opdrachtnemer de reeds gemaakte kosten bij de KB in rekening brengen. Wij stellen voor - zodat er een duidelijk belang wordt gecreëerd dat KB zich uiterst inspant om een test mogelijk te maken danwel planning scherp bewaakt - dat bij annulering binnen 2 weken voorafgaand aan de start de helft van het offertebedrag in rekening wordt gebracht.	Nee, dat is niet akkoord. Zie het antwoord op vraag 243.
249.	Programma van Eisen – E24 Verzetten Nadere Opdracht	Mag de KB een Nadere Opdracht onbeperkt en kosteloos verzetten, ook kort voor of tijdens de uitvoering? Wij stellen voor dat verzetten tot minimaal 5 werkdagen voor aanvang kosteloos is en dat daarna de annuleringsregeling van E23 van toepassing is. Hoe gaat de KB om met wachttijd door oorzaken aan de zijde van de KB, zoals een niet-beschikbare testomgeving of niet tijdig aangeleverde accounts?	Ja, dat is akkoord. Een Nadere Opdracht kan tot vijf werkdagen voor de geplande aanvang kosteloos door de KB worden verzet. Bij verzetten binnen vijf werkdagen voor aanvang mag Opdrachtnemer de reeds gemaakte kosten (zie het antwoord op vraag 243) in rekening brengen. Eis E24 wordt hierop aangepast. Wachttijd door oorzaken aan de zijde van de KB wordt behandeld conform eis E56.
250.	Programma van Eisen – E24 Verzetten Nadere Opdracht	Gaat opdrachtgever ermee akkoord dat opdrachtnemer zich het recht voorbehoudt om 75% van de totale opdracht waarde in rekening te brengen indien opdrachtgever de opdracht binnen 10 werkdagen vóór de geplande startdatum annuleert of wenst te verplaatsen?	Nee, dat is niet akkoord. Zie de antwoorden op de vragen 243 en 249.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
251.	Programma van Eisen – E24 Verzetten Nadere Opdracht	E24 geeft de KB het recht om een Nadere Opdracht zonder meerkosten naar een ander moment te verplaatsen. Een aankondigingstermijn, maximale verschuiving en maximaal aantal wijzigingen ontbreken. 1. Kan de KB aangeven: a. welke minimale aankondigingstermijn geldt; b. hoe vaak een Nadere Opdracht kosteloos mag worden verplaatst; c. binnen welke termijn de verplaatste opdracht alsnog moet worden uitgevoerd? 2. Bevestigt de KB dat aantoonbare kosten van reeds getroffen voorbereidingen en niet meer anders inzetbare capaciteit in rekening mogen worden gebracht wanneer de KB een opdracht op korte termijn of herhaaldelijk verplaatst?	Zie het antwoord op vraag 249. De verplaatste Nadere Opdracht wordt in overleg opnieuw ingepland.
252.	Programma van Eisen – E24 Verzetten Nadere Opdracht	E24 bevat geen minimale aankondigingstermijn voor het kosteloos verplaatsen van een opdracht. Kan de KB een redelijke minimale termijn opnemen en bevestigen dat aantoonbaar reeds gemaakte kosten en onvermijdbare verplichtingen mogen worden doorberekend?	Zie het antwoord op vraag 249.
253.	Programma van Eisen – E24 Verzetten Nadere Opdracht	In E23 geldt voor annulering een termijn van twee weken, terwijl E24 voor het verzetten van een Nadere Opdracht geen termijn vermeldt. Kunt u bevestigen dat ook voor E24 geldt dat een Nadere Opdracht tot uiterlijk twee weken voor de geplande uitvoeringsdatum kosteloos kan worden verplaatst, en dat bij verplaatsing binnen deze termijn de kosten van reeds gereserveerde capaciteit die redelijkerwijs niet elders kan worden ingezet, in rekening mogen worden gebracht?	Nee. Zie het antwoord op vraag 249.
254.	Programma van Eisen – E24 Verzetten Nadere Opdracht	Kan de KB bevestigen dat voor het kosteloos verplaatsen van een Nadere Opdracht dezelfde termijn geldt als voor kosteloze annulering genoemd in eis E23 (twee weken voorafgaand aan uitvoering)?	Nee. Zie het antwoord op vraag 249.
255.	Programma van Eisen – E24 Verzetten Nadere Opdracht	Kan de KB verduidelijken onder welke voorwaarden een reeds ingeplande Nadere Opdracht kan worden verzet? Indien een pentest	Zie het antwoord op vraag 249.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		reeds is ingepland en capaciteit, personeel en voorbereiding zijn gereserveerd, kan kosteloos uitstel leiden tot aantoonbare kosten voor Opdrachtnemer. Is de KB bereid deze bepaling aan te passen zodat verplaatsing kosteloos mogelijk is mits deze tijdig wordt aangekondigd en reeds gemaakte of aantoonbaar onvermijdbare kosten kunnen worden vergoed?	
256.	Programma van Eisen – E24 Verzetten Nadere Opdracht	Eis 23 regelt vergoeding van reeds gemaakte kosten bij annulering binnen twee weken voor uitvoering, terwijl Eis 24 verplaatsing zonder meerkosten toestaat zonder termijn of beperking. Bent u bereid voor verplaatsing dezelfde termijn van twee weken te hanteren en bij latere verplaatsing vergoeding toe te staan van aantoonbare, redelijkerwijs niet vermijdbare kosten, waaronder reeds gereserveerde capaciteit die niet elders kan worden ingezet?	Nee. Zie het antwoord op vraag 249.
257.	Programma van Eisen – E24 Verzetten Nadere Opdracht	In E23 is bepaald dat bij annulering binnen twee weken voor uitvoering reeds gemaakte kosten in rekening mogen worden gebracht. E24 bepaalt daarentegen dat de KB een Nadere Opdracht zonder meerkosten mag verplaatsen. Geldt het kosteloos verplaatsen ook wanneer dit binnen twee weken voor de geplande uitvoering plaatsvindt en Opdrachtnemer hiervoor reeds aantoonbare kosten heeft gemaakt of uitvoeringscapaciteit heeft gereserveerd? Of is in dat geval een vergelijkbare regeling als bij E23 van toepassing?	Zie het antwoord op vraag 249.
258.	Programma van Eisen – E24 Verzetten Nadere Opdracht	U geeft aan dat u het recht heeft om de uitvoering van Nadere opdrachten zonder kosten te verplaatsen. Hoe vaak verwacht u dat dit gaat gebeuren? Hoe vaak is dat in het verleden per jaar gebeurd?	De KB verwacht dat dit zeer incidenteel voorkomt. De KB houdt hier geen registratie van bij.
259.	Programma van Eisen – E24 Verzetten Nadere Opdracht	U geeft aan dat u het recht heeft om de uitvoering van Nadere opdrachten zonder kosten te verplaatsen. Dit lijkt enigszins tegenstrijdig met E23, kunt u dat toelichten?	Zie het antwoord op vraag 249.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
260.	Programma van Eisen – E25 Onderaanneming	Welke certificeringen bedoelt de KB in E25 met "de door de KB in de Aanbesteding geëiste certificeringen"? Betreft dit uitsluitend ISO 9001 en ISO 27001, of ook de persoonlijke certificeringen uit E27? Geldt E25 ook voor een groepsmaatschappij van Inschrijver die onder hetzelfde gecertificeerde managementsysteem valt?	Voor een Onderaannemer die uitsluitend (een deel van) de technische uitvoering van de Opdracht verzorgt, volstaat het dat het ingezette personeel voldoet aan de persoonsgebonden certificeringen uit E27.
261.	Programma van Eisen – E25 Onderaanneming	In eis E25 is opgenomen dat een Onderaannemer, net als Opdrachtnemer, moet beschikken over de door de KB in de Aanbesteding geëiste certificeringen. Kan de KB bevestigen of met de in E25 genoemde certificeringen uitsluitend wordt bedoeld op de persoonsgebonden pentestcertificeringen zoals opgenomen in E27, waaronder OSCP, OSWE, OSEP, GPEN en CompTIA PenTest+, of dat hieronder tevens de organisatiestandaarden ISO 9001 en ISO 27001 worden verstaan? Indien ook ISO 9001 en ISO 27001 hieronder vallen, kan de KB toelichten op welke wijze dit dient te worden toegepast wanneer de Hoofdaannemer zelfstandig aan deze geschiktheidseisen voldoet en een Onderaannemer uitsluitend voor de technische uitvoering van pentesten wordt ingezet?	Zie het antwoord op vraag 260.
262.	Programma van Eisen – E25 Onderaanneming	Geldt het vermelden van een Onderaannemer in de Inschrijving en het UEA als voorafgaande toestemming in de zin van artikel 23 ARBIT-2022? Volstaat een ISO-certificering op groepsniveau waaronder de Onderaannemer valt?	Ja. Na gunning geldt de vermelding van de Onderaannemer in de Inschrijving als toestemming als bedoeld in artikel 23.1 ARBIT-2022. Zie verder het antwoord op vraag 260. Voor zover certificering van de Onderaannemer relevant is, volstaat een ISO-certificaat op groepsniveau, mits uit het certificaat blijkt dat de Onderaannemer onder de scope van het gecertificeerde managementsysteem valt (zie ook het antwoord op vraag 87).
263.	Programma van Eisen – E26 Betrokkenheid senior pentesters	Bent u bereid te verlangen dat de senior pentester per Nadere Opdracht zelf aantoonbaar inhoudelijke testwerkzaamheden uitvoert en verantwoordelijkheid draagt voor de testaanpak, risicoanalyse en	Ja, dat is akkoord. De KB verlangt dat de betrokken senior pentester daadwerkelijk inhoudelijke testwerkzaamheden uitvoert. Er wordt daarvoor geen minimaal percentage gehanteerd.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		eindrapportage, zodat uitsluitend beperkte begeleiding of een eindcontrole niet voldoende is om aan Eis 26 te voldoen?	
264.	Programma van Eisen – E26 Betrokkenheid senior pentesters	Is het voldoende dat de senior pentester inhoudelijk betrokken is bij scope, methodiek, beoordeling van bevindingen en kwaliteitscontrole, of moet de senior pentester alle technische testwerkzaamheden zelf uitvoeren?	Zie het antwoord op vraag 263.
265.	Programma van Eisen – E26 Betrokkenheid senior pentesters	Wat verstaat de KB onder de verplichte betrokkenheid van een senior in E26? Moet deze persoon alle technische werkzaamheden zelf uitvoeren, of volstaat aantoonbare inhoudelijke betrokkenheid bij scoping, begeleiding, kwaliteitscontrole en rapportage?	Zie het antwoord op vraag 263.
266.	Programma van Eisen – E26 Betrokkenheid senior pentesters	Eis 26 verlangt betrokkenheid van een senior pentester, maar specificeert geen minimale inzet of werkzaamheden. Voldoet een inzet van bijvoorbeeld 10% van de totale inspanning, uitsluitend voor begeleiding en/of controle van de rapportage, aan deze eis? Zo niet, wilt u vastleggen welke werkzaamheden de senior zelf moet uitvoeren en welke minimale inzet per Nadere Opdracht vereist is, zodat alle aanbieders dezelfde uitgangspunten hanteren?	Nee. Zie het antwoord op vraag 263.
267.	Programma van Eisen – E26 Betrokkenheid senior pentesters	E26 Betrokkenheid Senior Pentesters, E27 Kwalificaties Pentesters E26 bepaalt dat bij de uitvoering van pentesten altijd een senior functionaris betrokken is en definieert deze als een medewerker met minimaal vijf jaar ervaring met vergelijkbare pentesten. Kan Opdrachtgever verduidelijken welke minimale inhoudelijke verantwoordelijkheden, activiteiten en beslismomenten onder deze betrokkenheid vallen?	Zie het antwoord op vraag 263.
268.	Programma van Eisen – E26 Betrokkenheid senior pentesters	E26 Betrokkenheid Senior Pentesters, E27 Kwalificaties Pentesters Kan Opdrachtgever bevestigen dat de senior functionaris ten minste de scope, testdoelstellingen en teststrategie inhoudelijk beoordeelt, betrokken is bij de technische uitvoering of daarop aantoonbaar	Ja, met dien verstande dat het uitsluitend houden van toezicht op de technische uitvoering niet volstaat; de betrokken senior pentester voert zelf inhoudelijke testwerkzaamheden uit (zie het antwoord op vraag 263).

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		inhoudelijk toezicht houdt en de volledigheid en diepgang van de uitgevoerde testactiviteiten beoordeelt?	
269.	Programma van Eisen – E26 Betrokkenheid senior pentesters	E26 Betrokkenheid Senior Pentesters, E27 Kwalificaties Pentesters Kan Opdrachtgever bevestigen dat de senior functionaris kritieke en hoge bevindingen technisch valideert, de risico- en impactduiding beoordeelt en de toepasbaarheid van hersteladviezen toetst?	Ja. Zie het antwoord op vraag 263.
270.	Programma van Eisen – E26 Betrokkenheid senior pentesters	E26 Betrokkenheid Senior Pentesters, E27 Kwalificaties Pentesters Kan Opdrachtgever bevestigen dat de senior functionaris het eindrapport inhoudelijk goedkeurt en beschikbaar is voor de rapportagebespreking en escalatie van materiële bevindingen?	Ja. Zie het antwoord op vraag 263.
271.	Programma van Eisen – E26 Betrokkenheid senior pentesters	Eis E26 bepaalt dat bij de uitvoering van de pentesten altijd een senior functionaris van Opdrachtnemer betrokken dient te zijn. Kan de KB bevestigen dat deze rol ook mag worden ingevuld door een senior pentester van een bij Inschrijving opgegeven Onderaannemer, mits deze persoon aantoonbaar beschikt over minimaal vijf jaar relevante ervaring en voldoet aan de kwalificatie-eisen uit E27?	Ja, mits de Onderaannemer bij Inschrijving is vermeld en de senior pentester voldoet aan E26 en E27. Opdrachtnemer blijft volledig verantwoordelijk voor de uitvoering.
272.	Programma van Eisen – E27 Kwalificaties pentesters	Dient iedere medewerker die feitelijke technische pentestwerkzaamheden uitvoert individueel te beschikken over minimaal één van de certificeringen uit E27?	Ja. Iedere medewerker die technische pentestwerkzaamheden uitvoert, dient te beschikken over minimaal één van de in E27 genoemde certificeringen.
273.	Programma van Eisen – E27 Kwalificaties pentesters	Geldt E27 voor iedere medewerker die enige bijdrage levert, inclusief projectleiding, kwaliteitscontrole en rapportbeoordeling, of uitsluitend voor de Security Specialisten die de technische testwerkzaamheden uitvoeren?	E27 geldt voor de medewerkers die technische testwerkzaamheden uitvoeren en voor de medewerker die de vierogencontrole uitvoert (zie het antwoord op vraag 293). Voor projectleiding en overige ondersteunende rollen geldt E27 niet. Zie ook het antwoord op vraag 272.
274.	Programma van Eisen – E27 Kwalificaties pentesters	Dient iedere in te zetten medewerker te beschikken over één van de genoemde certificeringen, of volstaat het dat de (senior) lead hierover	Zie het antwoord op vraag 272.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		beschikt? Accepteert de KB gelijkwaardige certificeringen, zoals CREST CRT/CCT, OSCE3, CRT0, eCPPT of GWAPT?	Naast de in E27 genoemde certificeringen accepteert de KB ook CREST CRT, CREST CCT, OSCE3, eCPPT en GWAPT, alsmede HTB CPTS en HTB CWES (zie het antwoord op vraag 276). CRT0 wordt niet als gelijkwaardig geaccepteerd.
275.	Programma van Eisen – E27 Kwalificaties pentesters	Accepteert de KB gelijkwaardige certificeringen naast de in E27 genoemde, zoals OSCE3, CRT0, eCPPT, CEH Practical of vakbekwaamheid aangetoond onder het CCV-certificatieschema Cyber Security Pen Test? Zo ja, hoe toont Inschrijver de gelijkwaardigheid aan?	Nee. De KB accepteert uitsluitend de in E27 genoemde certificeringen en de certificeringen die in het antwoord op vraag 274 zijn genoemd. CEH Practical wordt niet als gelijkwaardig geaccepteerd. Het CCV-certificatieschema Cyber Security Pen Test betreft een certificering van de organisatie en geldt niet als persoonscertificering in de zin van E27.
276.	Programma van Eisen – E27 Kwalificaties pentesters	Als ervaren pentestpartner voor vele NL-organisaties vergelijkbaar met KB, herkennen we deze eis niet in de dagelijkse praktijk. Herkenbaar vereiste certificeringen die wij hierbij tegenkomen zijn bijv. HackTheBox, CWES en CPTS. Wilt u om die reden deze toevoegen als mogelijke certificeringen bij deze eis?	Ja, dat is akkoord. De certificeringen HTB CPTS en HTB CWES worden toegevoegd aan de in E27 genoemde certificeringen.
277.	Programma van Eisen – E27 Kwalificaties pentesters	Is de Aanbestedende dienst bereid de in E27 genoemde certificeringen aan te vullen met de relevante vakinhoudelijke certificeringen die worden erkend binnen het CCV-keurmerk Pentesten?	Nee. De KB accepteert uitsluitend de certificeringen die zijn genoemd in E27 en in het antwoord op vraag 274. Zie ook het antwoord op vraag 275.
278.	Programma van Eisen – E28 VOG	Accepteert de KB voor medewerkers die niet in Nederland wonen een Nederlandse VOG die via de Justis-procedure voor niet-ingezetenen is aangevraagd?	Ja.
279.	Programma van Eisen – E28 VOG	Accepteert de KB daarnaast een gelijkwaardige officiële verklaring uit een andere EU-lidstaat, zoals een uittreksel uit het nationale strafregister, mits niet ouder dan twaalf maanden?	Nee. De KB verlangt een Nederlandse VOG. Zie het antwoord op vraag 278.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
280.	Programma van Eisen – E28 VOG	Accepteert de KB voor medewerkers die woonachtig zijn in een andere lidstaat van de EU een gelijkwaardig document, zoals een Belgisch uittreksel uit het strafregister? Dient de VOG gedurende de looptijd van de Raamovereenkomst jaarlijks te worden vernieuwd?	Nee, zie het antwoord op vraag 279. De VOG mag op het moment van inzet niet ouder zijn dan twaalf maanden en dient dus jaarlijks te worden vernieuwd.
281.	Programma van Eisen – E29 Toegang tot gegevens	Eis 29 beperkt toegang tot medewerkers die de feitelijke Nadere Opdracht uitvoeren, terwijl Eis 35 controle door een tweede medewerker vereist. Kunt u bevestigen dat medewerkers die senior begeleiding of de verplichte kwaliteitscontrole uitvoeren onder deze toegestane groep vallen en toegang mogen krijgen tot de daarvoor noodzakelijke gegevens en resultaten?	Ja, dat wordt bevestigd.
282.	Programma van Eisen – E31 Methodieken (Rules of Engagement)	Werkt KB met een standaard document voor Rules of Engagement? Zo ja, kan dit document beschikbaar worden gesteld?	De KB heeft hier geen standaard voor.
283.	Programma van Eisen – E32 en E33 Hertesten	E32 Activiteiten, E43 Rapportage, E55 Vaste aanneemsom, E56 Verzwaring of verlichting opdracht Kan Opdrachtgever verduidelijken of en in welke omvang hertesten onderdeel zijn van de oorspronkelijke pentest en vaste aanneemsom, dan wel als afzonderlijke Nadere Opdracht worden verstrekt?	Een hertest maakt geen standaard onderdeel uit van de vaste aanneemsom. De KB geeft per offerteaanvraag aan of een hertest gewenst is. In dat geval neemt Opdrachtnemer de hertest (omvang, termijn en rapportage) op in de offerte.
284.	Programma van Eisen – E32 en E33 Hertesten	Kunt u bevestigen of hertesten onderdeel zijn van de oorspronkelijke opdracht en, zo ja, onder welke voorwaarden en binnen welke omvang?	Zie het antwoord op vraag 283.
285.	Programma van Eisen – E32 en E33 Hertesten	Zijn hertesten na het verhelpen van kwetsbaarheden onderdeel van de vaste aanneemsom van de oorspronkelijke pentest, of worden deze als afzonderlijke Nadere Opdracht aangeboden? Indien hertesten inbegrepen moeten zijn, wilt u de inbegrepen omvang, het aantal hertestrondes en de termijn waarbinnen deze plaatsvinden vaststellen?	Zie het antwoord op vraag 283.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
286.	Programma van Eisen – E32 en E33 Hertesten	Maakt een hertest na herstel van de bevindingen onderdeel uit van de vaste aanneemsom van de oorspronkelijke pentest, of wordt een hertest als afzonderlijke Nadere Opdracht uitgevraagd?	Zie het antwoord op vraag 283.
287.	Programma van Eisen – E32 en E33 Hertesten	E32 Activiteiten, E43 Rapportage, E55 Vaste aanneemsom, E56 Verzwaring of verlichting opdracht Indien hertesten afzonderlijk worden verstrekt, kan Opdrachtgever bevestigen dat daarvoor een uniforme scope, kwaliteitsverwachting, urenbegroting en planning worden vastgesteld?	Zie het antwoord op vraag 283.
288.	Programma van Eisen – E32 en E33 Hertesten	E32 Activiteiten, E43 Rapportage, E55 Vaste aanneemsom, E56 Verzwaring of verlichting opdracht Kan Opdrachtgever bevestigen dat onderzoek naar nieuwe functionaliteit, een gewijzigde architectuur, een gewijzigde scope of nieuwe kwetsbaarheden niet als hertest van de oorspronkelijke bevinding wordt aangemerkt?	Ja, dat wordt bevestigd.
289.	Programma van Eisen – E32 en E33 Hertesten	E32 Activiteiten, E43 Rapportage, E55 Vaste aanneemsom, E56 Verzwaring of verlichting opdracht Indien één of meer hertestrondes in de oorspronkelijke pentest moeten zijn inbegrepen, kan Opdrachtgever verduidelijken welke rapportage of bevestiging na de hertest moet worden opgeleverd?	Zie het antwoord op vraag 283.
290.	Programma van Eisen – E32 en E33 Hertesten	E32 Activiteiten, E43 Rapportage, E55 Vaste aanneemsom, E56 Verzwaring of verlichting opdracht Indien één of meer hertestrondes in de oorspronkelijke pentest moeten zijn inbegrepen, kan Opdrachtgever verduidelijken welke bevindingen voor hertest in aanmerking komen, of uitsluitend aantoonbaar herstelde bevindingen worden onderzocht en welke verificatiediepte wordt verwacht?	Zie het antwoord op vraag 283.
291.	Programma van Eisen – E32 en E33 Hertesten	E32 Activiteiten, E43 Rapportage, E55 Vaste aanneemsom, E56 Verzwaring of verlichting opdracht	Zie het antwoord op vraag 283.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		Indien één of meer hertestrondes in de oorspronkelijke pentest moeten zijn inbegrepen, kan Opdrachtgever het aantal inbegrepen hertestrondes, de maximale omvang van een hertest en de periode waarbinnen de hertest moet plaatsvinden vaststellen?	
292.	Programma van Eisen – E33 Bespreken pentesten	In PvE-eis E33 is bepaald dat iedere pentest wordt afgesloten met een gesprek met de KB en dat de medewerker die eindverantwoordelijk was voor de uitvoering daarbij aanwezig moet zijn. Hieruit blijkt niet of ook de pentester(s) die het onderzoek feitelijk heeft uitgevoerd aan dit gesprek moet deelnemen. Kan de KB bevestigen dat bij de bespreking de pentester(s) aanwezig moet zijn die de pentest daadwerkelijk heeft uitgevoerd? Deze pentester moet de uitgevoerde testwerkzaamheden en bevindingen zelfstandig in het Nederlands kunnen toelichten en vragen van de KB rechtstreeks in het Nederlands kunnen beantwoorden, zonder tussenkomst van een vertaler of uitsluitend een Nederlandstalige projectleider. Zo niet, dan uw motivatie.	Nee, dat is niet vereist. Op grond van E33 is minimaal de medewerker aanwezig die eindverantwoordelijk is voor de uitvoering van de pentest. Het gesprek wordt in het Nederlands gevoerd (zie het antwoord op vraag 202).
293.	Programma van Eisen – E35 Vierogen-principe	Moet de tweede medewerker die de rapportage controleert (vierogen-principe) eveneens voldoen aan E27 en beschikken over een geldige VOG?	Ja. De tweede medewerker die de controle uitvoert, dient te beschikken over een certificering conform E27 en een geldige VOG (E28).
294.	Programma van Eisen – E35 Vierogen-principe	Eis E35 bepaalt dat alle rapportages door een tweede medewerker van Opdrachtnemer moeten worden gecontroleerd. Kan de KB bevestigen dat deze tweede medewerker niet zelfstandig hoeft te beschikken over één van de in E27 genoemde certificeringen, mits de uitvoerende senior pentester wel aan E27 voldoet en de tweede medewerker aantoonbaar beschikt over relevante pentestervaring en voldoende deskundigheid om de technische vierogencontrole uit te voeren?	Nee. Zie het antwoord op vraag 293.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
295.	Programma van Eisen – E35 Vierogen-principe	E35 Vierogen-principe Kan Opdrachtgever bevestigen dat de tweede beoordelaar passende technische ervaring heeft met het betreffende type pentest en dat de controle niet uitsluitend redactioneel of administratief van aard is?	Ja, dat wordt bevestigd.
296.	Programma van Eisen – E35 Vierogen-principe	E35 Vierogen-principe Kan Opdrachtgever verduidelijken wat zij minimaal verstaat onder de vereiste kwaliteitscontrole, waaronder de vierogencontrole, van een pentest en rapportage?	De KB verstaat onder de vierogencontrole een inhoudelijke (technische) controle van de rapportage door een tweede deskundige medewerker, gericht op de juistheid en volledigheid van de bevindingen, de risicoclassificaties en de adviezen. Een uitsluitend redactionele of administratieve controle volstaat niet.
297.	Programma van Eisen – E35 Vierogen-principe	E35 Vierogen-principe Kan Opdrachtgever bevestigen dat de vierogencontrole ten minste omvat dat de consistentie van risico- en impactclassificaties, de technische juistheid en toepasbaarheid van hersteladviezen en de samenhang tussen technisch bewijs, conclusie en advies worden gecontroleerd?	Zie het antwoord op vraag 296.
298.	Programma van Eisen – E35 Vierogen-principe	E35 Vierogen-principe Kan Opdrachtgever bevestigen dat de vierogencontrole ten minste omvat dat wordt geverifieerd dat de afgesproken scope aantoonbaar is getest, dat kritieke en hoge bevindingen technisch zijn gevalideerd en dat de reproduceerbaarheid van bevindingen is gecontroleerd?	Zie het antwoord op vraag 296.
299.	Programma van Eisen – E36 Opslag van data	E36 bepaalt enerzijds dat alle voor de pentesten gebruikte data moet worden opgeslagen op een plaats waar Nederlands recht van toepassing is en anderzijds dat alle data van de KB in Nederland moet worden bewaard. Kan de KB verduidelijken: a. welke gegevens onder “alle data die voor de uitvoering van de pentesten gebruikt wordt” vallen; b. of deze eis ook geldt voor back-ups, logbestanden, metadata, telemetrie en tijdelijk verwerkte gegevens;	a. Alle gegevens van de KB en alle gegevens die bij de uitvoering van de pentesten worden gegenereerd, zoals testresultaten, logbestanden, schermafbeeldingen, tooloutput, accountgegevens en rapportages. b. Ja, voor zover deze gegevens van de KB bevatten. c. Ja, verwerking binnen de EER is toegestaan, mits de data in Nederland wordt opgeslagen.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		c. of verwerking binnen de EER is toegestaan wanneer de data fysiek in Nederland wordt opgeslagen; d. of beheer en toegang vanuit een land buiten Nederland of buiten de EER zijn toegestaan? Bevestigt de KB tevens dat de eis uitsluitend betrekking heeft op gegevens van de KB en uit de pentest voortkomende gegevens, en niet op algemeen beschikbare methodieken, tooling en dreigingsinformatie?	d. Beheer en toegang vanuit een ander land binnen de EER zijn toegestaan; vanuit een land buiten de EER niet. Ja, de eis heeft geen betrekking op algemeen beschikbare methodieken, tooling en dreigingsinformatie.
300.	Programma van Eisen – E36 Opslag van data	Eis 36 : Vallen back ups, beveiligingsloggegevens, metadata, e-mailberichten, ticketsystemen en tijdelijke testbestanden eveneens onder de verplichting dat alle KB gegevens uitsluitend in Nederland worden opgeslagen	Ja, voor zover deze gegevens van de KB bevatten. Zie het antwoord op vraag 299.
301.	Programma van Eisen – E36 Opslag van data	Volstaat een uitsluitend door Opdrachtnemer beheerde tenant bij een cloudprovider met datacenters in Nederland wanneer primaire opslag, back-ups, snapshots en failover uitsluitend in Nederland plaatsvinden, of eist de KB opslag op eigen infrastructuur van Opdrachtnemer?	Ja, mits alle data (inclusief back-ups, snapshots en failover) uitsluitend in Nederland wordt opgeslagen en de omgeving uitsluitend door Opdrachtnemer wordt beheerd.
302.	Programma van Eisen – E36 Opslag van data	Bijlage 1 – Programma van Eisen, Eis 40. U stelt dat de opslag van alle data van de KB binnen Nederland opgeslagen dient te worden. Wij maken gebruik van cloudoplossingen voor bijvoorbeeld e-mail, datatransfer en dossiervorming. Deze oplossingen worden gehost in West-Europa, waar het Europees recht van toepassing is. Staat u er voor open om Eis 36 in lijn met deze inrichting aan te passen?	Nee, dat is niet akkoord. Data van de KB wordt uitsluitend in Nederland opgeslagen, ook wanneer deze via e-mail, bestandsuitwisseling of dossiervorming wordt verwerkt.
303.	Programma van Eisen – E36 en E46 Opslag en verwerking binnen de EER	E36 verlangt opslag van KB gegevens in Nederland, terwijl E46 verwerking binnen de EER toestaat. Kan de KB duidelijk maken welke gegevens uitsluitend in Nederland moeten worden opgeslagen en welke verwerkingen elders binnen de EER zijn toegestaan?	E36 heeft betrekking op de opslag van data: data van de KB wordt uitsluitend in Nederland opgeslagen. E46 heeft betrekking op de overige verwerking: deze mag plaatsvinden binnen de EER. Toegang tot de omgevingen en data van de KB vanuit een ander land binnen de EER is dus toegestaan, mits er geen data van de KB buiten Nederland wordt opgeslagen (bijvoorbeeld

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
			door gebruik te maken van een beveiligde test- of werkomgeving in Nederland). Verwerking en toegang van buiten de EER is niet toegestaan.
304.	Programma van Eisen – E36 en E46 Opslag en verwerking binnen de EER	E36 schrijft voor dat alle data van de KB in Nederland wordt bewaard, terwijl E46 verwerking van gegevens binnen de EER toestaat. Kunt u verduidelijken welke geografische eis prevaleert en bevestigen of verwerking en opslag binnen de EER is toegestaan, mits wordt voldaan aan de overige beveiligings- en privacyvereisten?	Zie het antwoord op vraag 303.
305.	Programma van Eisen – E36 en E46 Opslag en verwerking binnen de EER	E36 vereist dat alle data van de KB wordt bewaard in een beveiligde omgeving in Nederland, terwijl E46 verwerking binnen de EER toestaat. Welke eis is leidend? Is het toegestaan dat pentesters vanuit een andere lidstaat binnen de EER werkzaamheden uitvoeren via een beveiligde omgeving?	Zie het antwoord op vraag 303. Uitvoering vanuit een andere lidstaat binnen de EER is onder deze voorwaarden toegestaan.
306.	Programma van Eisen – E36 en E46 Opslag en verwerking binnen de EER	Is onze aanname correct dat alle voor de opdracht gebruikte pentestapparatuur en infrastructuur die KB-gegevens verwerkt of opslaat, waaronder werkstations, scanservers, virtuele testmachines, lokale AI-tools, rapportagevoorzieningen en back-ups, fysiek in Nederland moeten staan? Wilt u daarbij verduidelijken hoe deze eis zich verhoudt tot verwerking binnen de EER onder E46 en de mogelijkheid om onder artikel 5.4 van de Verwerkersovereenkomst toestemming te geven voor verwerking buiten de EER?	Ja, voor zover op deze apparatuur en infrastructuur data van de KB wordt opgeslagen. Zie verder het antwoord op vraag 303. De KB geeft op voorhand geen toestemming voor verwerking buiten de EER.
307.	Programma van Eisen – E36 en E46 Uitvoering vanuit het buitenland	In PvE-eis E36 is bepaald dat alle data van de KB in Nederland wordt opgeslagen. Op grond van E46 lijkt verwerking van KB-data en daarmee mogelijk ook toegang tot KB-omgevingen vanuit ieder land binnen de EER toegestaan. Pentesten geven medewerkers vergaande toegang tot applicaties, omgevingen, configuraties en informatie over aangetroffen kwetsbaarheden. Kan de KB daarom verduidelijken vanuit welke landen de werkzaamheden mogen worden uitgevoerd en van waaruit toegang tot KB-omgevingen is toegestaan?	De werkzaamheden mogen worden uitgevoerd vanuit landen binnen de EER, onder de voorwaarden zoals beschreven in het antwoord op vraag 303. De KB schrijft niet voor dat de uitvoering uitsluitend vanuit Nederland plaatsvindt. Tijdens de implementatie van de dienstverlening zullen verdere afspraken gemaakt worden over de toegang tot data en beveiliging.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		Gelet op de aard en kwetsbaarheid van de te onderzoeken omgevingen verzoeken wij de KB te overwegen voor te schrijven dat de feitelijke uitvoering van pentesten en de toegang tot KB-omgevingen uitsluitend vanuit Nederland plaatsvinden. Indien de KB uitvoering vanuit andere EER-landen toestaat, verzoeken wij haar toe te lichten: 1. welke beveiligingsvoorwaarden gelden voor toegang vanuit het buitenland; 2. of voorafgaande toestemming van de KB vereist is; 3. of bij iedere offerteaanvraag moet worden vermeld vanuit welk land de werkzaamheden worden uitgevoerd; 4. hoe de KB controleert dat lokaal geen testdata, rapportages, logbestanden, schermafbeeldingen of informatie over kwetsbaarheden worden opgeslagen.	
308.	Programma van Eisen – E36 en E46 Uitvoering vanuit het buitenland	Mogen medewerkers pentestwerkzaamheden op afstand uitvoeren vanuit een andere EU/EER-lidstaat, mits gegevens van de KB uitsluitend in Nederland worden opgeslagen, verwerking binnen de EER plaatsvindt en toegang beveiligd, beperkt en gelogd is?	Ja. Zie het antwoord op vraag 307.
309.	Programma van Eisen – E36 en E46 Uitvoering vanuit het buitenland	Bijlage 1. Programma van Eisen.pdf Dienstverlening algemeen - Is de KB bereid als eis of voorkeur op te nemen dat de uitvoerende pentesters werkzaam zijn vanuit Nederland, zodat kennis van lokale wet- en regelgeving en snelle beschikbaarheid wordt gewaarborgd?	Nee, dat is niet akkoord. Zie het antwoord op vraag 307.
310.	Programma van Eisen – E36 en E46 Uitvoering vanuit het buitenland	Is onze aanname correct dat alle medewerkers die bij de uitvoering toegang hebben tot KB-omgevingen, gegevens of testresultaten, inclusief senior begeleiders, reviewers en eventuele onderaannemers, zich tijdens deze werkzaamheden fysiek in Nederland moeten bevinden? De genoemde eisen bepalen wel de taal, opslaglocatie en verwerking binnen de EER, maar leggen de fysieke werklocatie niet expliciet vast. Indien onze aanname niet correct is, wilt u aangeven vanuit welke landen uitvoering en toegang op afstand zijn toegestaan?	Nee, die aanname is niet correct. Zie het antwoord op vraag 307.
311.	Programma van Eisen – E37 Ernstige kwetsbaarheden	Verwacht de KB bij bevindingen vanaf CVSS-score High ook buiten kantoortijden direct contact? Is er aan de zijde van de KB in dat geval	Ja. Bij bevindingen vanaf CVSS-score High neemt Opdrachtnemer direct telefonisch contact op met de in

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		24/7 een contactpersoon bereikbaar? Wat wordt onder direct contact verstaan. Is een e-mail vanuit een rapportage platform voldoende of dient er telefonisch contact worden opgenomen?	de Nadere Opdracht aangewezen contactpersoon van de KB. Een e-mail via een rapportageplatform volstaat niet. De bereikbaarheid van deze contactpersoon buiten kantooruren wordt per Nadere Opdracht afgestemd. Een e-mail via een rapportageplatform volstaat niet.
312.	Programma van Eisen – E37 Ernstige kwetsbaarheden	Verwacht de KB dat High en Critical kwetsbaarheden ook buiten de bereikbaarheidsuren uit E13 onmiddellijk worden gemeld? Zo ja, welke beschikbaarheid en reactietijd worden van Opdrachtnemer verwacht?	Ja. Zie het antwoord op vraag 311.
313.	Programma van Eisen – E37 Ernstige kwetsbaarheden	In E37 wordt gesproken over ernstige kwetsbaarheden vanaf CVSS High. Welke CVSS versie moet worden toegepast? Moet uitsluitend de basisscore worden gehanteerd of mag de score op basis van dreigingsinformatie en de specifieke bedrijfscontext van de KB worden aangepast?	De KB hanteert de meest recente versie van CVSS (op dit moment CVSS v4.0). Voor E37 is de basisscore leidend. Opdrachtnemer mag daarnaast een op de context van de KB aangepaste score opnemen.
314.	Programma van Eisen – E38 Voorkomen van verstoringen	Indien een pentest moet worden onderbroken door een storing, onvoldoende beschikbaarheid van de omgeving of een ontbrekende randvoorwaarde aan de zijde van de KB, kan de KB bevestigen dat de gevolgen voor planning en benodigde mandagen als scopewijziging worden behandeld?	Indien een onderbreking aantoonbaar het gevolg is van een oorzaak aan de zijde van de KB, treden Partijen in overleg over de gevolgen voor de planning en de kosten, conform eis E56.
315.	Programma van Eisen – E38 Voorkomen van verstoringen	Hoe worden uren en planningsverlies vergoed wanneer werkzaamheden worden stilgelegd als gevolg van een verstoring die niet aan Opdrachtnemer is toe te rekenen?	Zie het antwoord op vraag 314.
316.	Programma van Eisen – E38 Voorkomen van verstoringen	Worden pentesten ook uitgevoerd op productieomgevingen van de KB? Zo ja, kan de KB bevestigen dat zij verantwoordelijk blijft voor actuele back-ups, monitoring en herstel van de geteste omgevingen?	In de regel worden pentesten niet op productieomgevingen uitgevoerd; in uitzonderlijke gevallen kan dit wel voorkomen. De KB blijft dan verantwoordelijk voor de back-ups, monitoring en het herstel van haar eigen omgevingen.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
317.	Programma van Eisen – E38 Voorkomen van verstoringen	Back-ups, herstel en bedrijfscontinuïteit Kan Opdrachtgever bevestigen dat Opdrachtgever vóór aanvang verantwoordelijk is voor adequate back-ups, herstelmogelijkheden, monitoring en bedrijfscontinuïteitsmaatregelen voor de in scope gebrachte systemen? Kan tevens worden bevestigd dat Opdrachtnemer niet verantwoordelijk is voor schade die voorkomen of beperkt had kunnen worden door redelijke back-up- of herstelmaatregelen van Opdrachtgever?	De KB is verantwoordelijk voor de back-ups en herstelmogelijkheden van haar eigen omgevingen (zie het antwoord op vraag 316). Het tweede deel van de vraag wordt bevestigd, mits Opdrachtnemer de KB vooraf nadrukkelijk op het betreffende risico heeft gewezen.
318.	Programma van Eisen – Testautorisatie	Schriftelijke autorisatie en vrijwaring De uitvoering van pentesten kan handelingen omvatten die zonder uitdrukkelijke toestemming ongeautoriseerd of onrechtmatig zouden kunnen zijn. In de ontvangen documenten is geen afzonderlijke pentestautorisatie of waiver opgenomen. Kan Opdrachtgever bevestigen dat voor iedere Nadere Opdracht vóór aanvang een door een bevoegde vertegenwoordiger ondertekende schriftelijke autorisatie en vrijwaring wordt verstrekt, waarin ten minste de testobjecten, IP-adressen, domeinen, systemen, testperiode, toegestane technieken, uitgesloten handelingen, escalatiecontacten, betrokken derde eigenaren en eventuele productiebeperkingen zijn vastgelegd?	Ja. De KB verstrekt voor iedere Nadere Opdracht vóór aanvang een door een bevoegde vertegenwoordiger ondertekende schriftelijke testautorisatie, waarin de scope, testperiode, toegestane en uitgesloten technieken, contactpersonen en eventuele beperkingen zijn vastgelegd. Opdrachtnemer mag hiervoor een eigen model voorstellen; de definitieve inhoud wordt in overleg vastgesteld.
319.	Programma van Eisen – Testautorisatie	Machtiging voor systemen van derden Kan Opdrachtgever bevestigen en garanderen dat Opdrachtgever bevoegd is om toestemming te geven voor het testen van alle in scope gebrachte systemen, applicaties, infrastructuur en gegevens, waaronder systemen die worden gehost of beheerd door derden? Kan tevens worden bevestigd dat Opdrachtgever vóór aanvang alle noodzakelijke toestemmingen van eigenaren, hostingproviders, cloudleveranciers en andere betrokken derden verkrijgt en Opdrachtnemer vrijwaart tegen aanspraken die voortvloeien uit het ontbreken of de onjuistheid van die bevoegdheid of toestemming?	Ja. De KB draagt er zorg voor dat zij bevoegd is toestemming te geven voor het testen van de systemen in scope en verkrijgt vooraf de benodigde toestemming van betrokken derden (zoals hosting- en SaaS-leveranciers). Opdrachtnemer wordt niet aansprakelijk gehouden voor aanspraken van derden die uitsluitend het gevolg zijn van het ontbreken van deze toestemming, mits Opdrachtnemer binnen de geautoriseerde scope en conform de afspraken heeft gehandeld.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
320.	Programma van Eisen – Testautorisatie	Kunt u bevestigen dat opdrachtgever verantwoordelijk is voor het verkrijgen en in stand houden van alle benodigde toestemmingen, autorisaties en goedkeuringen voor het uitvoeren van de overeengekomen pentestwerkzaamheden?	Ja. Zie het antwoord op vraag 319.
321.	Programma van Eisen – Testautorisatie	Een deel van de applicaties en platformen van de KB wordt mogelijk gehost of geleverd door externe hosting-, cloud- of SaaS-leveranciers. Verstrekt de KB per Nadere Opdracht een schriftelijke testautorisatie, inclusief de benodigde toestemming van betrokken derden? En vrijwaart de KB Opdrachtnemer tegen aanspraken van derden wanneer binnen de door de KB geautoriseerde scope is getest?	Zie de antwoorden op de vragen 318 en 319.
322.	Programma van Eisen – Testautorisatie	Wij treffen geen specifieke pentest-vrijwaringsverklaring of toestemmingsverklaring aan, dit is echter wel gangbaar voor het uitvoeren van pentesten. Is de KB bereid voorafgaand aan iedere pentest een dergelijke verklaring te ondertekenen, waarin de KB bevestigt bevoegd te zijn toestemming te verlenen en de benodigde toestemming van eventuele derden te hebben verkregen, en Opdrachtnemer wordt gevrijwaard voor aanspraken wegens het ontbreken van die toestemming, voor zover binnen de gemaakte afspraken wordt gehandeld? Kunt u hiervoor een model beschikbaar stellen?	Zie de antwoorden op de vragen 318 en 319.
323.	Programma van Eisen / Raamovereenkomst – Vrijwaring pentestwerkzaamheden	Kunt u bevestigen dat Opdrachtnemer wordt gevrijwaard voor aanspraken van derden die uitsluitend voortvloeien uit het uitvoeren van de overeengekomen pentestwerkzaamheden overeenkomstig de door de KB verstrekte opdracht, autorisaties en instructies? Indien u hiermee niet kunt instemmen, kunt u dan bevestigen dat Opdrachtnemer niet aansprakelijk is voor aanspraken van derden die uitsluitend voortvloeien uit het uitvoeren van de overeengekomen pentestwerkzaamheden overeenkomstig de door de KB verstrekte opdracht, autorisaties en instructies?	Ja. De KB vrijwaart Opdrachtnemer voor aanspraken van derden die uitsluitend voortvloeien uit het uitvoeren van de overeengekomen pentestwerkzaamheden overeenkomstig de door de KB verstrekte opdracht, testautorisatie en instructies.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
324.	Programma van Eisen / Raamovereenkomst – Vrijwaring pentestwerkzaamheden	Het uitvoeren van een pentest brengt inherent een risico op verstoring of onbeschikbaarheid van systemen mee. Is de KB bereid aansprakelijkheid uit te sluiten voor schade die het gevolg is van overeengekomen testactiviteiten, wanneer deze binnen de afgesproken scope, testvensters en methodiek vakkundig zijn uitgevoerd?	Ja, voor zover de testactiviteiten binnen de overeengekomen scope, testvensters en methodiek vakkundig zijn uitgevoerd en geen sprake is van een toerekenbare tekortkoming van Opdrachtnemer. Zie verder de antwoorden op de vragen 214 en 487.
325.	Programma van Eisen / Raamovereenkomst – Vrijwaring pentestwerkzaamheden	Inherente risico's pentesten Kan Opdrachtgever bevestigen dat pentesten, ook indien zorgvuldig uitgevoerd, kunnen leiden tot tijdelijke verstoring, performanceverlies, uitval, beschadiging of verlies van gegevens? Kan worden bevestigd dat Opdrachtnemer niet aansprakelijk is voor dergelijke inherente gevolgen voor zover Opdrachtnemer binnen de goedgekeurde scope, testvoorwaarden en professionele standaarden handelt, behoudens opzet of grove schuld van Opdrachtnemer?	Zie de antwoorden op de vragen 323 en 324.
326.	Programma van Eisen / Raamovereenkomst – Vrijwaring pentestwerkzaamheden	Voor de gevraagde diensten is het gebruikelijk dat Opdrachtnemer wordt gevrijwaard voor claims van derden (bijvoorbeeld claims van werknemers waar naar persoonsgericht onderzoek wordt verricht, of voor aanspraken van derden op wiens systemen Opdrachtnemer pentesten uitvoert). Daar is in de ontvangen aanbestedingsdocumenten niet in voorzien. Is Opdrachtgever bereid met een dergelijke vrijwaring ten gunste van Opdrachtnemer – zoals te doen gebruikelijk is – in te stemmen?	Gedeeltelijk akkoord. De KB vrijwaart Opdrachtnemer zoals beschreven in het antwoord op vraag 323. Persoonsgericht onderzoek valt niet binnen de scope van de Opdracht (zie het antwoord op vraag 6).
327.	Programma van Eisen / Raamovereenkomst – Vrijwaring pentestwerkzaamheden	"Het is gewenst en gebruikelijk binnen de branche een vrijwaring overeen te komen ten gunste van Opdrachtnemer. Gezien de specifieke dienstverlening die voorziet in het opleveren van een rapportage wat een bepaalde mate van zekerheid (Assurance) biedt en specifiek voor Opdrachtgever wordt opgesteld acht Opdrachtnemer een vrijwaring redelijk maar ook noodzakelijk. Bent u daarom bereid de volgende bepaling overeen te komen: "Opdrachtgever vrijwaart Opdrachtnemer ter zake van alle aanspraken van derden die voortvloeien uit of verband houden met de	Nee, de voorgestelde bepaling wordt niet overgenomen. De KB vrijwaart Opdrachtnemer uitsluitend zoals beschreven in het antwoord op vraag 323.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		ten behoeve van Opdrachtgever (nog te) verrichte(n) werkzaamheden, tenzij deze aanspraken het gevolg zijn van opzet dan wel bewuste roekeloosheid aan de zijde van leidinggevend personeel van Opdrachtnemer. De vrijwaring heeft mede betrekking op alle schade en (proces)kosten die Opdrachtnemer in verband met zulk een aanspraak lijdt of maakt. Deze vrijwaring wordt mede bedongen ten behoeve van de personen binnen het opdrachtteam van Opdrachtnemer, zowel individueel als gezamenlijk." "	
328.	Programma van Eisen / Raamovereenkomst – Vrijwaring pentestwerkzaamheden	De Raamovereenkomst Pentesten bevat geen specifieke vrijwaring voor de uitvoering van penetratietesten. Gelet op de aard van deze werkzaamheden achten wij het gebruikelijk en marktconform om hiervoor een passende contractuele regeling op te nemen. Bij penetratietesten wordt immers, met uitdrukkelijke toestemming van de opdrachtgever, actief geïntervenieerd in IT-systemen, applicaties en infrastructuur. Ondanks het zorgvuldig en gecontroleerd uitvoeren van dergelijke werkzaamheden kan niet volledig worden uitgesloten dat daarbij onbedoeld verstoring, beschadiging of andere schade ontstaat. Dit risico hangt rechtstreeks samen met de aard van de overeengekomen dienstverlening en kan niet zonder meer als een reguliere tekortkoming in de dienstverlening worden aangemerkt. Wij zien daarbij een spanning tussen deze specifieke risico's van pentestwerkzaamheden en de huidige aansprakelijkheidsregeling in de raamovereenkomst, waarin de aansprakelijkheid wordt gekoppeld aan de ARBIT-2022. Hoewel artikel 26 ARBIT-2022 voorziet in aansprakelijkheidsbeperkingen, bevat de raamovereenkomst voor de specifieke risico's die inherent zijn aan geautoriseerde security testing geen passende vrijwaring of nadere risicoverdeling. Artikel 26 ARBIT-2022 bevat bovendien verschillende situaties waarin de aansprakelijkheidsbeperkingen niet gelden. Vraag Is de aanbestedende dienst bereid om de raamovereenkomst aan te vullen met een marktconforme regeling waarin:	Zie de antwoorden op de vragen 323 en 324. Voor de aansprakelijkheidsbeperking, zie het antwoord op vraag 487.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		een vrijwaring wordt opgenomen voor schade en aanspraken van derden die rechtstreeks voortvloeien uit of verband houden met de uitvoering van de overeengekomen pentestwerkzaamheden, voor zover deze werkzaamheden conform de opdracht, scope en instructies van de opdrachtgever zijn uitgevoerd; en een passende beperking van aansprakelijkheid wordt opgenomen die aansluit bij de aard en omvang van pentestwerkzaamheden en bij de daarvoor gebruikelijke verzekerbare risico's?	
329.	Programma van Eisen – E40 Bewaren en vernietigen	Wij achten dit niet relevant voor digitale gegevens. Kunt u deze eis laten vervallen?	Nee, dat is niet akkoord. De eis is ook van toepassing op digitale gegevens.
330.	Programma van Eisen – E40 Bewaren en vernietigen	Is het Opdrachtnemer toegestaan na vernietiging een beperkt dossier te bewaren (scope, testautorisatie, testlogs en eindrapportage) ten behoeve van verantwoording, aansprakelijkheid en ISO-audits? Hanteert de KB een voorgeschreven format voor het Certificate of Destruction?	Ja, Opdrachtnemer mag de opdrachtadministratie (zoals de offerte, Nadere Overeenkomst, testautorisatie en facturen) bewaren, mits deze geen testresultaten of bevindingen bevat. De KB hanteert geen voorgeschreven format voor het Certificate of Destruction. De inhoud hiervan kan verder afgestemd worden tijdens de implementatie van de Raamovereenkomst.
331.	Programma van Eisen – E40 Bewaren en vernietigen	Bijlage 1 – Programma van Eisen, Eis 40. U benoemt dat resultaten en bevindingen uit de pentest maximaal 6 maanden bewaard mogen worden en daarna vernietigd mogen worden. Hiermee kunnen wij niet akkoord gaan. Wij dienen op basis van wettelijke verplichtingen, gedrags- en beroepsregels en onze interne bewaarrichtlijnen een dossier bij te houden. Dit dossier is noodzakelijk om bij eventueel verschil van inzicht de kwaliteit van de test en bevindingen te kunnen reproduceren. Dit mede om - bij verschil van mening - de kwaliteit van onze werkzaamheden te kunnen verdedigen. Wij dragen natuurlijk zorg voor een zeer adequate beveiliging van het dossier, en zijn welwillend om voor KB aanvullende maatregelen te bespreken na gunning. Kunt u akkoord gaan met het buiten toepassing verklaren van deze Eis? Zo nee, waarom niet?	Zie het antwoord op vraag 330. Indien een wettelijk voorschrift de vernietiging verhindert, informeert Opdrachtnemer de KB daarover (artikel 32.3 ARBIT-2022).

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
332.	Programma van Eisen – E41 Inzet AI	Wat verstaat de KB onder "AI-tools die lokaal draaien bij Opdrachtnemer"? Is een volledig door Opdrachtnemer beheerde private omgeving in Nederland toegestaan, zonder gegevensdeling met een externe AI-aanbieder?	Onder 'lokaal draaien bij Opdrachtnemer' verstaat de KB AI-tools die draaien op infrastructuur die in eigendom of exclusief beheer is van Opdrachtnemer (on-premise of dedicated in een datacenter in Nederland), waarbij geen data van de KB met een externe (AI-)aanbieder wordt gedeeld. AI-diensten van externe aanbieders vanuit de cloud zijn niet toegestaan, ook niet binnen een afgeschermd tenant of private omgeving bij een cloudaanbieder.
333.	Programma van Eisen – E41 Inzet AI	Wat verstaat de KB in E41 precies onder AI die lokaal bij Opdrachtnemer draait? Is een volledig afgeschermd, door Opdrachtnemer beheerde private cloudomgeving toegestaan, of moet de verwerking fysiek op eigen apparatuur of in een eigen datacentrum plaatsvinden?	Zie het antwoord op vraag 332.
334.	Programma van Eisen – E41 Inzet AI	In eis E41 wordt cloudgebaseerde AI uitgesloten. Kan de KB verduidelijken of lokaal gehoste AI-oplossingen binnen een afgeschermd Europese cloudomgeving eveneens als cloud-gebaseerd worden beschouwd of onder de toegestane inzet vallen?	Zie het antwoord op vraag 332.
335.	Programma van Eisen – E41 Inzet AI	Wat bedoelt de KB met AI-tools die 'lokaal draaien'? Valt een dedicated, privé gehost model bij een Europese aanbieder daaronder, en vallen AI-functies in commerciële testtools die via de cloud werken onder het verbod?	Zie het antwoord op vraag 332.
336.	Programma van Eisen – E41 Inzet AI	U benoemt in Eis 41 dat het gebruik van AI-tools alleen is toegestaan indien deze 'lokaal draaien bij de opdrachtnemer'. Onze interne AI-tooling maakt gebruik van afgesloten omgevingen, in eigen beheer, in Azure, AWS Bedrock en Google Vertex. Data binnen deze omgeving wordt niet gebruikt voor analyse, training of fine-tuning van de daarin gebruikte modellen. Interacties met de diverse AI-modellen ('gesprekken') worden na 30 dagen verwijderd. Kunt u het gebruik van dergelijke AI-modellen en tools in eigen beheer toestaan?	Nee, dat is niet akkoord. Zie het antwoord op vraag 332.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
337.	Programma van Eisen – E41 Inzet AI	Eis E41 bepaalt dat eventuele AI-tools alleen zijn toegestaan wanneer deze lokaal bij Opdrachtnemer draaien en dat inzet van AI-tools vanuit de cloud niet is toegestaan. Kan de KB bevestigen dat aan E41 wordt voldaan wanneer een bij Inschrijving opgegeven Onderaannemer onderdelen van de pentest uitvoert en daarbij AI-tools lokaal op de eigen, beheerde infrastructuur van deze Onderaannemer gebruikt, waarbij geen gegevens via een publieke AI- of clouddienst worden verwerkt en Opdrachtnemer volledig verantwoordelijk blijft voor de uitvoering en naleving van de overige beveiligingseisen?	Ja, dat wordt bevestigd, mits ook de Onderaannemer voldoet aan het antwoord op vraag 332.
338.	Programma van Eisen – E41 Inzet AI	Geldt het verbod op cloud-AI uitsluitend voor de technische uitvoering van de pentest, of ook voor rapportage, vertaling, kwaliteitscontrole en administratieve ondersteuning?	Het verbod geldt voor alle inzet van AI waarbij data van de KB wordt verwerkt, dus ook voor rapportage, vertaling, kwaliteitscontrole en administratieve ondersteuning.
339.	Programma van Eisen – E41 Inzet AI	Heeft het verbod in E41 uitsluitend betrekking op AI voorzieningen, of verbiedt de KB ook andere beveiligde cloudvoorzieningen voor planning, dossiervorming, samenwerking en rapportage?	E41 heeft uitsluitend betrekking op AI-voorzieningen. Voor de opslag van data van de KB in overige (cloud)voorzieningen is eis E36 van toepassing.
340.	Programma van Eisen – E41 Inzet AI	Geldt het verbod op inzet van AI-tools vanuit de cloud ook voor gangbare pentesttools met een cloudcomponent zonder AI-functionaliiteit (zoals Burp Collaborator, online vulnerability-feeds en scanner-updates)? En geldt het ook voor AI-functionaliiteit in kantoorsoftware binnen een EU-tenant die wordt gebruikt voor rapportage, zonder dat testdata van de KB wordt verwerkt?	Nee, E41 heeft geen betrekking op tools zonder AI-functionaliiteit; voor de opslag van data is E36 van toepassing. Ja, het verbod geldt ook voor AI-functionaliiteit in kantoorsoftware, indien daarmee data van de KB (zoals rapportages) wordt verwerkt. Zie ook het antwoord op vraag 338.
341.	Programma van Eisen – E41 Inzet AI	Als ervaren pentestpartner voor vele NL-organisaties (ook in de publieke sector) vergelijkbaar met de KB, herkennen we dat toepassen van AI i.v.m. informatiebeveiliging vooralsnog weinig tot geen baat biedt, danwel juist recent risico's oplevert. Bent u bereid tot uitsluiten van het gebruik van AI voor de komende periode?	Nee, dat is niet akkoord. Inzet van AI is toegestaan onder de voorwaarden van E41.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
342.	Programma van Eisen – E41 Inzet AI	Kan de KB toelichten welke aspecten van AI-gebruik tijdens pentesten en rapportages worden meegewogen in de beoordeling, en of hiervoor specifieke randvoorwaarden of beperkingen gelden, buiten de genoemde eis in E41?	De inzet van AI wordt integraal beoordeeld binnen G1.1 (zie het antwoord op vraag 96). Naast E41 zijn de eisen ten aanzien van de opslag van data (E36) van toepassing.
343.	Programma van Eisen – E41 Inzet AI	G1.1 AI-gebruik Indien Opdrachtnemer AI-ondersteunde tooling gebruikt bij analyse, prioritering of rapportage, kan Opdrachtgever bevestigen dat dit is toegestaan mits menselijke controle plaatsvindt, geen vertrouwelijke informatie of Persoonsgegevens worden gebruikt voor het trainen van generieke modellen en de toepasselijke beveiligings- en privacyvereisten worden nageleefd? Kan tevens worden bevestigd dat Opdrachtnemer geen absolute garantie hoeft te geven dat AI-ondersteunde output volledig foutloos is?	Ja, mits wordt voldaan aan E41 en E36. Opdrachtnemer blijft volledig verantwoordelijk voor de juistheid van de opgeleverde resultaten, ook indien AI is ingezet.
344.	Programma van Eisen – E42 Testen op locatie	(a) Bevestigt de KB dat pentesten standaard op afstand worden uitgevoerd en dat uitvoering op locatie uitsluitend verplicht is wanneer dit expliciet in de offerteaanvraag staat? (b) Kan de KB een indicatie geven van het verwachte aandeel pentesten op locatie, de redenen daarvoor en de locatie(s)? (c) Biedt de KB voor interne testen een remote toegang (bijvoorbeeld VPN of een jumphost), zodat testen op locatie tot een minimum beperkt blijven?	a. Ja, dat wordt bevestigd. b. Nee, de KB kan hiervan geen indicatie geven. c. Dit zal per Nadere Opdracht afgestemd worden tussen Partijen.
345.	Programma van Eisen – E42 Testen op locatie	Kan opdrachtgever een inschatting geven van het aantal opdrachten welke op locatie van de KB uitgevoerd zou moeten worden?	Zie het antwoord op vraag 344, onderdeel b.
346.	Programma van Eisen – E42 Testen op locatie	Op welke locaties van de KB kunnen pentesten op locatie plaatsvinden, waarvoor geen reis- en verblijfskosten in rekening mogen worden gebracht?	Pentesten op locatie vinden plaats op de locatie van de KB in Den Haag (op dit moment Prins Willem-Alexanderhof 5).
347.	Programma van Eisen – E42 Testen op locatie	E42 Testen op locatie, E54 All-in tarieven E42 bepaalt dat pentesten op locatie kunnen worden uitgevoerd en dat reis- en verblijfskosten niet afzonderlijk in rekening mogen worden gebracht. Kan Opdrachtgever voor een uniforme calculatie aangeven	Zie het antwoord op vraag 344. Voor de locatie, zie het antwoord op vraag 346.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		welk indicatief aandeel van de Nadere Opdrachten geheel of gedeeltelijk op locatie wordt uitgevoerd en welke locatie of locaties van toepassing zijn?	
348.	Programma van Eisen – E42 Testen op locatie	E42 Testen op locatie, E54 All-in tarieven Indien informatie over de verwachte on-site-inzet niet beschikbaar is, kan Opdrachtgever een uniforme calculatieaannee opnemen, zodat alle Inschrijvers de gevolgen van on-site-inzet op dezelfde basis verwerken?	Nee, de KB neemt geen calculatieaannee op. Zie het antwoord op vraag 344.
349.	Programma van Eisen – E42 Testen op locatie	E42 Testen op locatie, E54 All-in tarieven Kan Opdrachtgever aangeven of aanwezigheid buiten reguliere werktijden kan worden gevraagd en voor welke activiteiten aanwezigheid op locatie kan worden verlangd?	Zie het antwoord op vraag 219. Aanwezigheid op locatie kan worden verlangd indien dit voor de uitvoering van de pentest vereist is.
350.	Programma van Eisen – E42 Testen op locatie	E42 Testen op locatie, E54 All-in tarieven Kan Opdrachtgever aangeven hoeveel medewerkers doorgaans op locatie aanwezig moeten zijn en hoeveel aaneengesloten dagen aanwezigheid doorgaans wordt verwacht?	Dit verschilt per Nadere Opdracht en wordt in de offerteaanvraag aangegeven.
351.	Programma van Eisen – E42 Testen op locatie	Als niet wordt gewerkt op locatie van de KB, is het voor ons mogelijk om op ons kantoor in een strikt gescheiden en afgesloten ruimte de pentestwerkzaamheden uit te voeren, iets wat voor ons als ervaren pentestpartner en onze opdrachtgevers heel gebruikelijk is. Deze professionaliteit vinden wij ook gepast bij KB. Bent u bereid deze mogelijkheid als eis toe te voegen?	Nee, hier wordt geen aanvullende eis voor opgenomen.
352.	Programma van Eisen – E43 Inhoud rapportage	Deze eis lijkt op het gebied van de managementsamenvatting tegenstrijdig met E17. Kunt u dit toelichten?	Er is geen sprake van tegenstrijdigheid. De managementsamenvatting (E43) maakt onderdeel uit van de rapportage per pentest. De managementinformatie (E17) betreft een overzicht over alle uitgevoerde pentesten.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
353.	Programma van Eisen – E43 Inhoud rapportage	E43 vraagt om een overzicht van aangeleverde tokens, accountnamen en wachtwoorden. Kan de KB bevestigen dat daadwerkelijke wachtwoorden, tokens en andere actieve geheimen niet in het rapport hoeven te worden opgenomen en dat een geredigeerd overzicht of verwijzing naar gebruikte testaccounts volstaat?	Ja, dat wordt bevestigd.
354.	Programma van Eisen – E43 Inhoud rapportage	In E43 wordt gevraagd om in de rapportage aangeleverde accountinformatie, waaronder tokens en wachtwoorden, op te nemen. Kunt u bevestigen dat het vanuit informatiebeveiligingsoogpunt voldoende is om gebruikte accounts en typen authenticatiemiddelen te vermelden, waarbij wachtwoorden, tokens en andere authenticatiegeheimen niet integraal in de rapportage worden opgenomen?	Ja. Zie het antwoord op vraag 353.
355.	Programma van Eisen – E43 Inhoud rapportage	M.b.t. Methodologie en Testprocedures: "Overzicht van aangeleverde accountinformatie (zoals tokens, accountnamen en passwords)"; Accountinformatie zoals tokens en wachtwoorden worden normaliter niet letterlijk in het rapport opgenomen in verband met de gevoelige aard van deze gegevens. Wenst de opdrachtgever een beschrijving van deze gegevens of daadwerkelijk de gebruikte tokens en wachtwoorden?	Zie het antwoord op vraag 353.
356.	Programma van Eisen – E43 Inhoud rapportage	Eis 43 verlangt een overzicht van accountinformatie, waaronder tokens en wachtwoorden, in de rapportage. Kunt u bevestigen dat accountnamen en rollen mogen worden vermeld, terwijl wachtwoorden, tokens en andere authenticatiegeheimen worden weggelaten, zodat de rapportage geen bruikbare toegangsgegevens bevat?	Ja. Zie het antwoord op vraag 353.
357.	Programma van Eisen – E43 Inhoud rapportage	M.b.t. Overzicht van Bevindingen: "Prioritering van de kwetsbaarheden op basis van de waarschijnlijkheid van exploitatie en de impact op het systeem"; Is de impliciete prioritering aan de hand van de CVSS score hiervoor	Nee. Een prioritering uitsluitend op basis van de CVSS-score is niet voldoende; de KB verwacht dat bij de prioritering ook de context van de KB wordt meegenomen. De wijze van presenteren is aan Opdrachtnemer.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		adequaat of wenst opdrachtgever een separaat veld of overzicht van een prioritering?	
358.	Programma van Eisen – E43 Inhoud rapportage	Kan de KB verduidelijken welk detailniveau wordt verwacht voor configuratie instellingen van gebruikte hulpmiddelen en scripts (eis 43)? Mag informatie die bedrijfsvertrouwelijk is of de beveiliging van de testinfrastructuur kan schaden worden beperkt tot de voor reproduceerbaarheid noodzakelijke informatie?	Ja. Opdrachtnemer neemt de informatie op die noodzakelijk is voor de reproduceerbaarheid van de bevindingen. Bedrijfsvertrouwelijke informatie die daarvoor niet noodzakelijk is, hoeft niet te worden opgenomen.
359.	Programma van Eisen – E43 Inhoud rapportage	M.b.t. Communicatie en Incidentbeheer: Hoort deze informatie/evaluatie niet beter thuis in de eerder genoemde managementrapportage?	Nee. Deze informatie heeft betrekking op de betreffende pentest en hoort daarom in de rapportage thuis.
360.	Programma van Eisen – E43 Inhoud rapportage	Hanteert de Aanbestedende dienst een vaste maximale oplevertermijn voor het concept- en definitieve pentestrapport na afronding van de technische testwerkzaamheden, of worden deze termijnen per Nadere Opdracht overeengekomen?	De termijnen worden per Nadere Opdracht in de offerte (planning) vastgelegd.
361.	Programma van Eisen – E44 Veilig delen van rapportages	Welke minimale technische en organisatorische criteria hanteert de KB voor goedkeuring van het mechanisme voor beveiligde bestandsuitwisseling? Kan ook gebruik worden gemaakt van een door de KB beschikbaar gestelde voorziening?	De KB verwacht hierbij minimaal: een versleutelde verbinding (HTTPS), multifactorauthenticatie (MFA), versleuteling van opgeslagen gegevens (encryption at rest), opslag in Nederland en een zo kort mogelijke bewaartermijn (minimale dataretentie). De KB kan niet garanderen dat gebruik kan worden gemaakt van een voorziening van de KB, maar is bereid dit tijdens de implementatie van de Raamovereenkomst te bespreken.
362.	Programma van Eisen – E44 Veilig delen van rapportages	Welke eisen stelt de KB aan het mechanisme voor het beveiligd uitwisselen van bestanden, en welke platformen accepteert de KB in ieder geval?	Zie het antwoord op vraag 361.
363.	Programma van Eisen – E50 Audit	Bijlage 1 – Programma van Eisen, Eis 50. Opdrachtnemer dient mee te werken aan een audit en alle informatie hiervoor ter beschikking te	Nee, dat is niet akkoord. De KB wenst de auditmogelijkheden (E50 en artikel 5 ARBIT-2022) niet verder in te perken. De KB mag maximaal één audit per

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		stellen en toegang te verschaffen tot de gebruikte systemen etc. Hiermee kunnen wij niet instemmen. Wij kunnen opdrachtgever geen onbeperkte toegang verlenen tot onze locaties en systemen (i.v.m. de geheimhoudingsverplichtingen jegens onze (andere) klanten) en werknemers. Kunt u akkoord gaan met het buiten toepassing verklaren van deze Eis van de raamovereenkomst, en te vervangen door een bepaling dat opdrachtnemer aan opdrachtgever op verzoek de informatie zal verschaffen die voorziet in de informatiebehoefte van Opdrachtgever, en dat een dergelijk verzoek niet op onredelijke grond geweigerd zal worden.	jaar laten uitvoeren. Eis E50 gaat daarbij voor artikel 5.3 ARBIT-2022. De KB zal de kosten voor uitvoering van de audit initieel zelf dragen. Indien bij de audit gebreken worden geconstateerd, worden de kosten van de audit doorbelast aan Opdrachtnemer. Deze kostenregeling wordt in de definitieve Raamovereenkomst verwerkt.
364.	Programma van Eisen – E52 Overdracht	U benoemt: "Opdrachtnemer draagt zorg voor een adequate overdracht van alle relevante gegevens aan de KB of een door de KB aan te wijzen derde partij". Doelt u met deze Eis op de eindrapportage van een opdracht? Zo nee, kan u dan nader duiden wat u bedoelt, en aanvullend een bepaling op te nemen dat deze overdracht niet geldt voor data en zaken waarvoor overdracht de commerciële belangen van opdrachtnemer zou schaden. Onze overweging is dat "alle relevante gegevens" een formulering zonder beperking is. Wij voeren testen uit deels met programmatuur die door onszelf zijn ontwikkeld en intellectueel eigendom zijn van opdrachtnemer. Wij achten het bezwaarlijk dat bijvoorbeeld deze zaken vanuit commerciële vertrouwelijkheid binnen scope van de overdracht zouden kunnen vallen.	Hiermee wordt bedoeld op de gegevens die Opdrachtnemer in het kader van de Opdracht van of voor de KB heeft verzameld of vervaardigd, zoals rapportages, bevindingen en opdrachtdocumentatie. De tooling en intellectuele eigendomsrechten van Opdrachtnemer (artikel 8.1 sub b ARBIT-2022) vallen hier niet onder.
365.	Programma van Eisen – E55 Kosten van pentesten	Artikel 3.1 verwijst naar '(uur)tarieven', terwijl Eis 55 een vaste aanneemsom voorschrijft op basis van het aangeboden mandagtarief van acht uur. Is onze aanname correct dat iedere Nadere Opdracht wordt aangeboden en afgerekend tegen een vooraf overeengekomen vaste prijs, waarbij de uren/mandagen uitsluitend de calculatie onderbouwen en geen afrekening op werkelijk bestede uren plaatsvindt? Wilt u artikel 3.1 hiermee in overeenstemming brengen?	Ja, die aanname is correct. Artikel 3.1 van de Raamovereenkomst wordt hiermee in overeenstemming gebracht.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
366.	Programma van Eisen – E55 Kosten van pentesten	Artikel 3.1 van de concept Raamovereenkomst spreekt van (uur)tarieven, terwijl E55 uitgaat van een tarief per mandag van 8 uur. Welke eenheid is leidend? Is het toegestaan in de offerte per Nadere Opdracht ook halve mandagen te begroten?	Het tarief per mandag (8 uur) is leidend; zie ook het antwoord op vraag 365. Het is toegestaan halve mandagen (4 uur) te begroten, mits dit gebaseerd is op het aangeboden tarief per mandag.
367.	Programma van Eisen – E56 Meer-/minderkosten	Binnen welke termijn reageert de KB op een onderbouwd voorstel voor meerwerk? Hoe wordt meerwerk behandeld wanneer de oorzaak bij de KB ligt, bijvoorbeeld door onvolledige informatie tijdens de inventarisatie?	De reactietermijn verschilt per situatie; de KB kan deze niet op voorhand vaststellen. Meerwerk waarvan de oorzaak aan de zijde van de KB ligt, wordt behandeld conform eis E56 (zie ook het antwoord op vraag 314).
368.	Programma van Eisen – E57 Facturatieschema	De tweede termijn van 50% is factureerbaar nadat de rapportage gezamenlijk is doorgenomen. Binnen welke termijn na oplevering van de rapportage plant de KB deze bespreking in? Is de KB bereid te bepalen dat de tweede termijn factureerbaar is indien de bespreking door een oorzaak aan de zijde van de KB niet binnen 15 werkdagen na oplevering heeft plaatsgevonden?	Gedeeltelijk. De KB is bereid te bepalen dat de tweede termijn van 50% factureerbaar is indien de bespreking van de rapportage door een oorzaak aan de zijde van de KB niet binnen twintig werkdagen na oplevering van de rapportage heeft plaatsgevonden. Het moment van de bespreking wordt per Nadere Opdracht in de planning van de offerte vastgelegd.
369.	Programma van Eisen – E57 Facturatieschema	Volgens E57 mag de tweede 50% worden gefactureerd nadat Partijen de rapportage gezamenlijk hebben doorgenomen. Wanneer de bespreking door omstandigheden aan de zijde van de KB wordt uitgesteld, wordt ook de facturatie uitgesteld. Binnen welke termijn na oplevering van de rapportage vindt deze bespreking plaats? Bevestigt de KB dat Opdrachtnemer de tweede 50% mag factureren wanneer de bespreking door omstandigheden aan de zijde van de KB niet binnen tien werkdagen na oplevering heeft plaatsgevonden?	Nee. De KB hanteert een termijn van twintig werkdagen; zie het antwoord op vraag 368.
370.	Programma van Eisen – E57 Facturatieschema	Volgens artikel 11.1 ARBIT-2022 is betaling voorafgaand aan Acceptatie niet verschuldigd, terwijl E57 toestaat dat 50% van de kosten bij start van de Nadere Opdracht wordt gefactureerd. Kan de KB bevestigen dat E57 voorgeeft en dat de eerste termijn van 50% niet onder een opschortende voorwaarde staat?	Ja, dat wordt bevestigd.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
371.	Programma van Eisen – E62 Verrekening	Opdrachtgever kan alleen van de mogelijkheid tot verrekening gebruik maken als is voldaan aan artikel 127 Boek 6 Burgerlijk Wetboek en Opdrachtnemer de verschuldigdheid en de omvang van het te verrekenen bedrag schriftelijk heeft erkend. Is Opdrachtgever hiermee akkoord?	Nee, dat is niet akkoord.
372.	Bijlage 2 – Invulbijlage referenties	De nummering in Bijlage 2 bevat tweemaal nummer 3. Kunt u een gecorrigeerde invulbijlage publiceren, dan wel bevestigen dat dit een kennelijke redactionele fout is zonder gevolgen voor de geldigheid van de inschrijving?	Dit betreft een kennelijke redactionele fout, zonder gevolgen voor de geldigheid van de Inschrijving.
373.	Bijlage 2 – Invulbijlage referenties	Kunt u bevestigen dat bij vraag 1 van Bijlage 2 letterlijk kan worden vermeld: “Kerncompetentie 1” en/of “Kerncompetentie 2”, zoals omschreven in paragraaf 4 van het Beschrijvend Document?	Ja, dat wordt bevestigd.
374.	Bijlage 2 – Invulbijlage referenties	Kunt u bevestigen dat bij onderdeel 1 met competentie(s) wordt gerefereerd aan de 2 kerncompetenties die beschreven worden in het Beschrijvend Document?	Ja. Zie het antwoord op vraag 373.
375.	Bijlage 2 – Invulbijlage referenties	Op het referentie invulformulier hoeft nergens de naam van de inschrijvende partij te worden genoemd. Kunt u dit toelichten en, desnoods, een nieuw formulier beschikbaarstellen waarop inschrijver haar naam wel kan noemen?	Het is niet nodig de naam van Inschrijver te vermelden; de referentieverklaring wordt als onderdeel van de Inschrijving via TenderNed ingediend.
376.	Bijlage 2 – Invulbijlage referenties	Kunt u bevestigen dat Bijlage 2 een referentieopgave van Inschrijver betreft en niet door de refererende organisatie hoeft te worden ondertekend?	Ja, dat wordt bevestigd.
377.	Bijlage 2 – Invulbijlage referenties	In paragraaf 4 staat dat lopende referentieopdrachten mogen worden ingediend. Bijlage 2 vraagt echter verplicht om een einddatum en een reden van beëindiging. Kunt u bevestigen dat inschrijvers bij een lopende referentie “lopend” mogen invullen bij einddatum en “niet van toepassing” bij reden beëindiging?	Ja, dat wordt bevestigd.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
378.	Bijlage 2 – Invulbijlage referenties	Kunt u bevestigen dat “reden beëindiging” bij regulier afgeronde opdrachten mag worden ingevuld als “contractueel afgerond” en bij lopende opdrachten als “niet van toepassing”?	Ja, dat wordt bevestigd.
379.	Bijlage 2 – Invulbijlage referenties	Bevestigt de KB dat geen minimale contractwaarde of minimale jaaromzet geldt voor de referentieopdrachten, ondanks de velden "Contractwaarde van de gehele opdracht" en "Omzetbedrag per jaar" in Bijlage 2, en dat voor een lopende opdracht de tot dusver gerealiseerde waarde mag worden opgegeven?	Ja, dat wordt bevestigd. Er geldt geen minimale contractwaarde of omzet. De velden dienen ter informatie. Onder de contractwaarde verstaat de KB de (geschatte) waarde van de pentestwerkzaamheden waarop de referentie betrekking heeft; bij een lopende opdracht de tot dusver gerealiseerde waarde. Een onderbouwde schatting is toegestaan.
380.	Bijlage 2 – Invulbijlage referenties	Kunt u toelichten wat bij Bijlage 2 wordt bedoeld met “contractwaarde van de gehele opdracht”: de totale gecontracteerde waarde van de volledige overeenkomst, de daadwerkelijk gerealiseerde omzet, of uitsluitend de waarde van de pentestwerkzaamheden waarop de referentie betrekking heeft?	Zie het antwoord op vraag 379.
381.	Bijlage 2 – Invulbijlage referenties	Kunt u toelichten waarom op het referentie invulformulier de Contractwaarde van de gehele opdracht en het omzetbedrag per jaar moeten worden vermeld? Zijn er (minimale of maximale) omvangseisen eisen aan de referentie(s) verbonden?	Nee, er zijn geen omvangseisen verbonden aan de referenties. Zie het antwoord op vraag 379.
382.	Bijlage 2 – Invulbijlage referenties	Het referentieformulier vraagt de contractwaarde van de gehele opdracht en het omzetbedrag per jaar. Voor de kerncompetenties is echter geen minimale financiële omvang voorgeschreven. Bent u bereid deze financiële velden te verwijderen en een aangepast formulier te publiceren? Indien niet, kunt u bevestigen dat deze velden met ‘niet van toepassing’ mogen worden ingevuld en geen rol spelen bij de toetsing van de referenties?	Nee, de velden worden niet verwijderd en mogen niet met ‘niet van toepassing’ worden ingevuld. Zie het antwoord op vraag 379.
383.	Bijlage 2 – Invulbijlage referenties	In Bijlage 2 wordt gevraagd naar de contractwaarde van de gehele referentieopdracht en het omzetbedrag per jaar.	Ja. Zie het antwoord op vraag 379.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		Is een onderbouwde schatting toegestaan wanneer de exacte contractwaarde tussen de eindklant en de detacheerder niet bij Inschrijver bekend is?	
384.	Bijlage 2 – Invulbijlage referenties	In Bijlage 2 wordt gevraagd naar de contractwaarde van de gehele referentieopdracht en het omzetbedrag per jaar. Indien meerdere pentesten zijn uitgevoerd binnen een langdurige detacheringsopdracht, dient Inschrijver dan de totale contractwaarde van de detacheringsopdracht op te geven, of uitsluitend de waarde van de daadwerkelijk uitgevoerde pentesten?	Zie het antwoord op vraag 379.
385.	Bijlage 2 – Invulbijlage referenties	Bijlage 2 - Format Referentieopdracht. U benoemt in het format de velden "Contractwaarde van de gehele opdracht" en "Omzetbedrag per jaar". Wij kunnen niet goed duiden wat u met deze bedragen bedoelt, kan u de definities nader duiden? Indien u verwacht dat wij de commerciële waarde van een raamcontract per jaar benoemen, dan verzoeken wij u dit veld te verwijderen. Dit is commercieel vertrouwelijke informatie die niets zegt over de complexiteit of omvang van sec de referentieopdracht.	Zie het antwoord op vraag 379.
386.	Bijlage 2 – Invulbijlage referenties	Kunt u bevestigen dat een overzicht van de minimaal vier uitgevoerde pentesten, met maand/jaar en beknopte omschrijving, in het veld "Omschrijving aard van opdracht" mag worden opgenomen?	Ja, dat wordt bevestigd.
387.	Bijlage 2 – Invulbijlage referenties	Is het toegestaan om in de referentieverklaring gevoelige klantinformatie te anonimiseren?	Ja, voor de beschrijving van de uitgevoerde opdracht is dat toegestaan. De contactgegevens van de referent dienen wel volledig te worden verstrekt.
388.	Bijlage 3A – Raamovereenkomst (nummering)	De nummering van de concept Raamovereenkomst bevat onder meer artikelleden 4.2 tot en met 4.4 onder hoofdstuk 3 en tweemaal artikel 5.1. Kan de KB vóór inschrijving een gecorrigeerde versie publiceren?	Ja. De nummering wordt in de definitieve Raamovereenkomst hersteld.
389.	Bijlage 3A – Raamovereenkomst art. 1.1	1.1 en proces Nadere Overeenkomsten	Gedeeltelijk. Opdrachtnemer is in beginsel verplicht een Offerte uit te brengen. Uitsluitend indien een

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		Opdrachtnemer is verplicht naar aanleiding van iedere Offerteaanvraag een Offerte uit te brengen, terwijl Opdrachtgever geen afnameverplichting heeft. Kan Opdrachtgever bevestigen dat Opdrachtnemer een Offerteaanvraag gemotiveerd mag afwijzen indien deze buiten de scope van de Raamovereenkomst valt, onvoldoende informatie bevat, niet uitvoerbaar is binnen de gevraagde termijn, strijdig is met professionele of wettelijke verplichtingen, of indien onvoldoende gekwalificeerde capaciteit beschikbaar is? Kan tevens worden bevestigd dat uitsluitend een door beide Partijen ondertekende Nadere Overeenkomst tot een bindende opdracht leidt?	Offerteaanvraag buiten de scope van de Raamovereenkomst valt, niet uitvoerbaar is binnen de door de KB gevraagde termijnen of in strijd is met professionele of wettelijke verplichtingen, kan Opdrachtnemer deze gemotiveerd afwijzen. Een Nadere Overeenkomst komt tot stand op het moment dat de offerte door de KB is ondertekend (E22).
390.	Bijlage 3A – Raamovereenkomst art. 1.2 Model Nadere Overeenkomst	Artikel 1.2 verwijst naar een als bijlage opgenomen Model Nadere Overeenkomst. Dit model treffen wij niet aan in de aangeleverde stukken. Wilt u dit beschikbaar stellen en verduidelijken of ondertekening van de offerte overeenkomstig E22 voldoende is om een Nadere Overeenkomst tot stand te brengen, of dat daarnaast een afzonderlijk model moet worden ondertekend?	Er wordt geen afzonderlijk model Nadere Overeenkomst gehanteerd. De Nadere Overeenkomst komt tot stand door ondertekening van de offerte door de KB (E22). Artikel 1.2 van de Raamovereenkomst wordt hierop aangepast.
391.	Bijlage 3A – Raamovereenkomst art. 1.3 Rangorde	De Nadere Overeenkomst en de Raamovereenkomst zijn in rangorde boven de Nota van inlichtingen geplaatst, terwijl de Nota van Inlichtingen specifiek afwijkingen worden voorgesteld. Het is derhalve logisch (en gebruikelijk) dat de Nota van Inlichtingen in rangorde boven de Nadere Overeenkomst komen te staan. Kunt u dit aanpassen?	Nee, dat is niet akkoord. De wijzigingen naar aanleiding van de Nota's van Inlichtingen worden verwerkt in de definitieve Raamovereenkomst (zie paragraaf 3.2 van het Beschrijvend document). Er ontstaat daardoor geen tegenstrijdigheid.
392.	Bijlage 3A – Raamovereenkomst art. 1.3 Rangorde	Uit dit artikel blijkt dat de overeenkomst, prevaleren boven de Nota's van Inlichtingen (Nvl), terwijl partijen tijdens de vragenronde en via de Nvl's de mogelijkheid krijgen om aanpassingen op de overeenkomst overeen te komen. Kunt u bevestigen dat de afwijkingen die partijen overeenkomen in de Nvl, worden verwerkt in de overeenkomst? Indien u dat niet kunt bevestigen, wensen wij de Nvl's in rang boven de overeenkomst, nadere overeenkomsten en verwerkersovereenkomst te plaatsen. Gaat u hiermee akkoord?	Ja, dat wordt bevestigd. Zie het antwoord op vraag 391.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
393.	Bijlage 3A – Raamovereenkomst art. 1.3 Rangorde	Kunt u bevestigen dat alle wijzigingen en verduidelijkingen uit de Nota's van Inlichtingen worden verwerkt in de definitieve Raamovereenkomst en eventuele modellen voor Nadere Overeenkomsten, zodat de hogere rangorde van deze overeenkomsten niet tot gevolg heeft dat eerdere teksten voorgaan op de antwoorden uit de Nota's van Inlichtingen?	Ja, dat wordt bevestigd. Zie het antwoord op vraag 391.
394.	Bijlage 3A – Raamovereenkomst art. 1.3 Rangorde	1.3 documentrangorde De Nadere Overeenkomst en Raamovereenkomst prevaleren boven de Nota's van Inlichtingen, terwijl geaccepteerde wijzigingen en verduidelijkingen in de Nota's van Inlichtingen de contractuele positie behoren te bepalen. Kan Opdrachtgever bevestigen dat antwoorden uit de Nota's van Inlichtingen die een hoger gerangschikt document verduidelijken, beperken of wijzigen, in de definitieve Raamovereenkomst en het Model Nadere Overeenkomst worden verwerkt en bij tegenstrijdigheid prevaleren boven eerdere versies van de betreffende bepalingen?	Ja, dat wordt bevestigd. Zie het antwoord op vraag 391. Er wordt geen afzonderlijk model Nadere Overeenkomst gehanteerd (zie het antwoord op vraag 390).
395.	Bijlage 3A – Raamovereenkomst art. 1.3 Rangorde	De 'Model Nadere Overeenkomst ARBIT-2022' waarnaar artikel 1.2 van de concept Raamovereenkomst verwijst, is niet gepubliceerd. Wil de KB dit model publiceren? Daarnaast wijkt de rangorde in artikel 1.3 van de concept Raamovereenkomst af van die in §7.13 van het Beschrijvend document. Welke rangorde is leidend?	Zie voor het model het antwoord op vraag 390. De rangorde in artikel 1.3 van de Raamovereenkomst is leidend; zie ook het antwoord op vraag 391.
396.	Bijlage 3A – Raamovereenkomst art. 2.4 Verlenging	De overeenkomst kan eenzijdig door u worden verlengd. Wij wensen de mogelijkheid te hebben een verlenging te weigeren. Onder omstandigheden kan in redelijkheid niet van ons verwacht worden in te stemmen met een verlenging. Wij stellen voor aan artikel 2.2 de volgende zin toe te voegen: “Het staat Opdrachtnemer vrij deze verlenging te weigeren.”	Nee, dat is niet akkoord.
397.	Bijlage 3A – Raamovereenkomst art. 3 Prijs en tarieven	3.1 en tarieven	Ja, met inachtneming van eis E56. Het aangeboden tarief per mandag blijft daarbij van toepassing.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		Kan Opdrachtgever bevestigen dat de aangeboden tarieven uitsluitend gelden voor de in de Aanbestedingsstukken omschreven scope en uitgangspunten en dat aanvullende werkzaamheden als gevolg van een wijziging van de scope, ontbrekende of onjuiste informatie, aanvullende testobjecten, hertesten, spoedverzoeken, herstel van testomgevingen of andere niet redelijkerwijs voorzienbare omstandigheden alleen na schriftelijke overeenstemming over planning en vergoeding worden uitgevoerd?	
398.	Bijlage 3A – Raamovereenkomst art. 3 Prijs en tarieven	Kan de KB bevestigen dat de indexeringsregeling zoals opgenomen in artikel 3.4 van de concept-raamovereenkomst eveneens van toepassing is op het in de aanbesteding aangeboden mandagtarief?	Ja, dat wordt bevestigd.
399.	Bijlage 3A – Raamovereenkomst art. 3 Prijs en tarieven	Kan de KB bevestigen dat zij haar akkoord op een indexatieverzoek niet onthoudt wanneer de voorgeschreven index en formule juist zijn toegepast?	Ja, dat wordt bevestigd.
400.	Bijlage 3A – Raamovereenkomst (aanvullende bepalingen)	Opdrachtnemer ziet graag een bepaling toegevoegd welke er op neer komt dat Opdrachtgever tijdens de looptijd van de Raamovereenkomst en/of een Nadere Overeenkomst, alsmede gedurende een periode van 12 maanden na afloop van de Raamovereenkomst of een Nadere Overeenkomst geen medewerker van Opdrachtnemer direct of indirect in dienst neemt. Is Opdrachtgever hiermee akkoord?	Nee, dat is niet akkoord. De KB wenst een dergelijke beperkende voorwaarde niet op te nemen binnen de Raamovereenkomst.
401.	Bijlage 3A – Raamovereenkomst (aanvullende bepalingen)	"Op grond van de onafhankelijkheidswetgeving dient er een non-sollicitatie tussen Opdrachtgever en Opdrachtnemer overeen te worden gekomen. Opdrachtnemer wenst graag daartoe de volgende bepaling in de Overeenkomst op te nemen: ""Partijen zullen tijdens de uitvoering van de werkzaamheden en binnen een (1) jaar na beëindiging van de Overeenkomst geen bij de werkzaamheden betrokken personen van de wederpartij in dienst nemen of anderszins werkzaamheden laten verrichten dan wel daarover met deze personen onderhandelen, behoudens	Nee, dat is niet akkoord. De KB is niet bekend met wet- en regelgeving die het opnemen van een dergelijke bepaling in deze Overeenkomst vereist. Eventuele verplichtingen die voor Opdrachtnemer voortvloeien uit de op hem van toepassing zijnde beroepsregels, dient Opdrachtnemer zelf na te leven.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		voorafgaande uitdrukkelijke schriftelijke toestemming van de wederpartij, welke toestemming niet op onredelijke grond zal worden onthouden." " "	
402.	Bijlage 3A – Raamovereenkomst (aanvullende bepalingen)	Wij hechten veel waarde aan het behoud van onze medewerkers, zij vormen immers ons ‘kapitaal’. Wij zouden graag willen overeenkomen dat Partijen elkaars (of diens onderaannemers) direct bij de Overeenkomst betrokken personeel niet in dienst zullen nemen of anderszins voor zich zullen laten werken tot 6 maanden na het einde van de Overeenkomst, tenzij Partijen het in een concreet geval eens worden over de betaling van een redelijke vergoeding door Opdrachtgever aan Opdrachtnemer. Bent u bereid tot deze afspraak? Zo niet, waarom niet?	Nee. Zie de antwoorden op de vragen 400 en 401.
403.	Bijlage 3A – Raamovereenkomst (aanvullende bepalingen)	"Een algemeen geformuleerde clause ten aanzien van op Opdrachtnemer van toepassing zijnde wet- en regelgeving, inclusief gedrags- en beroepsregels, ontbreekt in de Overeenkomst. Bent u bereid de volgende tekst aanvullend overeen te komen: “Opdrachtnemer voert de opdracht uit in overeenstemming met de toepasselijke wet- en (beroeps)regelgeving. Opdrachtnemer is nimmer gehouden tot enig handelen of nalaten dat met de hiervoor bedoelde regels strijdig of onverenigbaar is.” Bent u hiertoe bereid? "	Akkoord, voor zover het gaat om vastgestelde branche- en/of wettelijke gedrags- en beroepsregels (die betrekking hebben op de scope van onderhavige Opdracht).
404.	Bijlage 3A – Raamovereenkomst (aanvullende bepalingen)	De opdracht zal door de betrokken beroepsbeoefenaren worden uitgevoerd met inachtneming van de voor hen geldende gedrags- en beroepsregels. Hiermee wordt in de voorwaarden en/of (concept) overeenkomst geen rekening gehouden. Ter bevestiging dat voornoemde regels gerespecteerd worden, stellen wij voor onderstaande bepaling op te nemen. Gaat u hiermee akkoord? “X.X De Opdracht zal door Opdrachtnemer worden uitgevoerd met inachtneming van de voor de bij de uitvoering van de Opdracht betrokken beroepsbeoefenaren geldende gedrags- en beroepsregels. Opdrachtnemer is nimmer gehouden tot enig handelen of nalaten dat met de hiervoor bedoelde regels strijdig of onverenigbaar is.”	Zie het antwoord op vraag 403.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
405.	Bijlage 3A – Raamovereenkomst (aanvullende bepalingen)	Er is geen (tussentijdse) opzeggingsmogelijkheid opgenomen voor partijec. Er zijn echter omstandigheden denkbaar waaronder van geen der partijen kan worden gevegd dat de overeenkomst nog langer wordt voorgezet. Indien zich een dergelijke situatie voordoet dienen partijen de bevoegdheid te hebben de overeenkomst op te zeggen. Bent u daarom bereid de volgende bepaling op te nemen: “X.X Ieder der partijen is bevoegd de Overeenkomst met onmiddellijke ingang door opzegging te beëindigen, indien redelijkerwijs te verwachten is dat de Opdracht, zonder dat er sprake is van een toerekenbare tekortkoming door een van de partijen, niet (meer) kan of zal worden uitgevoerd zoals door partijen is overeengekomen. Opdrachtnemer is bovendien bevoegd de Overeenkomst door opzegging te beëindigen, indien van haar in redelijkheid niet (meer) verlangd kan worden dat zij de Opdracht uitvoert zoals door partijen is overeengekomen.”	Nee, dat is niet akkoord.
406.	Bijlage 3B – Verwerkersovereenkomst	Artikelen 2.3 en 2.4 Kan Opdrachtgever instemmen met vervanging van de ruim geformuleerde garanties door de verplichting dat Wederpartij de specifiek op Wederpartij als Verwerker rustende verplichtingen naleeft en passende technische en organisatorische maatregelen treft overeenkomstig de artikelen 28 en 32 AVG, zonder een absolute garantie te geven dat zich geen beveiligingsincident of Inbreuk in verband met Persoonsgegevens zal voordoen?	Nee, dat is niet akkoord.
407.	Bijlage 3B – Verwerkersovereenkomst	Artikel 4 Kan Opdrachtgever bevestigen dat Opdrachtgever verantwoordelijk blijft voor de doeleinden, rechtsgronden, gegevensminimalisatie, transparantie, bewaartermijnen en rechtmatigheid van de Persoonsgegevens en de gegeven instructies? Kan Opdrachtgever tevens bevestigen dat Wederpartij mag vertrouwen op de rechtmatigheid van gedocumenteerde instructies, tenzij deze	Dit is afhankelijk van de vraag of Opdrachtnemer als Verwerker kwalificeert (zie het antwoord op vraag 41). Indien dat het geval is, blijft artikel 4 van de Verwerkersovereenkomst ongewijzigd van toepassing.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		kennelijk in strijd zijn met gegevensbeschermingswetgeving, en de uitvoering van een mogelijk onrechtmatige instructie mag opschorten totdat hierover duidelijkheid is verkregen?	
408.	Bijlage 3B – Verwerkersovereenkomst	Artikel 5.4 en Bijlage 2 Kan Opdrachtgever bevestigen dat Verwerking buiten de EER kan plaatsvinden na voorafgaande schriftelijke toestemming van Opdrachtgever en met inachtneming van hoofdstuk V AVG, waaronder, indien van toepassing, een adequaatheidsbesluit, Standard Contractual Clauses of Binding Corporate Rules? Kan Opdrachtgever tevens bevestigen dat geanonimiseerde gegevens en technische informatie die niet als Persoonsgegevens kwalificeren buiten deze beperking vallen?	De KB geeft op voorhand geen toestemming voor verwerking buiten de EER. Zie ook het antwoord op vraag 306.
409.	Bijlage 3B – Verwerkersovereenkomst	Artikel 7, Subverwerkers Kan Opdrachtgever instemmen met algemene schriftelijke toestemming voor de door Wederpartij ingezette Subverwerkers en voor latere wijzigingen daarvan na voorafgaande kennisgeving? Kan tevens worden bevestigd dat Opdrachtgever uitsluitend binnen een redelijke termijn en op concrete gegevensbeschermingsrechtelijke gronden bezwaar kan maken? De gegevens van de specifieke Subverwerkers kunnen na gunning in de daarvoor bestemde bijlage worden vastgelegd.	Nee, dat is niet akkoord.
410.	Bijlage 3B – Verwerkersovereenkomst	Artikel 10, wettelijke bewaring Kan Opdrachtgever bevestigen dat Wederpartij na beëindiging Persoonsgegevens mag bewaren voor zover dit noodzakelijk is op grond van toepasselijke wetgeving, professionele bewaarplichten of voor het instellen, uitoefenen of onderbouwen van rechtsvorderingen, onder voortdurende geheimhoudings- en beveiligingsverplichtingen en zonder de Persoonsgegevens voor andere doeleinden te verwerken?	Ja, mits er sprake is van een wettelijke grondslag daarvoor.
411.	Bijlage 3B – Verwerkersovereenkomst	Artikel 11, auditvoorwaarden	Gedeeltelijk. De auditrechten op grond van eis E50, artikel 5 ARBIT-2022 en artikel 11 van de

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		De Verwerkersovereenkomst bevat een auditrecht naast de audit- en informatierechten uit de Raamovereenkomst en artikel 5 ARBIT-2022. Kan Opdrachtgever bevestigen dat deze rechten niet als afzonderlijke of cumulatieve auditrechten worden uitgeoefend, maar onder één gecoördineerd auditregime vallen en aan dezelfde voorwaarden zijn onderworpen? Bestaande certificeringen en onafhankelijke assurance-informatie worden daarbij eerst gebruikt. Een aanvullende audit vindt uitsluitend plaats bij een redelijke en concrete aanleiding, na voorafgaande schriftelijke aankondiging, door een onafhankelijke niet-concurrent die aan geheimhouding is gebonden, en zonder toegang tot gegevens van andere klanten, broncode, interne juridische adviezen, bedrijfsgeheimen, pentestmethoden of gedetailleerde kwetsbaarheidsinformatie. De audit mag de bedrijfsvoering niet onredelijk verstoren en de kosten komen voor rekening van Opdrachtgever, tenzij materiële en toerekenbare niet-naleving wordt vastgesteld.	Verwerkersovereenkomst worden in samenhang uitgeoefend, onder de voorwaarden zoals beschreven in de antwoorden op de vragen 363 en 417. Eis E50 gaat daarbij voor artikel 5.3 ARBIT-2022. De overige voorgestelde voorwaarden worden niet overgenomen.
412.	Bijlage 3B – Verwerkersovereenkomst	Artikel 11, audits Kan Opdrachtgever bevestigen dat bestaande certificeringen, auditrapporten en andere onafhankelijke assurance-informatie in beginsel volstaan en dat een aanvullende audit uitsluitend plaatsvindt indien daarvoor een redelijke en concrete aanleiding bestaat, maximaal eenmaal per twaalf maanden, na voorafgaande schriftelijke aankondiging en tijdens de normale kantooruren van Wederpartij?	Gedeeltelijk. De KB laat maximaal één audit per jaar uitvoeren en kondigt deze tijdig vooraf aan (zie de antwoorden op de vragen 363 en 417). De KB bevestigt niet dat bestaande certificeringen en assurance-informatie in beginsel volstaan en maakt een audit niet afhankelijk van een concrete aanleiding; eis E50 gaat daarbij voor artikel 5.3 ARBIT-2022.
413.	Bijlage 3B – Verwerkersovereenkomst	Verwerkersovereenkomst, Artikel 11. Opdrachtnemer dient mee te werken aan een audit. Hiermee kunnen wij niet instemmen. Wij kunnen opdrachtgever geen (onbeperkte) toegang verlenen tot onze locaties en systemen (i.v.m. de geheimhoudingsverplichtingen jegens onze (andere) klanten) en werknemers. Kunt u akkoord gaan met het buiten toepassing verklaren van dit artikel in de Verwerkersovereenkomst en te vervangen door een bepaling dat opdrachtnemer aan opdrachtgever op verzoek de informatie zal verschaffen die voorziet in de informatiebehoefte van Opdrachtgever,	Nee, dat is niet akkoord.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		en dat een dergelijk verzoek niet op onredelijke grond geweigerd zal worden.	
414.	Bijlage 4 – ARBIT-2022 art. 26.1 Ingebrekestelling	Het is redelijk dat Opdrachtnemer altijd eerst in gebreke wordt gesteld voordat sprake is van verzuim. Is Opdrachtgever hiermee akkoord?	Artikel 26.1 ARBIT-2022 bepaalt reeds dat een ingebrekestelling nodig is, tenzij sprake is van een Fatale termijn of uit een mededeling dan wel de houding van de andere partij blijkt dat deze zal tekortschieten. Dit wordt niet gewijzigd.
415.	Bijlage 4 – ARBIT-2022 art. 1	Wij gaan er vanuit dat de afspraken zoals opgenomen in de overeenkomst leidend zullen zijn voor de uitvoering van de Opdracht. Het kader zoals geschetst in het Bestek wordt immers door partijen nader ingevuld en uitgewerkt in de gezamenlijk overeengekomen specificaties. Wij stellen daarom de volgende aanpassing voor: “Gebrek: iedere storing en/of ander mankement als gevolg waarvan de Prestatie niet (meer) voldoet aan de objectief bepaalde functionele en/of technische specificaties zoals Partijen zijn overeengekomen in de Overeenkomst.” Kunt u hiermee instemmen? Zo niet, dan verzoeken wij u dat duidelijk te motiveren.	Akkoord.
416.	Bijlage 4 – ARBIT-2022 art. 4	Er ontbreekt een bepaling over de juistheid van informatie die u aan ons verstrekt in het kader van de uitoefening van deze opdracht. Om onze werkzaamheden correct uit te voeren, is het van belang dat de juiste, volledige en betrouwbare informatie wordt aangeleverd en wij daarvan mogen uitgaan. De informatie die u aan ons verstrekt is immers het uitgangspunt van onze werkzaamheden. Bent u bereid de volgende bepaling aan artikel 4 toe te voegen: “4.5 Opdrachtnemer mag uitgaan van de juistheid, volledigheid en betrouwbaarheid van de aan Opdrachtnemer verstrekte informatie, ook indien deze van derden afkomstig is.”	Akkoord.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
417.	Bijlage 4 – ARBIT-2022 art. 5 Audits	Opdrachtnemer is bereid onder nadere voorwaarden aan een verzoek tot het laten uitvoeren van een audit te voldoen. Een audit door Opdrachtgever: i) dient geruime tijd van te voren te worden aangekondigd; en ii) wordt uitgevoerd door een door partijen gezamenlijk aan te wijzen onafhankelijke derde, die gebonden is aan strikte geheimhouding en geen concurrent is van Opdrachtnemer; en iii) wordt uitgevoerd op basis van een vooraf afgesproken omvang en/of inhoud van de inzage; en iv) wordt alleen uitgevoerd indien er gerede twijfels bestaan omtrent de juistheid van de uitvoering van de overeenkomst door Opdrachtnemer v) de kosten van de audit worden gedragen door Opdrachtgever, tenzij uit het resultaat van de audit blijkt dat de overeenkomst materieel niet juist wordt uitgevoerd door Opdrachtnemer; en vi) kan alleen worden uitgevoerd als beurs- of regels van Opdrachtnemer zich niet tegen een audit verzetten. Is Opdrachtgever hiermee akkoord	Gedeeltelijk akkoord. De KB kondigt een audit tijdig vooraf aan en stemt de omvang en inhoud vooraf met Opdrachtnemer af. De audit wordt uitgevoerd door de KB of door een door de KB aangewezen onafhankelijke deskundige die aan geheimhouding is gebonden. De KB maakt een audit niet afhankelijk van gerede twijfel over de uitvoering van de Overeenkomst; de overige voorwaarden worden niet overgenomen. Voor de frequentie en de kosten, zie het antwoord op vraag 363.
418.	Bijlage 4 – ARBIT-2022 art. 5 Audits	Op grond van deze artikelen bent u gerechtigd audits uit te (laten) voeren, waarvoor ieder haar eigen kosten draagt. Wij achten het niet wenselijk dat u het recht heeft onderzoek te (laten) doen naar de naleving van de overeenkomst. Dergelijke audits brengen veel kosten met zich. Daarnaast zou het toestaan van audits door of namens klanten, gezien de grote hoeveelheid klanten die wij bedienen, ertoe leiden dat onze bedrijfsvoering verstoord wordt. Kunt u bevestigen dat u geen audits zult (laten) uitvoeren?	Nee. Zie het antwoord op vraag 363.
419.	Bijlage 4 – ARBIT-2022 art. 5 Audits	Artikel 5, auditwaarborgen Kan Opdrachtgever bevestigen dat een audit wordt uitgevoerd door een onafhankelijke deskundige die geen concurrent van Opdrachtnemer is, aan passende geheimhouding is gebonden en geen toegang krijgt tot gegevens van andere klanten, broncode, interne juridische adviezen, methodologieën, gedetailleerde	Gedeeltelijk. Zie het antwoord op vraag 417.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		kwetsbaarheidsinformatie, testtools of andere bedrijfsgeheimen, behoudens voor zover specifieke inzage strikt noodzakelijk is voor het doel van de audit?	
420.	Bijlage 4 – ARBIT-2022 art. 5 Audits	Artikel 5, audits Kan Opdrachtgever bevestigen dat audits en informatieverzoeken eerst gebruikmaken van bestaande certificeringen, auditrapporten en onafhankelijke assurance-informatie en dat een aanvullende audit uitsluitend bij een concrete en redelijke aanleiding plaatsvindt, vooraf schriftelijk wordt aangekondigd, tijdens normale kantooruren wordt uitgevoerd en de bedrijfsvoering niet onredelijk verstoort?	Gedeeltelijk. De KB laat maximaal één audit per jaar uitvoeren en kondigt deze tijdig vooraf aan (zie de antwoorden op de vragen 363 en 417). De KB bevestigt niet dat bestaande certificeringen en assurance-informatie in beginsel volstaan en maakt een audit niet afhankelijk van een concrete aanleiding; eis E50 gaat daarbij voor artikel 5.3 ARBIT-2022.
421.	Bijlage 4 – ARBIT-2022 art. 7.2 Eigendomsovergang	Opdrachtnemer stelt voor de tekst te wijzigen in: Onverminderd het bepaalde in artikel 8 gaat de eigendom van (onderdelen van) de Prestatie bij Acceptatie en na volledige betaling door Opdrachtgever over op Opdrachtgever. Is Opdrachtgever hiermee akkoord?	Akkoord.
422.	Bijlage 4 – ARBIT-2022 art. 7.2 Eigendomsovergang	Naar onze mening is het redelijk dat het eigendom van de de rechten op de resultaten van verrichte diensten, voor zover sprake is van een overdracht conform de contractuele afspraken, pas zullen overgaan op Opdrachtgever zodra de daarvoor verschuldigde betaling heeft plaatsgevonden. Bent u bereid dit af te spreken? Wij stellen voor om aan de artikelen 7.2, 8.1 onder a en 8.2 toe te voegen: ‘In afwijking op het vorenstaande geldt echter dat, voor zover conform het vorenstaande sprake zou zijn van overdracht van bepaalde intellectuele eigendomsrechten, die intellectuele eigendomsrechten eerst dan zullen overgaan nadat Opdrachtgever alle bedragen die hij in het kader van de uitvoering van de Opdracht verschuldigd is aan Opdrachtnemer volledig en tijdig heeft voldaan.’ Kunt u hiermee instemmen? Zo niet, dan verzoeken wij u dat duidelijk te motiveren.	Ja, dat is akkoord. Zie ook het antwoord op vraag 421.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
423.	Bijlage 4 – ARBIT-2022 art. 8 Intellectuele eigendomsrechten	Kan de KB bevestigen dat reeds bestaande methodieken, rapportagetemplates, hulpmiddelen, scripts, kennis en generieke werkwijzen eigendom van Opdrachtnemer blijven en dat alleen specifiek voor de KB vervaardigde resultaten onder de toepasselijke gebruiksrechten vallen?	Ja, dat wordt bevestigd. De rapportages en overige specifiek voor de KB vervaardigde resultaten vallen onder artikel 8.1 sub a ARBIT-2022. Bestaande en generieke methodieken, tools, scripts, templates en kennis van Opdrachtnemer vallen onder artikel 8.1 sub b ARBIT-2022.
424.	Bijlage 4 – ARBIT-2022 art. 8 Intellectuele eigendomsrechten	Op grond van dit artikel rusten alle intellectuele eigendomsrechten ten aanzien van de Prestatie die specifiek is of wordt ontworpen voor opdrachtgever, bij opdrachtgever. Wij gaan ervan uit dat de reeds bij opdrachtnemer rustende intellectuele eigendomsrechten onder artikel 8.1 sub b ARBIT vallen. Kunt u dit bevestigen?	Ja. Zie het antwoord op vraag 423.
425.	Bijlage 4 – ARBIT-2022 art. 8 Intellectuele eigendomsrechten	Kan de KB bevestigen dat de intellectuele eigendomsrechten op de rapportages bij de KB komen te berusten, maar dat de rechten op bestaande en generieke tools, scripts, exploits, templates, methodieken en kennis van Opdrachtnemer bij Opdrachtnemer blijven?	Ja. Zie het antwoord op vraag 423.
426.	Bijlage 4 – ARBIT-2022 art. 8 Intellectuele eigendomsrechten	Artikel 8, IE-rechten Kan Opdrachtgever bevestigen dat alle intellectuele-eigendomsrechten op bestaande en generieke methoden, testscenario's, scripts, tools, templates, rapportagestructuren, kwetsbaarheidsdatabanken, software, knowhow en generieke verbeteringen daarvan bij Opdrachtnemer of diens licentiegevers blijven berusten? Kan tevens worden bevestigd dat Opdrachtgever uitsluitend een niet-exclusief gebruiksrecht verkrijgt op de voor Opdrachtgever opgestelde rapportage en andere specifiek overeengekomen resultaten, voor intern gebruik en herstel van de geteste systemen?	Het eerste deel van de vraag wordt bevestigd (zie het antwoord op vraag 423). Het tweede deel wordt niet bevestigd: de intellectuele eigendomsrechten op de rapportages komen bij de KB te berusten (artikel 8.1 sub a ARBIT-2022).
427.	Bijlage 4 – ARBIT-2022 art. 8 Intellectuele eigendomsrechten	In art. 8.3 ARBIT-2022 wordt gesteld dat er bij verschil van mening over IE rechten ervan uit wordt gegaan dat deze bij Opdrachtgever	Nee, dat is niet akkoord.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		berusten. Dit lijkt een weinig evenwichtige en eenzijdige benadering. Bent u bereid art. 8.3 ARBIT-2022 buiten toepassing te verklaren?	
428.	Bijlage 4 – ARBIT-2022 art. 8 Intellectuele eigendomsrechten	Wij achten het onredelijk in geval van twijfel op voorbaat te bepalen dat de IE-rechten in dat geval bij u rusten. In dergelijke gevallen dienen partijen een procedure te starten bij een onafhankelijke rechter om te bepalen bij welke partij de intellectuele eigendomsrechten rusten. De laatste zin van het artikel bepaalt dat u ongeacht de uitkomst voort kunt gaan met het gebruik van de Prestatie. Deze zin is wat ons betreft handhaafbaar, zodat u te allen tijde de Prestatie kunt blijven gebruiken. Kunt u derhalve instemmen met het als volgt wijzigen van artikel 8.3 ARBIT: “Bij verschil van mening tussen partijen over intellectuele eigendomsrechten op (delen van) een Prestatie kan er, door één der partijen een procedure aanhangig worden gemaakt bij een daartoe bevoegde rechter, welke zal beslissen aan wie van de partijen de intellectuele eigendomsrechten toebehoren. Opdrachtgever mag ongeacht de uitkomst van dat geschil voortgaan met het Overeengekomen gebruik.”	Nee. Zie het antwoord op vraag 427.
429.	Bijlage 4 – ARBIT-2022 art. 8 Intellectuele eigendomsrechten	"In art. 8.5 ARBIT-2022 staat een tweetal vrijwaringen ten nadele van Opdrachtnemer vermeld. Opdrachtnemer is bereid Opdrachtgever een vrijwaring te verschaffen tegen aanspraken van derden ter zake van een (gestelde) inbreuk op intellectuele eigendomsrechten van die derden (de eerste vrijwaring). Kunt u bevestigen dat deze vrijwaring uitsluitend van toepassing is voor zover Opdrachtgever de Prestatie gebruikt overeenkomstig het overeengekomen gebruik en voor het overeengekomen doel? Voorts is Opdrachtnemer van mening dat een onbeperkte vrijwaring ten gunste van Opdrachtgever tegen alle schade en kosten waartoe Opdrachtgever eventueel wordt veroordeeld, alsook tegen de kosten van die procedure zelf, inclusief de kosten die verband houden met het inwinnen van juridisch advies, veel te ver strekt en is voor Opdrachtnemer niet acceptabel. Wij vernemen graag of u bereid bent	Gedeeltelijk. De KB bevestigt dat de vrijwaring van toepassing is voor zover de KB de Prestatie gebruikt overeenkomstig het Overeengekomen gebruik. De tweede vrijwaring van artikel 8.5 ARBIT-2022 blijft van toepassing en wordt niet beperkt; artikel 26.4 sub c ARBIT-2022 wordt niet gewijzigd.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		(a) de tweede vrijwaring in art. 8.5 ARBIT-2022 (kosten veroordeling en procedure) buiten toepassing te verklaren, of (b) indien u hiertoe niet bereid bent, deze tweede vrijwaring te beperken tot het maximale aansprakelijkheidsbedrag, zoals wij dat voorstellen in verband met art. 26 ARBIT-2022? "	
430.	Bijlage 4 – ARBIT-2022 art. 8 Intellectuele eigendomsrechten	Wij zijn uiteraard bereid u te vrijwaren voor aanspraken van derden ter zake van een (gestelde) inbreuk op intellectuele eigendomsrechten. We achten het wel redelijk dat daarop de overeengekomen aansprakelijkheidsbeperking van toepassing is. Gaat u daarmee akkoord?	Nee. Zie het antwoord op vraag 429.
431.	Bijlage 4 – ARBIT-2022 art. 8 Intellectuele eigendomsrechten	Uiteraard zijn wij bereid aansprakelijkheid te accepteren echter dan moet het wel gaan om een situatie waarin daadwerkelijk vastgesteld wordt dat wij inderdaad toerekenbaar inbreuk maken op intellectuele eigendomsrechten van derden. Wij stellen daarom de volgende aanpassing voor: “Wederpartij vrijwaart Opdrachtgever tegen gerechtvaardigde aanspraken van derden jegens Opdrachtgever indien en voor zover in rechte wordt vastgesteld dat in het kader van de uitvoering van de Opdracht door Wederpartij ontwikkelde programmatuur een toerekenbare inbreuk op een in Nederland geldend recht van intellectueel eigendom van deze derde oplevert.” Kunt u hiermee instemmen? Zo niet, dan verzoeken wij u dat duidelijk te motiveren danwel aan te geven in hoeverre u wel dit tekstvoorstel kunt aanvaarden.	Nee. Zie het antwoord op vraag 429.
432.	Bijlage 4 – ARBIT-2022 art. 8 Intellectuele eigendomsrechten	Op grond van dit artikel dienen wij op onze kosten alle maatregelen te nemen die kunnen bijdragen tot het voorkomen van stagnatie van Opdrachtgevers bedrijfsvoering. Onzes inziens dient deze bepaling onder de algemene aansprakelijkheidsbeperking van artikel 26 ARBIT te vallen. Kunt u daarom instemmen met het schrappen van artikel 8.6 ARBIT?	Akkoord.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
433.	Bijlage 4 – ARBIT-2022 art. 8 Intellectuele eigendomsrechten	Het nemen van maatregelen op onze kosten is slechts redelijk voor zover deze maatregelen noodzakelijk zijn om stagnatie in de bedrijfsvoering te voorkomen. Het nemen van maatregelen die ‘kunnen bijdragen aan het voorkomen van stagnatie’ is wel erg omvangrijk. Kunt u bevestigen dat wij alleen aan dit artikellid worden gehouden voor zover dat redelijkerwijs van ons verlangd kan worden? Zo niet, dan verzoeken wij u dat duidelijk te motiveren.	Zie het antwoord op vraag 432.
434.	Bijlage 4 – ARBIT-2022 art. 8 Intellectuele eigendomsrechten	Kunt u bevestigen dat u pas gebruik zult maken van uw rechten op grond van artikel 8.7 als in rechte is vastgesteld dat het door ons geleverde Product inbreuk maakt op intellectuele eigendomsrechten van derden en wij aangeven redelijkerwijs niet in staat te zijn die inbreuk op te heffen, bijvoorbeeld door het beschikbaar stellen van een vervangend gelijkwaardig Product? Graag uw reactie. Indien die afwijzend is, verzoeken wij u om een duidelijke motivering.	Ja, dat wordt bevestigd.
435.	Bijlage 4 – ARBIT-2022 art. 9 Documentatie	Art. 9.2 ARBIT-2022 bepaalt dat Opdrachtgever gerechtigd is: “Documentatie”, zonder daarvoor een nadere vergoeding verschuldigd te zijn, te verveelvoudigen, te wijzigen en voor eigen gebruik binnen zijn organisatie openbaar te maken, mits daarop voorkomende aanduidingen van auteursrechten e.d. worden gehandhaafd. In dit kader is het niet acceptabel dat Opdrachtgever “Documentatie” mag wijzigen. Derhalve verzoeken wij u om het woord “wijzigen” in art. 9.2 ARBIT-2022 buiten toepassing te verklaren. Bent u hiertoe bereid?	Akkoord.
436.	Bijlage 4 – ARBIT-2022 art. 11 Acceptatie	Dit artikel is zo geformuleerd dat wij voor betaling afhankelijk zijn van de acceptatie, zonder dat duidelijk is aan welke criteria voldaan moet zijn voor acceptatie. Dit creëert veel onzekerheid en onduidelijkheid. Wij stellen daarom de volgende toevoeging voor: “Opdrachtgever is enkel gerechtigd Acceptatie te onthouden indien het opgeleverde niet voldoet aan de vooraf overeengekomen specificaties of acceptatiecriteria.”	Nee, dat is niet akkoord. De Acceptatie vindt plaats op basis van de eisen uit de Aanbestedingsstukken (waaronder E43) en de Nadere Overeenkomst.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		Kunt u hiermee instemmen? Zo niet, dan verzoeken wij u dat duidelijk te motiveren danwel aan te geven in hoeverre u wel dit tekstvoorstel kunt aanvaarden.	
437.	Bijlage 4 – ARBIT-2022 art. 11 Acceptatie	Wij zien graag een toevoeging op dit artikel. Het is namelijk zo dat vanaf het moment dat Opdrachtgever het Product operationeel in gebruik neemt er wijzigingen (kunnen) plaatsvinden in het opgeleverde Product, waarop wij geen invloed hebben en welke ons niet aangerekend kunnen worden. Vanaf dat moment zal het Product dan ook als geaccepteerd worden beschouwd. Wij stellen daarom de volgende toevoeging voor: “Bij in productie name en/of ingebruikname van het opgeleverde Product door Opdrachtgever, of bij het uitblijven van enige mededeling (...)” Kunt u hiermee instemmen? Zo niet, dan verzoeken wij u dat duidelijk te motiveren danwel aan te geven in hoeverre u wel dit tekstvoorstel kunt aanvaarden.	Nee, dat is niet akkoord. De Prestatie onder deze Raamovereenkomst bestaat uit de uitvoering van een pentest en de daarbij opgeleverde rapportage. Er is geen sprake van een Product dat door de KB in productie wordt genomen en waarin na oplevering wijzigingen kunnen plaatsvinden. De door Inschrijver geschetste situatie is daarmee niet van toepassing. Daarnaast voorziet artikel 11.5 ARBIT-2022 reeds in acceptatie bij het uitblijven van een mededeling van de KB binnen de gestelde termijn.
438.	Bijlage 4 – ARBIT-2022 art. 11 Acceptatie	Wij vinden het redelijk dat de nader door Opdrachtgever te stellen termijn wordt gemaximeerd, om een duidelijk kader te creëren en te voorkomen dat de termijn onredelijk lang wordt. Hierbij speelt mee dat de betaling is gekoppeld aan Acceptatie. Wij stellen voor om aan artikel 11.4 de volgende tekst toe te voegen: “De nader door Opdrachtgever gestelde termijn bedraagt maximaal twee weken, tenzij Partijen na onderling overleg een langere termijn zijn overeengekomen.” Kunt u hiermee instemmen? Zo niet, dan verzoeken wij u dat duidelijk te motiveren danwel aan te geven in hoeverre u wel dit tekstvoorstel kunt aanvaarden.	Nee, dat is niet akkoord. Op grond van artikel 11.4 ARBIT-2022 meldt de KB vóór afloop van de reguliere termijn de reden van de vertraging en de termijn waarbinnen zij alsnog uitsluitel geeft. Opdrachtnemer heeft daarmee vooraf duidelijkheid. De benodigde termijn is afhankelijk van de omvang en complexiteit van de rapportage en de beschikbaarheid van de betrokken interne en externe partijen, en wordt daarom niet vooraf gemaximeerd. Daarnaast is de betaling niet volledig afhankelijk van de Acceptatie: conform eis E57 mag 50% bij de start van de Nadere Opdracht worden gefactureerd en 50% nadat de rapportage gezamenlijk is besproken (zie ook het antwoord op vraag 370).
439.	Bijlage 4 – ARBIT-2022 art. 11 Acceptatie	Artikelen 11 en 15, acceptatie en betaling	Nee, dat is niet akkoord. Zie het antwoord op vraag 436.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		Kan Opdrachtgever bevestigen dat per Nadere Overeenkomst vooraf objectieve acceptatiecriteria en een acceptatietermijn worden overeengekomen en dat een pentest en rapportage als geaccepteerd gelden indien Opdrachtgever niet binnen tien Werkdagen na oplevering schriftelijk en gemotiveerd een materiële afwijking meldt? Kan tevens worden bevestigd dat geringe afwijkingen die het overeengekomen gebruik niet verhinderen geen reden vormen om acceptatie of betaling uit te stellen?	
440.	Bijlage 4 – ARBIT-2022 art. 12 Garanties	Het opnemen van een garantietermijn is gelet op de aard van de door Opdrachtgever gevraagde dienstverlening niet van toepassing. Opdrachtnemer stelt voor dit artikel niet van toepassing te verklaren. Is Opdrachtgever hiermee akkoord? Indien Opdrachtgever niet bereid is het artikel niet van toepassing te verklaren en onverlet het voorgaande met betrekking tot de aard van de dienstverlening, stelt Opdrachtnemer voor de garantie termijn te verkorten tot een meer marktconforme periode van 3 maanden.	Gedeeltelijk. Artikel 12.3 ARBIT-2022 blijft van toepassing. De garantie heeft uitsluitend betrekking op Gebreken in de geleverde Prestatie, zoals onjuistheden in de rapportage (bijvoorbeeld een onjuiste risicoclassificatie, niet-reproduceerbare bevindingen of technisch onjuiste adviezen) en overeengekomen testwerkzaamheden die niet zijn uitgevoerd. De KB is wel bereid de garantietermijn te verkorten naar zes maanden na Acceptatie.
441.	Bijlage 4 – ARBIT-2022 art. 12 Garanties	Op grond van dit artikel dienen wij gedurende twaalf maanden na Acceptatie, gebreken voor onze rekening te herstellen. Dit artikel is wat ons betreft niet passend bij het soort dienstverlening dat u uitvraagt. Wij leveren adviesdiensten, waarbij wij een advies geven over een bepaalde toestand op een bepaald moment. Wij kunnen hiervoor geen langdurige garantie geven, nu de situatie omtrent informatiebeveiliging na verloop van tijd kan veranderen. Kunt u er daarom mee instemmen dat artikel 12.3 buiten toepassing wordt verklaard?	Zie het antwoord op vraag 440.
442.	Bijlage 4 – ARBIT-2022 art. 12 Garanties	Een garantietermijn van 12 maanden is zeer lang en niet marktconform. Dit heeft een prijsverhogend effect. Wij stellen daarom voor deze termijn bij te stellen naar 3 maanden na acceptatie. Kunt u daarmee instemmen?	Zie het antwoord op vraag 440.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		Kunt u hiermee instemmen? Zo niet, dan verzoeken wij u dat duidelijk te motiveren.	
443.	Bijlage 4 – ARBIT-2022 art. 12 Garanties	Artikel 12.3, garantie Kan Opdrachtgever bevestigen dat de garantie uitsluitend betrekking heeft op herstel van aantoonbare fouten in de opgeleverde rapportage of niet-uitgevoerde overeengekomen testwerkzaamheden en geen garantie inhoudt dat alle aanwezige kwetsbaarheden worden ontdekt, dat de geteste omgeving vrij is of blijft van kwetsbaarheden, of dat na de test geen nieuwe kwetsbaarheden ontstaan?	Ja. Zie het antwoord op vraag 440.
444.	Bijlage 4 – ARBIT-2022 art. 14.3 Boetes	Wij zijn van mening dat het niet redelijk is dat Opdrachtgever, naast een boete, ook nog schadevergoeding zou kunnen vorderen zonder dat het betaalde boetebedrag hiervan afgetrokken wordt (dit gedeelte van de schade wordt dan feitelijk dubbel betaald). Wij stellen voor om in algemene zin het volgende overeen te komen: “Betaalde boetes strekken in mindering op eventueel verschuldigde schadevergoeding.”. Kunt u hiermee instemmen? Zo niet, dan verzoeken wij u dat duidelijk te motiveren danwel aan te geven in hoeverre u wel dit tekstvoorstel kunt aanvaarden.	Akkoord.
445.	Bijlage 4 – ARBIT-2022 art. 14.3 Boetes	Artikel 14.3, boetes en cumulatie Kan Opdrachtgever bevestigen dat eventuele boetes, kortingen of service credits uitsluitend gelden indien deze uitdrukkelijk in een Nadere Overeenkomst zijn overeengekomen, gezamenlijk aan een redelijk maximum zijn onderworpen en volledig in mindering worden gebracht op schadevergoeding wegens dezelfde tekortkoming of gebeurtenis?	Gedeeltelijk. Betaalde boetes strekken in mindering op eventueel verschuldigde schadevergoeding wegens dezelfde tekortkoming; zie het antwoord op vraag 444. De KB bevestigt niet dat boetes uitsluitend gelden indien deze in een Nadere Overeenkomst zijn overeengekomen: de boete van artikel 17.5 ARBIT-2022 is via de Raamovereenkomst van toepassing op alle Nadere Overeenkomsten. Boetes worden niet gemaximeerd.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
446.	Bijlage 4 – ARBIT-2022 art. 15 Betaling en controle	Opdrachtnemer kan niet zonder meer externe partijen inzage geven in de financiële en/of projectadministratie en/of andere gegevens. Een dergelijke controle: i) dient ruim vooraf te worden aangekondigd; en ii) dient te worden uitgevoerd door een door partijen gezamenlijk aan te wijze onafhankelijke derde, die gebonden is aan strikte geheimhouding en geen concurrent is van Opdrachtnemer; en iii) dient op basis van een van te voren afgesproken omvang en/of inhoud van de inzage.; en iv) mag alleen worden verzocht als er redelijke twijfels bestaan omtrent de juistheid van de factuur; en. v) worden de gegevens en informatie verschaft door Opdrachtnemer die in redelijkheid van hem kunnen worden verlangd; en vi) komen de kosten van het accountantsonderzoek alleen voor rekening van Opdrachtnemer indien het gaat om ernstige fouten in de facturen; en vii) is beperkt tot één per periode van 12 maanden; en viii) kan uitsluitend worden uitgevoerd als beurs- of regels van Opdrachtnemer zich niet tegen een audit verzetten. Is Opdrachtgever hiermee akkoord?	Akkoord.
447.	Bijlage 4 – ARBIT-2022 art. 15 Betaling en controle	Artikel 15.3, factuurcontrole Kan Opdrachtgever bevestigen dat een factuurcontrole vooraf schriftelijk wordt aangekondigd, beperkt blijft tot informatie die strikt noodzakelijk is voor verificatie van de betreffende factuur en geen toegang geeft tot informatie over andere klanten, interne kostprijzen, marges, bedrijfsgeheimen of juridisch geprivilegieerde informatie?	Ja, dat wordt bevestigd.
448.	Bijlage 4 – ARBIT-2022 art. 15 Betaling en controle	Op grond van art. 15.5 ARBIT-2022 doet Opdrachtnemer afstand van haar recht tot opschorting of beëindiging van werkzaamheden, in geval van overschrijding van een betalingstermijn door Opdrachtgever of (gedeeltelijke) niet betaling door Opdrachtgever van een factuur. Het is voor Opdrachtnemer onwenselijk om op voorhand afstand te	Nee, dat is niet akkoord.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		doen van opschortings- en/of ontbindingsrechten. Dit kan leiden tot situaties waarin Opdrachtnemer gehouden is werkzaamheden uit te (blijven) voeren, terwijl er geen betaling zal plaatsvinden. Dit is een onredelijke eis. Wij vernemen graag of u bereid bent (a) art. 15.5 ARBIT-2022 buiten toepassing te verklaren, of (b) indien u hiertoe niet bereid bent, deze bepaling aan te vullen met de volgende zinsnede: “... tenzij dit niet redelijk is jegens Wederpartij.”	
449.	Bijlage 4 – ARBIT-2022 art. 15 Betaling en controle	Eén van de belangrijkste verplichtingen die u jegens ons heeft is betaling voor de verrichtte diensten. Als u deze verplichting niet (tijdig) nakomt, dienen wij de mogelijkheid te hebben onze verplichtingen op te schorten, hetgeen ook een wettelijk recht is. Van dit middel zullen wij slechts gebruik maken, indien u structureel uw betalingsverplichtingen niet (tijdig) nakomt. Wij stellen daarom voor artikel 15.5 sub a buiten toepassing te verklaren. Gaat u daarmee akkoord?	Nee. Zie het antwoord op vraag 448.
450.	Bijlage 4 – ARBIT-2022 art. 15 Betaling en controle	Het wettelijk opschortings- en ontbindingsrecht bestaan niet voor niets. Het geeft ons ook een instrument in handen op het moment dat Opdrachtgever onverhoopt haar verplichtingen niet nakomt. Anders is er voor ons geen enkel middel om Opdrachtgever tot nakoming aan te sporen, dat is niet redelijk. Wij zullen hier niet lichtvoetig mee om gaan en redelijk handelen. Wij stellen daarom de volgende toevoeging voor: “, voor zover dit in redelijkheid van Wederpartij kan worden verwacht.” Kunt u hiermee instemmen? Zo niet, dan verzoeken wij u dat duidelijk te motiveren.	Nee. Zie het antwoord op vraag 448.
451.	Bijlage 4 – ARBIT-2022 art. 16 Voorschot	Wij verstrekken geen bankgaranties aan opdrachtgevers. Bent u bereid af te zien van een bankgarantie en artikel 16.1 en 16.3 ARBIT-2022 van de algemene inkoopvoorwaarden buiten toepassing te verklaren?	Akkoord. Artikel 16.1 en 16.3 ARBIT-2022 komen te vervallen.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
452.	Bijlage 4 – ARBIT-2022 art. 16 Voorschot	Wij kunnen niet instemmen met het overleggen van een afroepgarantie (bankgarantie), maar zijn op uw verzoek wel bereid een concernverklaring te overleggen. Onzes inziens biedt een dergelijke verklaring voldoende zekerheid, omdat de moedermaatschappij u schadeloos stelt in geval het ons onverhoopt niet lukt om onze contractuele verplichtingen na te komen. Indien u voornemens bent betalingen te verrichten voor diensten die nog niet geleverd zijn, verzoeken wij u artikel 16.1 en 16.3 buiten toepassing te verklaren. Gaat u hiermee akkoord?	Akkoord. Zie het antwoord op vraag 451.
453.	Bijlage 4 – ARBIT-2022 art. 16 Voorschot	Uit de toelichting op de ARBIT blijkt ook dat terughoudend moet worden omgegaan met het vragen van een dergelijke garantie. Dit is ook niet vreemd aangezien er een aanzienlijk beslag op het vermogen van een opdrachtnemer gelegd wordt. Wij verzoeken u dan ook het vereiste van een kredietinstellingsgarantie te laten vervallen, waarbij partijen wel kunnen afspreken dat in geval hiertoe aanleiding is, bijvoorbeeld in het geval van een verhoogd faillissementsrisico, Opdrachtgever een beroep kan doen op een zekerheidstelling. Kunt u hiermee instemmen? Graag uw reactie.	Akkoord. Zie het antwoord op vraag 451.
454.	Bijlage 4 – ARBIT-2022 art. 17 Geheimhouding	"Graag komen we in aanvulling op de uitzonderingen op de geheimhoudingsplicht zoals genoemd in artikel 17.1 AIV de volgende uitzonderingen overeen: "De geheimhoudingsplicht geldt niet voor zover Opdrachtnemer verplicht is tot openbaarmaking uit hoofde van enig voorschrift van een orgaan aan het toezicht waarvan Opdrachtnemer is onderworpen, een op Opdrachtnemer of personen werkzaam bij/voor of verbonden aan Opdrachtnemer rustende beroepsplicht of een bindende uitspraak van de rechter of een overheidsorgaan. Daarnaast geldt de geheimhoudingsplicht niet indien: i) Opdrachtnemer namens zichzelf optreedt, ii) of personen bij Opdrachtgever in dienst, voor Opdrachtgever werkzaam, of aan Opdrachtgever verbonden, namens zichzelf optreden in een tuchtrechtelijke, strafrechtelijke of	Gedeeltelijk akkoord. Het is Opdrachtnemer toegestaan Vertrouwelijke Informatie te delen met gelieerde entiteiten, mits dit noodzakelijk is voor de feitelijke uitvoering van de Opdracht en Opdrachtnemer de KB hierover vooraf informeert. Eis E36 (opslag van data van de KB in Nederland) blijft onverkort van toepassing. De overige voorgestelde uitzonderingen worden niet overgenomen.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		civielrechtelijke procedure of iii) voor het inwinnen van advies van onze professionele adviseurs en verzekeraars.” Daarnaast is het voor Opdrachtnemer van belang dat we in het kader van wettelijke verplichtingen informatie kunnen delen met gelieerde entiteiten en derden die door ons zijn ingeschakeld ten behoeve van ondersteunende diensten van administratieve en IT aard. Om eventuele onduidelijkheid en verwarring te voorkomen lichten wij u graag toe dat voornoemde derden niet direct betrokken zijn bij de uitvoering van de diensten die wij mogelijk aan u zullen leveren. Voornoemde derden ondersteunen ons enkel ten aanzien van onze interne processen. Uiteraard zijn wij verantwoordelijk voor de inzet van deze derden en de geheimhouding van alle vertrouwelijke informatie. Van derden, die namens ons data verwerken, verlangen wij dat zij voldoen aan de toepasselijke wet- en beroepsregelgeving. Graag willen wij u verzoeken of u, met inachtneming van voornoemde toelichting, akkoord kunt gaan met onderstaand tekstvoorstel in aanvulling op artikel 17 ARBIT-2022: ""Tenzij zulks op grond van de toepasselijke wetgeving verboden is, is het Opdrachtnemer toegestaan om alle door of namens Opdrachtgever verstrekte informatie ('Cliëntinformatie') te gebruiken en deze te verstrekken aan (i) andere gelieerde entiteiten en hun personeel en/of (ii) andere partijen, die ondersteunend zijn ten behoeve van Opdrachtnemer's administratie of infrastructuur en/of de verlening van overige ondersteunende diensten van administratieve en IT-aard ten behoeve van (a) het verrichten van cliënt-, en opdrachtacceptatie procedures, (b) conflict beoordeling van interne risico's en onafhankelijkheid en (c) het onderhouden van kwaliteitsnormen en professionele normen ten aanzien van de Werkzaamheden of diensten.” "	
455.	Bijlage 4 – ARBIT-2022 art. 17 Geheimhouding	Dit artikel houdt de geheimhoudingsplicht in en de uitzondering daarop voor zover enig wettelijk voorschrift daartoe noopt. Kunt u bevestigen dat in de zin van dit artikel onder wettelijke voorschriften	Ja, voor zover het gaat om vastgestelde branche- en/of wettelijke gedrags- en beroepsregels (gericht op de scope van de Opdracht). Zie ook het antwoord op vraag 403.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		eveneens wordt begrepen de toepasselijke gedrags- en beroepsregels?	
456.	Bijlage 4 – ARBIT-2022 art. 17 Geheimhouding	Artikel 17, noodzakelijke informatiedeling Kan Opdrachtgever bevestigen dat iedere Partij Vertrouwelijke Informatie op need-to-knowbasis mag delen met gelieerde ondernemingen, vooraf goedgekeurde onderaannemers, verzekeraars, accountants, advocaten en professionele adviseurs, mits deze ontvangers aan ten minste gelijkwaardige geheimhoudings- en beveiligingsverplichtingen zijn gebonden en de delende Partij verantwoordelijk blijft voor hun naleving?	Gedeeltelijk akkoord. Zie het antwoord op vraag 454. Delen met overige partijen is uitsluitend toegestaan voor zover dit noodzakelijk is voor de uitvoering van de Opdracht (zoals bij een goedgekeurde Onderaannemer).
457.	Bijlage 4 – ARBIT-2022 art. 17 Geheimhouding	Artikel 17, geheimhouding Kan Opdrachtgever bevestigen dat de geheimhoudingsverplichtingen wederkerig gelden en dat Opdrachtgever rapportages, testmethoden, aanvalsscenario's, tooling, technische documentatie en andere vertrouwelijke informatie van Opdrachtnemer ten minste op hetzelfde niveau beschermt als de eigen vertrouwelijke informatie?	Ja, artikel 17.1 ARBIT-2022 geldt voor beide Partijen.
458.	Bijlage 4 – ARBIT-2022 art. 17 Geheimhouding	Gebruik rapportage en openbaarmaking Kan Opdrachtgever bevestigen dat pentestresultaten en rapportages zeer vertrouwelijk worden behandeld, uitsluitend intern en voor herstel- en compliance-doeleinden worden gebruikt en niet zonder voorafgaande schriftelijke toestemming van Opdrachtnemer integraal aan derden worden verstrekt, behoudens wettelijke verplichtingen en verstrekking aan betrokken leveranciers op need-to-knowbasis? Kan tevens worden bevestigd dat Opdrachtnemer vooraf de gelegenheid krijgt feitelijke onjuistheden te corrigeren voordat een rapportage extern wordt gedeeld?	De KB behandelt de rapportages vertrouwelijk. De KB is gerechtigd de rapportages (of delen daarvan) te delen met betrokken leveranciers en adviseurs ten behoeve van herstel en met toezichthouders en auditors. Voorafgaande toestemming van Opdrachtnemer is daarvoor niet vereist.
459.	Bijlage 4 – ARBIT-2022 art. 17 Geheimhouding	"In art. 17.3 ARBIT-2022 dient Wederpartij haar medewerking te verlenen aan het uitoefenen van toezicht door Opdrachtgever op de bewaring en het gebruik van vertrouwelijk informatie door Wederpartij. Het is onduidelijk hoe Opdrachtgever het in art. 17.3	Nee. Het toezicht op grond van artikel 17.3 ARBIT-2022 kan bijvoorbeeld bestaan uit het opvragen van informatie over de wijze waarop testresultaten en rapportages worden opgeslagen, beveiligd en

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		ARBIT-2022 genoemde toezicht op de bewaring en het gebruik van vertrouwelijke informatie door Wederpartij wil uitoefenen en welke partij de hiermee gemoeide kosten draagt. Kunt u een voorbeeld geven van het in artikel 17.3 ARBIT 2022 genoemde toezicht door/namens Opdrachtgever en kunt u bevestigen dat uit deze maatregelen niet volgt, dat u inzage heeft in de administratie van Opdrachtnemer, dan wel toegang wenst tot locaties van Opdrachtnemer? Gaat u daarom akkoord met het volgende tekstvoorstel in aanvulling op art. 17.3 ARBIT-2022: “Dergelijke activiteiten, welke voor rekening van Opdrachtgever komen, strekken zich in ieder geval niet uit tot het verkrijgen van inzage in de administratie van de Wederpartij of tot het verkrijgen van toegang tot locaties van de Wederpartij.” Bent u hiertoe bereid? "	vernietigd, het opvragen van certificaten en auditrapportages, of een controle op locatie. De KB sluit inzage in de relevante administratie en toegang tot locaties daarom niet uit. Het toezicht wordt vooraf met Opdrachtnemer afgestemd, met inachtneming van de geheimhoudingsverplichtingen van Opdrachtnemer jegens andere opdrachtgevers. Voor de kosten geldt hetzelfde als voor een audit; zie het antwoord op vraag 363.
460.	Bijlage 4 – ARBIT-2022 art. 17 Geheimhouding	Wij beschikken over een Informatie Privacy Management Systeem (hierna: IPMS) dat voorziet in een plan-do-check-act cyclus, waardoor continu aandacht bestaat voor informatiebeveiliging en privacy in de producten en diensten die wij onze klanten leveren. Dit systeem is gebaseerd op de ISO-27001-norm. Het IPMS wordt jaarlijks zowel intern (door onze eigen afdeling ICT) als extern beoordeeld door middel van audits. Dit zorgt ervoor dat wij inzicht hebben in de risico's en kwetsbaarheden van onze IT-beveiliging en dat onze organisatie blijft voldoen aan de ISO-27001-normering. Door het overleggen van de ISO-verklaring kunnen wij aantonen dat wij onze IT-beveiliging op orde hebben. Dit neemt onzes inziens het belang voor het uitvoeren van een audit weg. Op verzoek kunnen wij een kopie van het certificaat opsturen alsmede de verklaring van toepasselijkheid hiervan. Wij verzoeken u daarom artikel 17.3 te schrappen. Kunt u hiermee instemmen?	Nee. Zie het antwoord op vraag 459.
461.	Bijlage 4 – ARBIT-2022 art. 17 Geheimhouding	Het is niet duidelijk wat er in de praktijk verstaan wordt onder het hier genoemde 'toezicht' terwijl dit in theorie heel ingrijpend zou kunnen zijn. Wij stellen daarom voor aan artikel 17.3 toe te voegen: "Partijen	Nee. Zie het antwoord op vraag 459.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		komen overeen dat in onderling overleg tot nadere invulling van een dergelijk toezicht wordt gekomen, waarbij uitgangspunt is dat een dergelijk toezicht alleen wordt uitgeoefend indien daar gegronde redenen voor bestaan”. Kunt u daarmee instemmen? Zoniet, waarom niet?	
462.	Bijlage 4 – ARBIT-2022 art. 17 Geheimhouding	"In artikel 17.4 staat beschreven dat Wederpartij alle gegevens die zij in het kader van de uitvoering van de Overeenkomst onder zich heeft, op eerste verzoek van Opdrachtgever ter beschikking stelt. Het aanhouden van een intern dossier is verplicht op grond van regelgeving. Deze bepaling staat haaks op de voor ons verplichte dossiervorming. Bent u daarom bereid in aanvulling van artikel 17.4 ARBIT-2022 het volgende overeen te komen: “Artikel 17.4 ARBIT- 2022 laat onverlet, dat Wederpartij een dossier aanhoudt ter zake van de Opdracht. Wederpartij neemt passende maatregelen om de vertrouwelijkheid en veilige bewaring van het dossier te waarborgen en de dossiers te bewaren gedurende een periode die voor een goede beroepsuitoefening aanvaardbaar is en die in overeenstemming is met de wettelijke bepalingen en beroepsregels inzake bewaartermijnen. De dossiers zijn eigendom van Wederpartij.” "	Gedeeltelijk akkoord. Opdrachtnemer mag ter zake van de Opdracht een dossier aanhouden met de opdrachtadministratie, zoals bedoeld in het antwoord op vraag 330. Testresultaten en bevindingen maken geen deel uit van dit dossier en worden vernietigd overeenkomstig E40, tenzij een wettelijk voorschrift dit verhindert (artikel 32.3 ARBIT-2022). Opdrachtnemer waarborgt de vertrouwelijkheid en veilige bewaring van het dossier en bewaart het niet langer dan de toepasselijke wettelijke bewaartermijnen en beroepsregels voorschrijven.
463.	Bijlage 4 – ARBIT-2022 art. 17 Geheimhouding	Wij zijn op grond van wet- en (beroeps)regelgeving alsmede bewaarrichtlijnen voor kwaliteitssystemen verplicht in het kader van de opdracht een dossier aan te houden met daarin kopieën van relevante documenten, welk dossier – op grond van diezelfde regelgeving - ons eigendom dient te zijn. Wij verzoeken u het volgende artikel op te nemen: “17.4 Op verzoek van Opdrachtgever zal Opdrachtnemer alle door Opdrachtgever verstrekte documenten retourneren, voor zover het hier niet gaat om gegevens die Opdrachtnemer op digitale gegevensdragers bewaard en waar noodzakelijke reserve kopieën van worden gemaakt (deze gegevens blijven onverkort onderworpen aan de geheimhoudingsplicht). Het voorgaande laat onverlet dat	Gedeeltelijk akkoord. Zie het antwoord op vraag 462. Gegevens op back-upmedia worden na afloop van de reguliere back-upcyclus verwijderd.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		Opdrachtnemer ter zake van de opdracht een dossier aanhoudt en blijft houden met daarin kopieën van relevante stukken. Opdrachtnemer zal zijn dossier bewaren gedurende een periode die voor een goede beroepsuitoefening aanvaardbaar is en die in overeenstemming is met de wettelijke bepalingen en beroepsregels inzake bewaartermijnen.”	
464.	Bijlage 4 – ARBIT-2022 art. 17 Geheimhouding	Wij zijn gebonden aan wettelijke bewaarplichten (bijv. t.a.v. de fiscus). Door het teruggeven van alle gegevens welke wij in het kader van de uitvoering van de Overeenkomst onder ons hebben, inclusief kopieën, kunnen wij niet aan deze wettelijke verplichtingen voldoen. Kunt u bevestigen dat voor zover wij een wettelijke bewaarplicht hebben, wij de betreffende gegevens mogen bewaren gedurende deze verplichte bewaarperiode?	Ja. Zie het antwoord op vraag 462.
465.	Bijlage 4 – ARBIT-2022 art. 17 Geheimhouding	Opdrachtnemer is van mening dat deze boete te hoog is en stelt voor deze te verlagen tot maximaal € 10.000,= per overtreding. Is Opdrachtgever hiermee akkoord?	Nee, dat is niet akkoord. Gelet op de aard van de informatie waarover Opdrachtnemer beschikt (kwetsbaarheden in de systemen van de KB) acht de KB de boete proportioneel.
466.	Bijlage 4 – ARBIT-2022 art. 17 Geheimhouding	We achten een boetebepaling onwenselijk, aangezien het contract reeds voorziet in aansprakelijkheid in geval van toerekenbare tekortkoming en contractuele boetes. Opdrachtnemer verzoekt u artikel 17.5 ARBIT-2022 buiten toepassing te verklaren. Kan Opdrachtgever daarmee instemmen?	Nee. Zie het antwoord op vraag 465.
467.	Bijlage 4 – ARBIT-2022 art. 17 Geheimhouding	In geval van schending van de geheimhoudingsplicht geldt een boete van € 50.000 per gebeurtenis. Dit boetebeding werkt aanvullend op overige toekomstige rechten, waaronder het recht op schadevergoeding. Dit betekent dat niet alleen een flinke boete verschuldigd zou zijn, maar ook een aanspraak op schadevergoeding kan worden gemaakt. Er zijn voldoende contractuele en wettelijke mogelijkheden om schade vergoed te krijgen, indien de geheimhoudingsplicht geschonden wordt. Een dergelijke flinke boete	Gedeeltelijk. Het boetebeding wordt niet geschrapt en het boetebedrag wordt niet verlaagd (zie het antwoord op vraag 465). Betaalde boetes strekken wel in mindering op eventueel verschuldigde schadevergoeding (zie het antwoord op vraag 444).

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		daarnaast, is daarom niet nodig en onzes inziens buiten proportioneel. Wij stellen daarom voor het boetebeding te schrappen. Indien u hiertoe niet bereid bent, wensen wij het boetebedrag te verlagen naar € 10.000 per gebeurtenis. Daarnaast wensen wij het boetebedrag in mindering te brengen op eventuele schadevergoeding. Bent u op grond van het voorgaande bereid artikel 17.5 te schrappen? Zo nee, bent u bereid artikel 17.5 overeenkomstig onze suggesties aan te passen?	
468.	Bijlage 4 – ARBIT-2022 art. 17 Geheimhouding	Wij begrijpen de ratio achter het verbinden van een boete aan schending van de geheimhoudingsplicht. Echter, een boete van EUR 50.000,- is zeker niet altijd proportioneel, zeker ook omdat het recht op schadevergoeding is voorbehouden. Daarbij is een boete van EUR. 50.000,- hoger dan in de markt gebruikelijk. Wij stellen voor deze boete aan te passen naar maximaal EUR 20.000,- en toe te voegen: : “Betaalde boetes strekken in mindering op eventueel verschuldigde schadevergoeding.” Stemt u daar mee in? Zo niet, in hoeverre dan wel?	Gedeeltelijk. Het boetebedrag wordt niet verlaagd (zie het antwoord op vraag 465). Betaalde boetes strekken wel in mindering op eventueel verschuldigde schadevergoeding (zie het antwoord op vraag 444).
469.	Bijlage 4 – ARBIT-2022 art. 17 Geheimhouding	Artikel 17.5, geheimhoudingsboete Opdrachtnemer acht een afzonderlijke contractuele boete wegens schending van de geheimhoudingsverplichting niet passend, aangezien Opdrachtgever bij een aan Opdrachtnemer toerekenbare schending reeds aanspraak kan maken op schadevergoeding. Cumulatie van een boete en schadevergoeding kan leiden tot dubbele compensatie en een risico dat niet in redelijke verhouding staat tot de aard en omvang van de dienstverlening. Kan Opdrachtgever daarom instemmen met het vervallen van artikel 17.5?	Nee. Zie het antwoord op vraag 465.
470.	Bijlage 4 – ARBIT-2022 art. 17 Geheimhouding	Is de KB bereid de boete van € 50.000 per overtreding te maximeren, zowel per gebeurtenis als in totaal, en te bevestigen dat een verbeurde boete in mindering strekt op een eventuele schadevergoeding?	Gedeeltelijk. De boete wordt niet gemaximeerd (zie het antwoord op vraag 465). Een betaalde boete strekt wel in mindering op eventueel verschuldigde schadevergoeding (zie het antwoord op vraag 444).

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
471.	Bijlage 4 – ARBIT-2022 art. 17 Geheimhouding	Ter voorkoming van misverstanden stellen wij voor om aan artikel 17.5 het volgende toe te voegen: “Samenhangende gebeurtenissen zullen tezamen aangemerkt worden als één overtreding”.	Dat is akkoord.
472.	Bijlage 4 – ARBIT-2022 art. 18 Verwerking gegevens	Op grond van dit artikel dient Wederpartij persoonsgegevens te verwerken in opdracht en op basis van schriftelijke instructies van Opdrachtgever. Dergelijke instructies zijn niet passend bij een rol als verwerkingsverantwoordelijke. Wij verzoeken u derhalve het artikel als volgt aan te vullen: “Voor zover Wederpartij in het kader van de Overeenkomst persoonsgegevens verwerkt ten behoeve van Opdrachtgever houdt hij zich aan de geldende wet- en regelgeving op het terrein van het beschermen van persoonsgegevens. Indien Wederpartij als verwerker kwalificeert, verwerkt zij persoonsgegevens in voorkomend geval uitsluitend in opdracht en op basis van schriftelijke instructies van Opdrachtgever, tenzij er sprake is van andersluidende wettelijke voorschriften.” Kunt u hiermee instemmen?	Akkoord.
473.	Bijlage 4 – ARBIT-2022 art. 18 Verwerking gegevens	Op grond van dit artikel betrekken partijen elkaar bij het voeren van verweer tegen aanspraken van derden. Wij wensen deze mogelijkheid optioneel te maken, zodat partijen per aanspraak kunnen beoordelen of het betrekken van de andere partij zinvol is. Wij verzoeken u derhalve het artikel als volgt aan te vullen: “Partijen kunnen elkaar betrekken bij het voeren van verweer tegen aanspraken van derden in verband met de verwerking van persoonsgegevens in het kader van de Overeenkomst.” Kunt u hiermee instemmen?	Nee, dat is niet akkoord.
474.	Bijlage 4 – ARBIT-2022 art. 19 Beveiligingsprocedures	"Op grond van artt. 19.1, 19.2 en 19.3 ARBIT-2022 dienen de medewerkers van Opdrachtnemer de beveiligingsprocedures en huisregels van Opdrachtgever in acht te nemen, kan Opdrachtgever een VOG verzoeken van de Personeel van Wederpartij en is Opdrachtgever gerechtigd het personeel van Opdrachtnemer aan een	De beveiligingsprocedures en huisregels van de KB worden bij aanvang van de dienstverlening aan Opdrachtnemer verstrekt. Het op verzoek verstrekken van een VOG is voldoende.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		veiligheidsonderzoek te onderwerpen. Opdrachtgever kan op grond van de uitkomsten daarvan de inzet van het betrokken personeelslid bij de uitvoering van de opdracht/overeenkomst weigeren. Opdrachtnemer wenst graag duidelijkheid over de beveiligingsprocedures, huisregels en het veiligheidsonderzoek. Kunt u ons hierover nader informeren? Opdrachtnemer merkt hierbij op dat zij een uitvoerige pre employment screening laat uitvoeren bij haar werknemers voordat zij in dienst treden, waarvan het aanleveren van een VOG onderdeel is. Bent u bereid om uw optie tot het verlangen van een VOG en veiligheidsonderzoek achterwege te laten op grond van het feit dat voornoemde pre-employment screening door opdrachtnemer voldoende waarborgen biedt? "	
475.	Bijlage 4 – ARBIT-2022 art. 19 Beveiligingsprocedures	Op grond van dit artikel kunt u onze medewerkers (doen) onderwerpen aan een veiligheidsonderzoek. Wij onderwerpen onze werknemers aan een Pre-employment screening en kunnen desgewenst een VOG van onze werknemers overleggen. Onzes inziens is uw belang hiermee voldoende gewaarborgd. Kunt u er gelet op vorenstaande mee instemmen om artikel 19.3 ARBIT buiten toepassing te verklaren?	Zie het antwoord op vraag 474.
476.	Bijlage 4 – ARBIT-2022 art. 19 Beveiligingsprocedures	Dit artikel bepaalt dat u kunt vorderen dat onze werknemers voor aanvang van de werkzaamheden een Verklaring Omtrent Gedrag (hierna: VOG) aan u zullen overleggen. Kunt u aangeven of het voor u noodzakelijk is om een VOG te ontvangen? Wij dienen namelijk, net als u, de wettelijke verplichtingen uit de Algemene verordening gegevensbescherming te volgen. Wij zijn derhalve slechts bereid om een VOG van onze medewerkers te overleggen indien dat voor u noodzakelijk is en u een gerechtvaardigd belang heeft voor de verwerking van deze persoonsgegevens. Als zelfstandig verwerkingsverantwoordelijke ligt de verantwoordelijkheid voor deze rechtmatigheidstoets bij u maar wij willen graag bevestigd zien dat	Ja. Gelet op de aard van de werkzaamheden (toegang tot systemen en kennis van kwetsbaarheden) acht de KB een VOG noodzakelijk (zie E28).

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		deze toets ook heeft plaatsgevonden alvorens wij de VOG's van onze medewerkers verstrekken. Kunt u dit bevestigen?	
477.	Bijlage 4 – ARBIT-2022 art. 19 Beveiligingsprocedures	Wij nemen de privacy van onze medewerkers serieus. Privacygevoelige informatie van onze medewerkers, zoals een VOG, wordt centraal en beveiligd opgeslagen binnen onze organisatie. Zodra een VOG in ons systeem wordt opgenomen, informeren wij u dat voor de betreffende medewerker een VOG bij ons aanwezig is. Desgewenst kunt u hierin inzage vragen. De VOG zal dus niet fysiek aan u worden verzonden. Kunt u daarmee instemmen? Kunt u dat bevestigen? Zo niet, dan verzoeken wij u dat duidelijk te motiveren.	Akkoord. Opdrachtnemer beheert de VOG's en toont deze alleen op verzoek van de KB aan (zie E28).
478.	Bijlage 4 – ARBIT-2022 art. 19 Beveiligingsprocedures	Het aanvragen van een Verklaring omtrent het Gedrag neemt enige tijd in beslag. Om vertraging te voorkomen stellen wij voor om in spoedeisende gevallen de inzet te laten starten met het overleggen van een bewijs van aanvraag. Direct na ontvangst van de VOG zal dit worden medegedeeld aan Opdrachtgever. Kunt u met deze procedure instemmen? Kunt u dat bevestigen? Zo niet, dan verzoeken wij u dat duidelijk te motiveren.	Nee, dat is niet akkoord. De medewerker beschikt bij aanvang van de werkzaamheden over een geldige VOG.
479.	Bijlage 4 – ARBIT-2022 art. 21 Publicaties	Op grond van dit artikel is het ons niet toegestaan in publicaties of reclame-uitingen melding te maken van de Prestatie of uw naam te gebruiken als referentie, tenzij wij daarvoor toestemming hebben ontvangen van u. Wij wensen dit artikel wederkerig te maken. Ook u mag de naam van Wederpartij niet openbaren, tenzij wij daarvoor schriftelijke toestemming hebben gegeven. Kunt u gelet op bovenstaande instemmen met het wederkerig maken van artikel 21?	Akkoord. De KB maakt in publicaties of reclame-uitingen geen melding van de Prestatie en gebruikt de naam van Opdrachtnemer niet, dan na voorafgaande toestemming van Opdrachtnemer, behoudens wettelijke verplichtingen (zoals de Wet open overheid).
480.	Bijlage 4 – ARBIT-2022 art. 21 Publicaties	Is Opdrachtgever bereid om de vereiste toestemming op voorhand aan ons te verlenen, onder de voorwaarde dat wij terughoudend en in beperkte vorm - intern danwel extern - uitingen mogen doen	Nee. De KB beoordeelt een verzoek om toestemming per geval.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		over (bereikte) successen/resultaten betreffende de opdracht dan wel de naam van Opdrachtgever mogen gebruiken als referentie?	
481.	Bijlage 4 – ARBIT-2022 art. 21 Publicaties	Is het Opdrachtnemer toegestaan de KB, na voorafgaande toestemming, op te geven als referentie in toekomstige aanbestedingen, uitsluitend niet-publiek richting de betreffende aanbestedende dienst?	Ja, na voorafgaande schriftelijke toestemming van de KB per geval (zie ook E4).
482.	Bijlage 4 – ARBIT-2022 art. 22 Vervanging Personeel	Op grond van dit artikel hebben wij uw instemming nodig voor het vervangen van onze werknemers. Wij achten het redelijk dat wij de mogelijkheid hebben te beslissen welke werknemers wij op verschillende opdrachten inzetten en deze gedurende de looptijd van de overeenkomst naar eigen inzicht te veranderen. Een instemmingsvereiste voor het vervangen van werknemers beperkt onze mogelijkheden daarin. Uiteraard zullen wij ervoor zorgdragen dat een werknemer altijd vervangen wordt door iemand met een vergelijkbare deskundigheid, opleiding en ervaring. Wij verzoeken u daarom dit artikel te vervangen door het volgende: “Het staat Opdrachtnemer vrij personeelsleden tijdelijk of definitief te vervangen.”	Nee, dat is niet akkoord. Vervanging van Personeel is mogelijk, met voorafgaande toestemming van de KB (artikel 22.1 ARBIT-2022). Daarbij is artikel 22.4 ARBIT-2022 van toepassing.
483.	Bijlage 4 – ARBIT-2022 art. 22 Vervanging Personeel	Geldt de toestemmingsvereiste voor vervanging van Personeel uitsluitend binnen een lopende Nadere Opdracht? Is het toegestaan per Nadere Opdracht een team samen te stellen uit een vooraf aan de KB kenbaar gemaakte pool van medewerkers?	Ja. Artikel 22 ARBIT-2022 ziet op de vervanging van Personeel binnen een lopende Nadere Opdracht. Per Nadere Opdracht stelt Opdrachtnemer het team voor in de offerte (E20); dit team moet voldoen aan E26 tot en met E28.
484.	Bijlage 4 – ARBIT-2022 art. 23 en 24 Onderaanneming en overdracht	Artikel 23, onderaannemers Kan Opdrachtgever instemmen met algemene voorafgaande toestemming voor de in de Inschrijving of een bijlage genoemde onderaannemers en gelieerde ondernemingen, en voor latere wijzigingen na voorafgaande kennisgeving? Kan tevens worden bevestigd dat bezwaar uitsluitend binnen een redelijke termijn en op	Gedeeltelijk. De vermelding van een Onderaannemer in de Inschrijving geldt na gunning als toestemming als bedoeld in artikel 23.1 ARBIT-2022 (zie het antwoord op vraag 262). Voor andere of nieuwe Onderaannemers en gelieerde ondernemingen is voorafgaande toestemming van de KB vereist; de overige voorwaarden worden niet overgenomen.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		concrete juridische, beveiligings- of continuïteitsgronden kan worden gemaakt?	
485.	Bijlage 4 – ARBIT-2022 art. 23 en 24 Onderaanneming en overdracht	Opdrachtnemer gaat er vanuit dat overdracht van rechten en verplichtingen binnen het concern van Opdrachtnemer mogelijk is zonder toestemming? Is Opdrachtgever hiermee akkoord?	Nee, dat is niet akkoord. Ondernemingen binnen het concern van Opdrachtnemer gelden als derden in de zin van artikel 24 ARBIT-2022.
486.	Bijlage 4 – ARBIT-2022 art. 23 en 24 Onderaanneming en overdracht	Wij zouden graag de mogelijkheid hebben om ondernemingen behorende tot ons concern te betrekken in de uitvoering van de overeenkomst. Wij verzoeken u daarom om op te nemen dat onder 'derden' niet wordt verstaan vennootschappen die eveneens deel uitmaken van het concern waartoe Opdrachtnemer behoort. Bent u daartoe bereid? Zo niet, waarom niet?	Nee. Inzet van concernondernemingen is mogelijk als Onderaannemer, met inachtneming van artikel 23 ARBIT-2022. Zie het antwoord op vraag 485.
487.	Bijlage 4 – ARBIT-2022 art. 26 Aansprakelijkheid	"Art. 26.2 ARBIT-2022 beperkt de aansprakelijkheid voor persoons- en zaakschade en daaruit voortvloeiende schade tot EURO 1.250.000, - per gebeurtenis. Art. 26.3 ARBIT-2022 geeft aan, dat de aansprakelijkheid voor schade die geen persoons- of zaakschade is (dus bijvoorbeeld alle gevolgschade), is beperkt tot een bedrag van ten hoogste viermaal de hoogte van de vergoeding per gebeurtenis. Daarmee staan de opdrachtwaarde en het voor opdrachtnemer te accepteren risico niet met elkaar in verhouding, althans is het risico niet proportioneel in verhouding met de baten. Daarnaast is het totaal aantal gebeurtenissen niet gemaximeerd tot een bedrag of tot een periode (per contractjaar). Normaal gesproken wordt in onze branche de aansprakelijkheid voor directe schade beperkt tot een bedrag van maximaal eenmaal de door opdrachtgever voor de diensten verschuldigde en betaalde vergoedingen. Dit behoudens opzet of bewuste roekeloosheid van opdrachtnemer. Aansprakelijkheid voor indirecte schade pleegt geheel te worden uitgesloten. Wij stellen voor dat in afwijking van artt. 26.2 en 26.3 ARBIT-2022- een redelijke en marktconforme aansprakelijkheidsbeperking wordt overeengekomen (zoals ook de Gids Proportionaliteit voorschrijft) waarbij de maximum	Nee, dat is niet akkoord. Gelet op de aard van de werkzaamheden (het actief testen van applicaties en (productie)omgevingen van de KB) acht de KB de aansprakelijkheidsregeling van artikel 26 ARBIT-2022 proportioneel en maakt geen onderscheid tussen directe en indirecte schade. De KB is aanvullend wel bereid om overeen te komen dat de aansprakelijkheid voor persoons- en zaakschade (artikel 26.2 ARBIT-2022) per kalenderjaar is beperkt tot in totaal € 2.500.000,-.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		aansprakelijkheid in redelijke verhouding staat tot het met de nadere opdracht gemoeide honorarium. Graag vernemen wij of u akkoord gaat met het opnemen van de volgende bepaling: “Wederpartij zal de Opdracht naar beste kunnen verrichten en daarbij de zorgvuldigheid in acht nemen die van haar kan worden verwacht. Wederpartij is slechts aansprakelijk indien Opdrachtgever aantoont dat Opdrachtgever schade heeft geleden door een wezenlijke fout van Wederpartij. De aansprakelijkheid van Wederpartij voor directe schade van Opdrachtgever is beperkt tot een bedrag gelijk aan één (1) maal de Vergoeding voor de Nadere Opdracht in verband waarmee de toerekenbare tekortkoming is ontstaan, behoudens opzet dan wel bewuste roekeloosheid aan de zijde van leidinggevend personeel van Wederpartij. Aansprakelijkheid van Wederpartij voor indirecte schade (waaronder, maar niet beperkt tot gederfde winst, gemiste besparingen, schade door bedrijfsstagnatie) is uitgesloten, behoudens opzet dan wel bewuste roekeloosheid aan de zijde van leidinggevend personeel van Wederpartij.” Art. 26.4 ARBIT-2022 zou moeten worden beperkt tot: “... (c) in geval van schending van intellectuele eigendomsrechten als bedoeld in art. 8 ARBIT-2022.” De overige gevallen (a), (b) en (d) blijven buiten toepassing. Bent u hiertoe bereid? ”	
488.	Bijlage 4 – ARBIT-2022 art. 26 Aansprakelijkheid	De aansprakelijkheid voor persoons- en zaakschade en daaruit voortvloeiende schade is beperkt tot een bedrag per gebeurtenis, het aantal gebeurtenissen is echter onbeperkt. Graag dit artikel als volgt aanpassen: De in artikel 26.1 bedoelde aansprakelijkheid voor persoons- en zaakschade is beperkt tot de directe schade en tot een bedrag van EURO 1.250.000,– per gebeurtenis met een maximum van EURO 2.500.000,=. Samenhangende aanspraken worden daarbij aangemerkt als één gebeurtenis. De aansprakelijkheid van partijen voor gevolgschade en/of indirecte schade is uitgesloten. Onder gevolgschade en/of indirecte schade wordt onder andere verstaan gederfde winst, gemiste besparingen, geleden verlies, verminderde goodwill, en schade door bedrijfsstagnatie.	Zie het antwoord op vraag 487.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		Is Opdrachtgever hiermee akkoord?	
489.	Bijlage 4 – ARBIT-2022 art. 26 Aansprakelijkheid	Dit artikel bepaalt dat de aansprakelijkheid voor persoons- of zaakschade is beperkt tot € 1.250.000 per gebeurtenis. In voorkomend geval leidt dit tot een aansprakelijkheid van een veelvoud van de fee die niet meer in redelijke verhouding staat. Wanneer de fee bijvoorbeeld € 50.000 is, is de mogelijke maximale aansprakelijkheid 25 keer de fee. Binnen onze branche is het gebruikelijk de aansprakelijkheid per jaar te beperken tot driemaal het honorarium voor het verrichten van de werkzaamheden. In dit geval kunnen wij echter instemmen met een algemene aansprakelijkheidsbeperking van vier keer de fee per jaar. We stellen daarom voor de aansprakelijkheid als genoemd in artikel 26.3 in algemene zin te laten gelden, waarbij de vergoeding per jaar als uitgangspunt wordt genomen. Dit zou ertoe leiden dat de artikelen 26.2 en 26.3 samengevoegd kunnen worden tot de volgende bepaling: “De aansprakelijkheid van Partijen is beperkt tot een bedrag van ten hoogste viermaal de hoogte van de Vergoeding per gebeurtenis, waarbij voor wat betreft de Vergoeding alleen dat gedeelte in aanmerking wordt genomen dat betrekking heeft op de laatste twaalf (12) maanden waarin die Prestatie is verricht. Samenhangende gebeurtenissen worden daarbij aangemerkt als één gebeurtenis.” Uiteraard is deze beperking (conform artikel 26.4) onder andere niet aan de orde in geval van dood of letsel of opzet of grove schuld. Kunt u instemmen met de hiervoor voorgestelde wijziging?	Zie het antwoord op vraag 487.
490.	Bijlage 4 – ARBIT-2022 art. 26 Aansprakelijkheid	Artikel 26.2, persoons- en zaakschade Kan Opdrachtgever instemmen met een geaggreerd maximum per contractjaar van EUR 2.500.000 voor aansprakelijkheid wegens persoons- en zaakschade, waarbij samenhangende gebeurtenissen als één gebeurtenis gelden?	Ja. Zie het antwoord op vraag 487.
491.	Bijlage 4 – ARBIT-2022 art. 26 Aansprakelijkheid	De aansprakelijkheid voor schade anders dan die bedoeld in artikel 26.2 is beperkt tot een bedrag per gebeurtenis, het aantal	Zie het antwoord op vraag 487.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		gebeurtenissen is echter onbeperkt. Graag dit artikel als volgt aanpassen: De in artikel 26.1 bedoelde aansprakelijkheid voor schade anders dan die bedoeld in artikel 26.2 is beperkt tot de directe schade en tot een bedrag van maximaal éénmaal de hoogte van de Vergoeding ongeacht het aantal gebeurtenissen. Opdrachtnemer is niet aansprakelijk voor gevolgschade en/of indirecte schade. Onder gevolgschade en/of indirecte schade wordt in ieder geval verstaan gederfde winst, gemiste besparingen, geleden verlies, verminderde goodwill, en schade door bedrijfsstagnatie. Is Opdrachtgever hiermee akkoord?	
492.	Bijlage 4 – ARBIT-2022 art. 26 Aansprakelijkheid	Wij kunnen slechts aansprakelijkheid aanvaarden voor directe schade die redelijkerwijs in verhouding staat tot de opdrachtwaarde van de te leveren werkzaamheden. Uit de toelichting op de ARBIT blijkt ook dat de mogelijkheid bestaat om de aansprakelijkheid nader te beperken indien o.a. de aard van de prestatie daartoe aanleiding geeft. Daarnaast is in het geval van een duurovereenkomst, een overeenkomst op naclaculatiebasis of bijvoorbeeld een raamovereenkomst niet helder wat er verstaan moet worden onder de ‘Vergoeding’. Het lijkt ons niet redelijk dat wanneer er sprake is van toerekenbare tekortkoming onder een Nadere Overeenkomst met een vergoeding van bijvoorbeeld EUR 250.000,- de aansprakelijkheid daarvoor viermaal de totale Vergoeding onder de Raamovereenkomst (dus alle Nadere Overeenkomsten tezamen) is. Wij stellen daarom de volgende aanpassing voor: “De in artikel 26.1 bedoelde aansprakelijkheid voor schade anders dan die bedoeld in artikel 26.2 is [per nadere overeenkomst] per jaar beperkt tot een bedrag van ten hoogste de betaalde vergoedingen voor de door Opdrachtnemer verrichte werkzaamheden [met betrekking tot de betreffende nadere overeenkomst] in het jaar voorafgaand aan de schade toebrenkende gebeurtenis. Daarnaast geldt dat de totale aansprakelijkheid van Wederpartij onder de Overeenkomst [en alle daaronder te sluiten nadere overeenkomsten]	Zie het antwoord op vraag 487.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		een bedrag van EUR [100% contractwaarde per jaar], - per kalenderjaar nimmer te boven zal gaan.” Kunt u dat bevestigen? Zo niet, dan verzoeken wij u dat duidelijk te motiveren en/of een redelijk alternatief te vermelden.	
493.	Bijlage 4 – ARBIT-2022 art. 26 Aansprakelijkheid	Wat geldt in het kader van deze Raamovereenkomst als 'Vergoeding' in de zin van artikel 26.3 ARBIT-2022: de waarde van de betreffende Nadere Overeenkomst of de maximale waarde van de Raamovereenkomst (€ 500.000)? Is de KB bereid de Vergoeding van de betreffende Nadere Overeenkomst te hanteren, met een totaalmaximum per kalenderjaar dat aansluit op de verzekerde som?	Zie het antwoord op vraag 214.
494.	Bijlage 4 – ARBIT-2022 art. 26 Aansprakelijkheid	Artikel 26.3, overige schade Kan Opdrachtgever instemmen met beperking van de aansprakelijkheid voor overige schade tot eenmaal de onder de schadeveroorzakende Nadere Overeenkomst betaalde of verschuldigde Vergoeding per gebeurtenis en per contractjaar, met een absoluut maximum van EUR 1.000.000? Kan tevens worden bevestigd dat één oorzaak of samenhangende reeks van oorzaken als één gebeurtenis geldt?	Zie het antwoord op vraag 487.
495.	Bijlage 4 – ARBIT-2022 art. 26 Aansprakelijkheid	Is de KB bereid aansprakelijkheid voor indirecte schade en gevolgschade (waaronder gedeelde inkomsten, reputatieschade en kosten van herstel of reconstructie van gegevens) uit te sluiten?	Zie het antwoord op vraag 487.
496.	Bijlage 4 – ARBIT-2022 art. 26 Aansprakelijkheid	Artikel 26, indirecte schade Kan Opdrachtgever instemmen met uitsluiting van aansprakelijkheid voor indirecte schade en gevolgschade, waaronder gedeelde winst, omzetverlies, gemiste besparingen, verlies van goodwill, verlies van contracten en bedrijfsstagnatie, behoudens voor zover uitsluiting op grond van dwingend recht niet is toegestaan?	Zie het antwoord op vraag 487.
497.	Bijlage 4 – ARBIT-2022 art. 26 Aansprakelijkheid	Opdrachtnemer aanvaardt geen onbeperkte aansprakelijkheid voor schade voor de onder a, c en d van dit artikel opgenomen	Zie het antwoord op vraag 487.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		omstandigheden. Deze dienen te vallen onder de aansprakelijkheidsbeperking van (het tekstvoorstel bij) artikel 26.2 en 26.3. Is Opdrachtgever hiermee akkoord?	
498.	Bijlage 4 – ARBIT-2022 art. 26 Aansprakelijkheid	Op grond van dit artikel komt de aansprakelijkheidsbeperking te vervallen indien sprake is van een schending van intellectuele eigendomsrechten als bedoeld in artikel 8 ARBIT. Wij wensen op dergelijke vorderingen de aansprakelijkheidsbeperking van toepassing te verklaren en derhalve artikel 26.4.c buiten toepassing te verklaren. Kunt u hiermee instemmen?	Zie het antwoord op vraag 487.
499.	Bijlage 4 – ARBIT-2022 art. 26 Aansprakelijkheid	In dit artikel worden gevallen beschreven wanneer de aansprakelijkheidsbeperking komt te vervallen. Wij zijn alleen bereid een onbeperkte aansprakelijkheid te accepteren voor eventuele verhaalsacties op grond van artikel 82 AVG. Overigens menen wij dat een verhaalsactie op grond van artikel 82 AVG niet aan de orde zal zijn c.q. niet zal slagen, aangezien partijen zelfstandig verwerkingsverantwoordelijke zijn en niet betrokken bij dezelfde verwerking (zoals lid 4 van artikel 82 AVG vereist). Bovendien is het verhalen van boetes niet conform de werking van de AVG. Boetes die opgelegd kunnen worden door een toezichthoudende autoriteit zijn geregeld in artikel 83 AVG. Boetes kunnen opgelegd worden aan een verwerker of een verwerkingsverantwoordelijke indien er gehandeld is in strijd met een (beboetbare) verplichting op grond van de AVG. De door u opgenomen zin suggereert echter dat een partij een boete opgelegd kan krijgen die toerekenbaar is aan een andere partij en dat de eerste partij daarom het recht moet hebben om de boete te verhalen. Er is echter geen juridische grondslag op grond waarvan de opdrachtgever een boete opgelegd krijgt die toerekenbaar is aan opdrachtnemer. Opdrachtgever kan alleen een boete opgelegd krijgen indien zij zelf een op haar rustende verplichting geschonden heeft. Dit geldt ongeacht of er sprake is van een verwerker – verwerkingsverantwoordelijke verhouding tussen partijen of dat er sprake is van een verhouding tussen twee	Nee, de KB wenst dit niet aan te passen. Zie ook het antwoord op vraag 41. Er zal eerst vastgesteld worden of er sprake is van een verwerkersrelatie.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		verwerkingsverantwoordelijken. Kunt u instemmen met het wijzigen van artikel 26.4.d ARBIT als volgt: “In geval van een verhaalsactie op grond van artikel 82 AVG.”	
500.	Bijlage 4 – ARBIT-2022 art. 26 Aansprakelijkheid	Dat de aansprakelijkheidsbeperking komt te vervallen in geval van schending van de verwerkersovereenkomst vinden wij niet redelijk. Een onbeperkte aansprakelijkheid is voor Opdrachtnemer niet verzekeraar en is ook niet in lijn met de Gids Proportionaliteit. Wij stellen voor om lid d te schrappen en in de verwerkersovereenkomst op te nemen: ‘De tussen Partijen in de Overeenkomst overeengekomen beperkingen en uitsluitingen van aansprakelijkheid is van overeenkomstige toepassing op deze verwerkersovereenkomst.’ Kunt u daarmee instemmen? Zo niet, dan verzoeken wij u dat duidelijk te motiveren en/of een redelijk alternatief te vermelden.	Nee, de KB wenst dit niet aan te passen. Zie ook het antwoord op vraag 41. Er zal eerst vastgesteld worden of er sprake is van een verwerkersrelatie.
501.	Bijlage 4 – ARBIT-2022 art. 26 Aansprakelijkheid	Bij de uitvoering van pentesten komt Opdrachtnemer hooguit incidenteel in aanraking met persoonsgegevens. Op grond van artikel 26.4 sub d ARBIT-2022 is de aansprakelijkheid bij schending van privacywetgeving (inclusief boetes) onbeperkt. Is de KB bereid ook hiervoor een maximum te hanteren, bijvoorbeeld gelijk aan het maximum van artikel 26.3?	Nee, de KB wenst dit niet aan te passen. Zie ook het antwoord op vraag 41. Er zal eerst vastgesteld worden of er sprake is van een verwerkersrelatie.
502.	Bijlage 4 – ARBIT-2022 art. 26 Aansprakelijkheid	Artikel 26.4, carve-outs Kan Opdrachtgever instemmen met toepassing van een afzonderlijk geaggregeerd maximum op aansprakelijkheid wegens IE-inbreuk en gegevensbeschermingskwesties, bijvoorbeeld tweemaal de algemene aansprakelijkheidslimiet? Kan tevens worden bevestigd dat onbeperkte aansprakelijkheid wegens opzet of grove schuld uitsluitend geldt voor opzet of bewuste roekeloosheid van het leidinggevend personeel van Opdrachtnemer?	Nee. Zie het antwoord op vraag 487.
503.	Bijlage 4 – ARBIT-2022 art. 26 Aansprakelijkheid	Artikel 26.4(d), privacyboetes	Opdrachtnemer is aansprakelijk voor zover de schade (waaronder een boete) aan Opdrachtnemer is toe te

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		Kan Opdrachtgever bevestigen dat Opdrachtnemer uitsluitend aansprakelijk is voor toezichthouderboetes voor zover deze rechtstreeks en aantoonbaar zijn veroorzaakt door een aan Opdrachtnemer toerekenbare schending van specifiek op Opdrachtnemer rustende wettelijke verplichtingen of rechtmatige, gedocumenteerde instructies van Opdrachtgever?	rekenen (artikel 26.1 ARBIT-2022). Artikel 26.4 sub d ARBIT-2022 wordt niet gewijzigd.
504.	Bijlage 4 – ARBIT-2022 art. 26 Aansprakelijkheid	Wij zijn bereid een dergelijke vrijwaring te geven voor verplichtingen met betrekking tot Personeel van Opdrachtnemer echter niet voor die gevallen waarin de totstandkoming van desbetreffende verplichting is toe te rekenen aan Opdrachtgever. Zo gaan wij er bijvoorbeeld van uit dat Opdrachtgever het Personeel zal behandelen als een externe professional en niet als een eigen werknemer. Wij stellen daarom de volgende toevoeging aan de laatste volzin voor: “(...), voorzover de totstandkoming van de desbetreffende verplichting niet toerekenbaar is aan Opdrachtgever.” Kunt u daarmee instemmen? Zo niet, dan graag een toelichting.	Akkoord.
505.	Bijlage 4 – ARBIT-2022 art. 26 Aansprakelijkheid	Ter voorkoming van misverstanden stellen we voor toe te voegen: “Partijen aanvaarden slechts aansprakelijkheid, ongeacht de grondslag daarvan, voor zover dat in dit artikel 26 is geregeld.” Akkoord? Zo niet, waarom niet?	Nee, dat is niet akkoord. Artikel 26 ARBIT-2022 regelt de aansprakelijkheid voor schade, maar is geen uitputtende regeling van de rechten van Partijen. De voorgestelde tekst zou afbreuk kunnen doen aan onder andere de bepalingen in de Raamovereenkomst.
506.	Bijlage 4 – ARBIT-2022 art. 26 Aansprakelijkheid	Om eventuele onduidelijkheid te voorkomen stellen wij voor om expliciet toe te voegen dat de beperking van aansprakelijkheid zoals hiervoor vermeld ook geldt in geval van garantie en vrijwaring: “De in artikel 26.2 en 26.3 opgenomen beperkingen en uitsluitingen van aansprakelijkheid gelden ook in geval van garantie en vrijwaring.” Kunt u dat bevestigen? Zo niet, dan verzoeken wij u dat duidelijk te motiveren en/of een redelijk alternatief te vermelden.	Akkoord, met uitzondering van de gevallen genoemd in artikel 26.4 ARBIT-2022.
507.	Bijlage 4 – ARBIT-2022 art. 27 Overmacht	Artikel 27, overmacht Kan Opdrachtgever bevestigen dat per geval wordt beoordeeld of een gebeurtenis buiten de redelijke invloedssfeer van Opdrachtnemer lag	Ja, conform artikel 27 ARBIT-2022. Artikel 27.2 ARBIT-2022 blijft onverkort van toepassing.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		en redelijkerwijs niet kon worden voorkomen of ondervangen, waaronder uitzonderlijke uitval van noodzakelijke infrastructuur, overheidsmaatregelen, grootschalige cyberincidenten en niet-toerekenbare tekortkomingen van essentiële derde leveranciers?	
508.	Bijlage 4 – ARBIT-2022 art. 29 Verzekering	Wij kunnen niet akkoord gaan met het bepaalde in artikel 29.3, daar wij geen mededelingen doen van eerdere claims onder de verzekering. Dit beschouwen wij als bedrijfsvertrouwelijke informatie. Wij verzoeken u daarom artikel 29.3 als volgt aan te passen: “Wederpartij overlegt op verzoek onverwijld bewijs van premiebetaling aan Opdrachtgever.” Kunt u hiermee instemmen?	Akkoord. Opdrachtnemer hoeft geen mededeling te doen van eerdere claims. Opdrachtnemer kan op verzoek volstaan met een verklaring van de verzekeraar waaruit blijkt dat Opdrachtnemer conform de gestelde eisen is verzekerd en de premie heeft voldaan.
509.	Bijlage 4 – ARBIT-2022 art. 29 Verzekering	Opdrachtnemer heeft de voor haar activiteiten gebruikelijke verzekeringen afgesloten. Opdrachtnemer verstrekt hierover geen details, zoals polisvoorwaarden, bewijzen van betaling of mededelingen over eerdere claims. Op verzoek van Opdrachtgever kan Opdrachtnemer een certificaat van verzekering aan Opdrachtgever verstrekken. Wij gaan er vanuit dat wij hiermee kunnen volstaan.	Akkoord. Zie het antwoord op vraag 508.
510.	Bijlage 4 – ARBIT-2022 art. 29 Verzekering	Als beursgenoteerde onderneming en op basis van de afspraken met onze verzekeraar kunnen wij helaas geen inzage geven in de polis, de bewijzen van premiebetaling of eventuele eerdere claims onder onze polis. Uit de toelichting op de ARBIT blijkt dat het mogelijk is om in plaats daarvan een kopie te verstrekken van het door de verzekeraar afgegeven certificaat waaruit blijkt dat de omvang van de verzekeringsdekking voldoet aan de door u gestelde verzekeringseis. Kunt u akkoord gaan met het verstrekken van een dergelijk certificaat?	Akkoord. Zie het antwoord op vraag 508.
511.	Bijlage 4 – ARBIT-2022 art. 30 Ontbinding en opzegging	Beëindiging van de overeenkomst zou naar onze mening slechts mogelijk kunnen zijn wanneer de ernst van de tekortkoming dit rechtvaardigt. Daarnaast heeft de term ‘ontbinden’ juridisch gezien het gevolg dat Opdrachtnemer de geleverde diensten moet	Nee, dat is niet akkoord. Ontbinding is uitsluitend mogelijk in de gevallen zoals bepaald in de Raamovereenkomst en de ARBIT-2022 (waaronder de artikelen 30.1, 30.3 en 30.4 ARBIT-2022). De KB ziet

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		terugnemen en het betaalde moet terugbetalen. Gelet op de aard van de opdracht is dit een slecht uitvoerbaar en voor beide Partijen onwenselijk en onredelijk gevolg. Wij verzoeken u daarom om in een apart artikellid aan de ARBIT toe te voegen: 'Voor zover in de Voorwaarden en de Overeenkomst wordt gesproken over 'ontbinden' geldt dat dit enkel geldt voor toekomstige verplichtingen en geen ongedaanmakingsverplichtingen met zich brengt.' Akkoord? Zo niet, waarom niet?	geen aanleiding af te wijken van de wettelijke gevolgen van ontbinding.
512.	Bijlage 4 – ARBIT-2022 art. 30 Ontbinding en opzegging	Ter voorkoming van misverstanden, kunt u bevestigen dat interne fusies of reorganisatie niet vallen onder "een ingrijpende wijziging in de zeggenschap over de activiteiten van de onderneming van Wederpartij"?	Ja, mits de uiteindelijke zeggenschap over de onderneming van Opdrachtnemer niet wijzigt.
513.	Bijlage 4 – ARBIT-2022 art. 30 Ontbinding en opzegging	Kan de KB bevestigen dat een interne herstructurering binnen een concern, waarbij de uiteindelijke zeggenschap niet wijzigt, niet wordt aangemerkt als een 'ingrijpende wijziging in de zeggenschap' in de zin van artikel 30.3 ARBIT-2022?	Ja. Zie het antwoord op vraag 512.
514.	Bijlage 4 – ARBIT-2022 art. 30 Ontbinding en opzegging	Naar onze mening is het redelijk dat de vergoeding in verhouding staat tot de ernst van de toerekenbaarheid. Anders zou immers een onevenredig groot risico bij Opdrachtnemer worden gelegd. Wij stellen de volgende aanpassing voor: "Indien Opdrachtgever echter aantoonbaar dat de onrechtmatigheid (mede) aan Wederpartij toerekenbaar is, komt Wederpartij een vergoeding toe die in verhouding staat tot de mate van toerekenbaarheid." Akkoord? Zo niet, dan graag een duidelijke motivering.	Akkoord.
515.	Bijlage 4 – ARBIT-2022 art. 30 Ontbinding en opzegging	Beëindiging dient naar onze redelijke mening slechts mogelijk te zijn indien de rechter daadwerkelijk overgaat tot vernietiging van de overeenkomst op grond van de aanbestedingswet. Wij stellen voor om de woorden "hij op goede gronden aanneemt dat" te schrappen. Stemt u daarmee in? Zoniet, dan graag een duidelijke motivering.	Nee, dat is niet akkoord. Indien de rechter de Overeenkomst vernietigt, is beëindiging niet meer aan de orde; de bepaling is juist bedoeld voor situaties waarin de KB de Overeenkomst op grond van het

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
			aanbestedingsrecht niet in stand mag laten, ook zonder rechterlijke uitspraak (artikel 73 Richtlijn 2014/24/EU).
516.	Bijlage 4 – ARBIT-2022 art. 30 Ontbinding en opzegging	"Art. 30.6 ARBIT-2022 eerste en tweede zin biedt de Opdrachtgever de mogelijkheid om een opdracht met onmiddellijke ingang eenzijdig te beëindigen. Dit is onredelijk en nadelig voor Opdrachtnemer. Graag zouden wij hier een redelijke opzegtermijn afspreken. Daarnaast zouden wij deze opzegmogelijkheid wederkerig willen maken, zodat ook Opdrachtnemer in een dringend geval kan opzeggen. Bent u bereid art. 30.6 ARBIT-2022 eerste en tweede zin te vervangen voor de volgende zinsnede: "De Overeenkomst kan door zowel Opdrachtgever als Wederpartij door middel van een aangetekend schrijven worden opgezegd met inachtneming van een redelijke termijn van ten minste vier weken. Indien Opdrachtgever opzegt vindt in dat geval afrekening plaats op basis van het bepaalde in artikel 30.7 t/m 30.9" "	Nee, dat is niet akkoord. Artikel 30.6 ARBIT-2022 blijft ongewijzigd. Bij opzegging van een Nadere Overeenkomst vindt afrekening plaats conform artikel 30.7 ARBIT-2022, op basis van de reeds door Opdrachtnemer uitgevoerde werkzaamheden.
517.	Bijlage 4 – ARBIT-2022 art. 30 Ontbinding en opzegging	Indien Opdrachtgever de opdracht met onmiddellijke ingang opzegt, worden wij onder meer geconfronteerd met vrijgekomen personeel, welke wij op dat moment niet direct bij een andere opdrachtgever zullen kunnen inzetten. Wij verzoeken u dan ook om ofwel te voorzien in een vergoeding voor leegloop van personeel ofwel een redelijke opzegtermijn van ten minste 3 maanden te hanteren. Bent u daartoe bereid? Zoniet, waarom dan niet en in hoeverre kunt u er dan wel mee instemmen?	Nee. Zie het antwoord op vraag 516.
518.	Bijlage 4 – ARBIT-2022 art. 30 Ontbinding en opzegging	In onderhavig geval is sprake van een Opdracht als bedoeld in artikel 30.7. Ingeval Opdrachtgever opzegt, is het aannemelijk dat wij schade lijden als bedoeld in de artikelen 30.8b en c. Wij stellen voor de artikelen 30.8b en c van overeenkomstige toepassing te verklaren op de afrekening als bedoeld in dit artikel 30.7. Stemt u daarmee in? Zoniet, dan graag een toelichting daarop.	Nee, dat is niet akkoord. Bij tussentijdse opzegging van een Nadere Overeenkomst vindt afrekening plaats conform artikel 30.7 ARBIT-2022, uitsluitend op basis van de reeds door Opdrachtnemer uitgevoerde werkzaamheden.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
519.	Bijlage 4 – ARBIT-2022 art. 30 Ontbinding en opzegging	Wat is de afwikkeling van lopende Nadere Opdrachten bij (tussentijdse) opzegging van de Raamovereenkomst? Worden deze afgerond onder de geldende voorwaarden, of worden reeds verrichte werkzaamheden en aangegane verplichtingen naar rato vergoed?	Lopende Nadere Overeenkomsten worden bij opzegging van de Raamovereenkomst uitgevoerd onder de geldende voorwaarden, tenzij de KB ook de betreffende Nadere Overeenkomst opzegt. In dat geval vindt afrekening plaats conform artikel 30.7 ARBIT-2022.
520.	Bijlage 4 – ARBIT-2022 art. 30 Ontbinding en opzegging	Artikel 30, beëindiging Kan Opdrachtgever bevestigen dat bij beëindiging van een Nadere Overeenkomst alle reeds uitgevoerde werkzaamheden, gemaakte kosten en niet-annuleerbare verplichtingen worden vergoed, tenzij de beëindiging rechtstreeks het gevolg is van een materiële en aan Opdrachtnemer toerekenbare tekortkoming?	Nee, dat wordt niet bevestigd. Zie het antwoord op vraag 519.
521.	Bijlage 4 – ARBIT-2022 art. 32 Exitclausule	In dit artikel is opgenomen dat opdrachtnemer alle ter hand gestelde documenten, etc. aan opdrachtgever moet retourneren. Kunt u bevestigen dat dit niet van toepassing is documenten, etc. die opgeslagen zijn in back-up media of andere elektronische gegevensopslag systemen in overeenstemming met algemene systeem archivering of back-up richtlijnen?	Ja, mits deze gegevens onder de geheimhoudingsverplichting blijven vallen en na afloop van de reguliere back-upcyclus worden verwijderd.
522.	Bijlage 4 – ARBIT-2022 art. 32 Exitclausule	Het bepaalde in deze artikelen is onzes inziens reeds afdoende geregeld in artikel 17.4 ARBIT. Om enige tegenstrijdigheid tussen de bepalingen te voorkomen, verzoeken wij u artikel 32.3 en 32.4 buiten toepassing te verklaren. Kunt u hiermee instemmen?	Nee, dat is niet akkoord.
523.	Bijlage 4 – ARBIT-2022 Bijzondere bepalingen	Opdrachtnemer gaat er vanuit dat gelet op de aard van de door Opdrachtgever gevraagde dienstverlening de navolgende bijzondere bepalingen niet van toepassing zijn: - Koop; - Gebruiksrechten; - Adviesdiensten; - Ontwikkeling maatwerkprogrammatuur; en - Onderhoud. Kan Opdrachtgever dit bevestigen?	Gedeeltelijk. De Bijzondere bepalingen Opdrachten (Opdrachten algemeen en Adviesdiensten) zijn van toepassing. De overige Bijzondere bepalingen (Koop, Gebruiksrechten, Ontwikkeling Maatwerkprogrammatuur, Detachering en Onderhoud) zijn niet van toepassing.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
524.	Bijlage 4 – ARBIT-2022 Bijzondere bepalingen	Welke bijzondere bepalingen van ARBIT-2022 zijn van toepassing op deze Opdracht? Wij gaan uit van 'Opdrachten – Adviesdiensten' en niet van Ontwikkeling Maatwerkprogrammatuur, Detachering of Onderhoud. Kan de KB tevens bevestigen dat artikel 12.3 (garantie van twaalf maanden) en artikel 12.7 (onderhoud tot 5 jaar na Acceptatie) niet van toepassing zijn op pentestrapportages?	Zie het antwoord op vraag 523. Artikel 12.7 ARBIT-2022 is niet van toepassing. Artikel 12.3 ARBIT-2022 is wel van toepassing (zie het antwoord op vraag 440).
525.	Bijlage 5 – Prijzenblad	Inschrijver neemt aan dat alle bedragen exclusief BTW ingevuld dienen te worden in het prijzenblad, klopt dat?	Ja, dat is correct.
526.	Bijlage 5 – Prijzenblad	Bevestigt de KB dat één all-in mandagtarief geldt voor alle rollen, senioriteitsniveaus en werkzaamheden op locatie?	Ja, dat wordt bevestigd.
527.	Bijlage 5 – Prijzenblad	Kan de KB bevestigen dat hetzelfde mandagtarief geldt voor alle rollen en activiteiten, waaronder inventarisatie na opdrachtverlening, uitvoering, senior betrokkenheid, kwaliteitscontrole, rapportage, rapportbespreking en projectcoördinatie?	Ja. Zie het antwoord op vraag 526.
528.	Bijlage 5 – Prijzenblad	Wanneer KB spreekt over het "all-in mandag tarief", wordt verwacht dat alle relevante kosten hierin zijn verwerkt? Denk hierbij aan licenties, reis- en verblijfskosten. Zo nee, ontvangen wij graag een lijst met zaken welke buiten dit tarief worden gelaten.	Ja, alle kosten zijn in het all-in tarief per mandag verwerkt (zie E54).
529.	Bijlage 5 – Prijzenblad	Kan KB bevestigen dat binnen de raamovereenkomst uitsluitend één uniform mandagtarief wordt gehanteerd en dat geen onderscheid mag worden gemaakt naar senioriteitsniveau van de ingezette medewerkers? Indien ja, hoe waarborgt KB dat inschrijvers die structureel senior medewerkers inzetten niet worden benadeeld ten opzichte van inschrijvers die hoofdzakelijk medior medewerkers inzetten, terwijl eis E26 uitsluitend de betrokkenheid van een senior functionaris voorschrijft?	Ja, dat wordt bevestigd. De KB heeft bewust gekozen voor één tarief per mandag, zodat Inschrijvers op dezelfde basis worden vergeleken. Het is aan Inschrijver om de inzet van zijn medewerkers in dit tarief te verwerken.
530.	Bijlage 5 – Prijzenblad	Het prijzenblad vraagt één all-in tarief per mandag, terwijl bij de uitvoering verschillende ervaringsniveaus kunnen worden ingezet.	Nee, dat is niet akkoord. Zie het antwoord op vraag 529.

Nota van Inlichtingen 1 – Pentesten

Nr.	Onderwerp	Vraag:	Antwoord:
		Bent u bereid het prijzenblad aan te passen zodat afzonderlijke junior-, medior- en seniortarieven per mandag van acht uur kunnen worden aangeboden? Wilt u daarbij uniforme definities van de ervaringsniveaus en een vaste weging of fictieve inzetverdeling voor de prijsbeoordeling vaststellen, zodat aanbieders op dezelfde uitgangspunten worden vergeleken?	
531.	Bijlage 7 en 8 – Beroep op Derden	Kunt u bevestigen dat, indien inschrijver geen beroep doet op de financiële en economische draagkracht van een Derde, dit document niet ingevuld/aangepast noch ingediend hoeft te worden?	Ja, dat wordt bevestigd.
532.	Bijlage 7 en 8 – Beroep op Derden	Kunt u bevestigen dat, indien inschrijver geen beroep doet op de technische en beroepsbekwaamheid van een Derde, dit document niet ingevuld/aangepast noch ingediend hoeft te worden?	Ja. Zie het antwoord op vraag 531.
533.	Bijlage 7 en 8 – Beroep op Derden	Dit document is als PDF beschikbaar gesteld. Er dienen door inschrijver gegevens te worden ingevuld. Kunt u daartoe dit document in MS Word beschikbaar stellen?	De KB stelt Bijlage 7 en 8 gelijktijdig met deze Nota van Inlichtingen alsnog in Word-formaat beschikbaar via TenderNed. De inhoud van deze Bijlagen is ongewijzigd.
534.	Bijlage 7 en 8 – Beroep op Derden	Dit document is als PDF beschikbaar gesteld. Er dienen door inschrijver gegevens te worden ingevuld. Kunt u daartoe dit document in MS Word beschikbaar stellen?	Zie het antwoord op vraag 533.
535.	Bijlage 9 – Crediteurenformulier	Dit formulier wordt nergens in het bestek toegelicht. Kunt u dat alsnog doen?	Het crediteurenformulier wordt gebruikt om de gegevens van Opdrachtnemer in de financiële administratie van de KB te registreren. Inschrijver vult het formulier in en dient het in bij de Inschrijving (zie paragraaf 7.4).