



Belastingdienst

BIJLAGE A – Specificatie van de opdracht

Behorende bij : Informatie Beveiliging Attack- & Penetratietesten 2023 (IB A&P 2023)

Versie : 1.0
Kenmerk : IUC23-011
Datum : 13-09-2023

INHOUDSOPGAVE

Hoofdstuk 1. Doel van dit document.....	4
1.1. Eisen en wensen	4
Hoofdstuk 2. Uitvoeringseisen	5
2.1. Verplichtingen belastingen, milieubescherming, arbeidsvoorwaarden	5
2.2. Verzekering	5
2.3. Maatschappelijk verantwoord inkopen	5
2.3.1. Klimaat.....	6
2.3.2. Circulariteit (inclusief biobased).....	6
2.3.3. Milieu	6
2.3.4. Ketenverantwoordelijkheid (ISV)	6
2.3.5. Diversiteit en Inclusie	8
2.3.6. Social return	8
2.3.7. Duurzaamheidsbijdrage opdrachtnemer	9
Hoofdstuk 3. Integriteit	12
3.1 Business Etiquette	12
Hoofdstuk 4. Financiële afspraken	13
4.1. Prijsmodel.....	13
4.2. Indexering Prijs.....	13
4.3. Elektronisch factureren (e-factureren).....	13
Hoofdstuk 5. Functionele eisen en wensen	15
5.1. Algemeen (voor alle Diensten)	15
5.1.1. Offerteprocedure.....	15
5.1.2. Sleutelfiguren van de Opdrachtnemer	16
5.1.3. Eisen en wensen uit te voeren Opdracht(en)	16
5.1.4. Eisen en wensen ten aanzien van kennisdeling	17
5.2. A&P testen	18
5.2.1. Sleutelfiguren	18
5.2.2. Plan van Aanpak.....	19
5.2.3. Onderzoeksrapport.....	19
5.2.4. Evaluatie	20
5.3. IB kaders.....	20
5.3.1. Gegevens.....	21
5.3.2. Personeel	22
5.3.3. Informatiesystemen	22
5.3.4. Veilige informatie-overdracht	23
Hoofdstuk 6. Contractmanagement en Rapportage	24
6.1. Inleiding.....	24
6.2.1. A&P testen	24

6.2.2. Rapportage	25
Hoofdstuk 7. Lijst van Bijlagen en Verklaringen	26

Hoofdstuk 1. Doel van dit document

Dit document beschrijft de eisen en wensen die de Aanbestedende dienst stelt in het kader van de Europese aanbesteding Informatie Beveiliging Attack- & Penetratietesten 2023 (IB A&P 2023). Dit document maakt integraal onderdeel uit van het Beschrijvend Document. En is als onderdeel van de Aanbestedingsstukken gepubliceerd op TenderNed als “Bijlage A - Specificaties van de opdracht”.

1.1. Eisen en wensen

De aanbestedende dienst heeft geen voorkeur voor bepaalde Inschrijvers, noch voor bepaalde merken, types, fabricaten, herkomst e.d. Als er wordt gerefereerd aan bepaalde fabricaten, merken, typen, specifieke standaarden en dergelijke, dan dient dit te worden gelezen met de toevoeging “of daaraan gelijkwaardig”.

Aan gunningseisen moet worden voldaan. Het niet voldoen aan een gunningseis betekent uitsluiting van verdere beoordeling en wordt de Inschrijving terzijde gelegd (knock-out criterium).

De wensen worden inhoudelijk beoordeeld door een beoordelingscommissie.

Eisen en wensen worden als volgt weergegeven:

GUE	Gunningseisen Aan een gunningseis moet ten tijde van de inschrijving worden voldaan. Het niet voldoen aan een Gunningseis leidt tot uitsluiting van de aanbestedingsprocedure en is dus een knock-out criterium. De gunningseisen zijn opgenomen in Bijlage A – Specificaties van de opdracht. In Bijlage VI – Conformiteitenlijst dient u per gunningseis aan te geven dat u onvoorwaardelijk akkoord gaat met de gunningseisen.
W	Wensen Wensen maken onderdeel uit van gunningscriteria op basis waarvan de economisch meest voordelige Inschrijving wordt bepaald.
UE	Uitvoeringseisen Voorwaarden waar Opdrachtnemer zich bij de uitvoering van de Opdracht aan dient te houden zijn uitvoeringseisen. De uitvoeringseisen zijn opgenomen in dit document. Door het indienen van een inschrijving gaat u onvoorwaardelijk akkoord met het voldoen aan de uitvoeringseisen gedurende de uitvoering van de overeenkomst.

Hoofdstuk 2. Uitvoeringseisen

In dit hoofdstuk zijn specifieke uitvoeringseisen opgenomen. De bepalingen in dit hoofdstuk hebben allemaal specifiek betrekking op de uitvoeringsperiode van de aanbesteedde opdracht.

2.1. Verplichtingen belastingen, milieubescherming, arbeidsvoorwaarden

UE1	Inschrijvers dienen bij het opstellen van hun inschrijving rekening te hebben gehouden met de verplichtingen uit hoofde van de bepalingen inzake de arbeidsbescherming en de arbeidsvoorwaarden die gelden in het land waar de opdracht wordt uitgevoerd, zoals bedoeld in artikel 2.81 lid 2Aw2012. Kennis omtrent die belastingen en milieubescherming, arbeidsvoorwaarden en arbeidsbescherming kunnen Inschrijvers, voor zover het gaat om uitvoering in Nederland, verkrijgen bij: - de Belastingdienst, www.belastingdienst.nl - het Ministerie van Infrastructuur en Milieu, www.rijksoverheid.nl/ministeries/ienm - het Ministerie van Sociale Zaken en Werkgelegenheid, www.rijksoverheid.nl/ministeries/szw.
-----	---

2.2. Verzekering

UE 2	Gezien de aard van de werkzaamheden acht de Opdrachtgever het noodzakelijk dat Inschrijver verzekerd is tegen bedrijfsaansprakelijkheid, dan wel bereid en in staat te zijn om bij gunning zich voor beroepsfouten te verzekeren met een dekking van € 1.000.000 of equivalente tegenwaarde, gedurende tenminste de looptijd van de opdracht. Op daartoe strekkend verzoek verstrekt de winnende Inschrijver bewijs van adequate verzekering dan wel een verklaring waaruit blijkt dat deze hiertoe bereid en in staat is de bij gunning af te sluiten.
------	--

2.3. Maatschappelijk verantwoord inkopen

UE 3	Inschrijver voldoet gedurende de gehele looptijd van de Overeenkomst aantoonbaar aan alle vigerende milieu en arbo wet- en regelgeving.
------	--

Het Inkoopuitvoeringscentrum (IUC) van de Belastingdienst heeft ambitie op het gebied van duurzaamheid. Zij wil klanten, behoeftezoekers en leveranciers begeleiden in het vormgeven van de duurzaamheidsaspecten in producten en diensten op het vlak van bedrijfsvoering, bij aanbestedingen en gedurende de looptijd van de contracten (maatschappelijk verantwoord inkopen).

De Rijksoverheid wil met het eigen handelen een bijdrage leveren aan de verduurzaming van Nederland. Door in de eigen bedrijfsvoering en inkoop duurzame oplossingen toe te passen, wil de Rijksorganisatie bijdragen aan de duurzame transitie van Nederland. Met haar manier van inkopen van producten en diensten stelt de Rijksoverheid zich ten doel:

- de gevolgen van klimaatverandering aanpakken;
- de ontwikkeling naar een circulaire (duurzame) economie versnellen;
- baankansen creëren voor mensen die minder makkelijk op de arbeidsmarkt komen.

Zie te dien aangaande de informatie van de rijksoverheid over maatschappelijk verantwoord ondernemen en inkopen: <https://www.rijksoverheid.nl/onderwerpen/zakendoen-met-het-rijk/maatschappelijk-verantwoord-ondernemen>

De thema's die voor deze aanbesteding van belang zijn, betreffen:

- Klimaat
- Circulair

- Milieu
- Ketenverantwoordelijkheid
- Diversiteit en Inclusie
- Social Return

De Opdrachtnemer wordt gevraagd om gedurende de looptijd van de overeenkomst een bijdrage te leveren op het gebied van duurzaamheid. Hier wordt aandacht aan geschonken tijdens de gunning van de overeenkomst.

2.3.1. Klimaat

Het gaat binnen dit thema om het voorkomen of minimaliseren van de uitstoot van CO₂ en andere broeikasgassen. Aspecten van dit thema zijn:

- Uitstoot van CO₂, methaan, lachgas en waterdamp;
- Energieverbruik en de transitie naar duurzame energiebronnen.

Mogelijke prestatie-indicatoren zijn de CO₂-voetafdruk of de hoeveelheid duurzaam opgewekte energie (percentage of kWh)

2.3.2. Circulariteit (inclusief biobased)

In een circulaire economie worden producten en materialen eendeloos hergebruikt, zodat afval niet meer bestaat. Hierdoor behouden producten en materialen hun waarde en wordt verspilling van grondstoffen voorkomen. Om inzet van fossiele, schaarse en niet duurzaam gewonnen grondstoffen te minimaliseren zijn biograndstoffen in een circulaire economie essentieel. Zo kunnen bijvoorbeeld bladeren van landbouwgewassen worden gebruikt om gevelplaten te maken.

Het gaat binnen dit thema om:

- Materialen en grondstoffen;
- Levensduurverlenging;
- Hoogwaardig hergebruik;
- Biobased materiaalgebruik.

Mogelijke prestatie-indicatoren zijn materiaalbesparing in m³ of kg, het percentage hergebruikt materiaal, de impact bepaald door een levenscyclusanalyse (LCA) of de mate waarin levensduurverlenging mogelijk is.

2.3.3. Milieu

Dit thema gaat over voorkomen van een negatieve impact op milieu of over het leveren van een positieve bijdrage. Aspecten van dit thema zijn:

- Lucht, water en bodem;
- Natuur en biodiversiteit;
- Ruimtegebruik, watergebruik en inzet van landbouwgrond.

2.3.4. Ketenverantwoordelijkheid (ISV)

De internationale sociale voorwaarden (ISV) richten zich op het voorkomen en aanpakken van misstanden op het gebied van arbeidsomstandigheden, mensenrechten en milieu in de toeleveringsketen. Deze voorwaarden vereisen dat leveranciers actie ondernemen om risico's hierop in de keten te verkleinen.

Aspecten van dit thema zijn:

- Geen dwangarbeid en kinderarbeid;
- Goede werkomstandigheden;
- Leefbaar loon en leefbaar inkomen;
- Geen discriminatie.

Mogelijke stappen zijn een risicoanalyse en plan van aanpak om risico's in de keten te prioriteren en mitigeren.

2.3.4.1. Internationale Sociale Voorwaarden

De Internationale Sociale Voorwaarden (ISV) dragen bij aan het uitbannen van sociale misstanden in de inkoopketen, zoals kinderarbeid, hongerlonen en onmenselijke werkomstandigheden. Via een proces van due diligence richten de ISV zich op het bevorderen van het naleven van de internationale arbeidsnormen en mensenrechten in de productieketen van Rijksleveranciers.

Voor nadere informatie zie “duediligence-handreikingvoorbedrijven-mei2017.pdf”, <https://www.pianoo.nl/sites/default/files/documents/documents/duediligence-handreikingvoorbedrijven-mei2017.pdf>. Door middel van het inschrijven op onderhavige aanbesteding committeert inschrijver zich aan het naleven van de ISV. Dit is aldus een uitvoeringsvoorwaarde.

Vragen over het toepassen van de ISV kunnen worden gesteld tijdens de aanbestedingsprocedure. De Opdrachtgever geeft zo nodig een toelichting in een Nota van Inlichtingen.

UE 4	Opdrachtnemer committeert zich aan bovenstaande zoals beschreven in paragraaf 2.3.4.1
UE 5	Opdrachtnemer verplicht zich om onderstaande gestelde normen te implementeren, voor zover uit die normen een verantwoordelijkheid voor Opdrachtnemer voortvloeit, door in het kader van de uitvoering van de Overeenkomst de navolgende werkzaamheden te verrichten. • De fundamentele arbeidsnormen, zoals vastgelegd in de conventies van de International Labour Organisation (ILO), inzake afschaffing van dwangarbeid en slavernij (29, 105), afschaffing van kinderarbeid (138, 182), vrijwaring van discriminatie op het werk en in beroep (100, 111), de vrijheid van vakvereniging en recht op collectief onderhandelen (87, 98). • De mensenrechten uit de Universele Verklaring van de Rechten van de Mens (UVRM) en uitwerkingen daarvan in bindende verdragen, die arbeids- en bedrijfsrelevant zijn.
UE 6	Risicoanalyse productieketen: Opdrachtnemer levert uiterlijk 3 maanden na de definitieve gunning van de opdracht een risicoanalyse van de risico's op schending van arbeids- en mensenrechten van de gehele keten.
UE 7	Plan van aanpak mitigeren risico's: Indien van toepassing levert Opdrachtnemer uiterlijk 6 maanden na de definitieve gunning van de opdracht een plan van aanpak op om de risico's die in de risicoanalyse zijn vermeld te mitigeren. In het plan van aanpak zijn opgenomen: • een overzicht en beschrijving van de inspanningen die de Opdrachtnemer zal leveren om de risico's te mitigeren; • een planning ten aanzien van de inspanningen die de Opdrachtnemer zal leveren; • (optioneel) een toelichting op het tot stand komen van het plan van aanpak, bijvoorbeeld informatie over de betrokkenheid van stakeholders.
UE 8	Jaarlijkse rapportage: Gedurende de contractperiode rapporteert de Opdrachtnemer jaarlijks ten opzichte van de ingangsdatum van de Overeenkomst over zijn inzet ten aanzien van het naleven van de ISV. Hieruit moet blijken dat de Opdrachtnemer een 'redelijke inspanning' heeft geleverd om de ISV na te leven. De rapportage moet tevens gelijktijdig openbaar worden gemaakt, al dan niet als onderdeel van een rapportage die een breder deel van de activiteiten van de Opdrachtnemer betreft, zoals een (duurzaamheids)jaarverslag. Openbaarmaking kan worden bereikt door plaatsing op de website van de Opdrachtnemer. De rapportage bevat in ieder geval:

- een risicoanalyse zoals beschreven onder 0;
 - de maatregelen die in het jaar waarover gerapporteerd wordt zijn genomen om risico's te verminderen en eventuele schendingen van de ISV in de keten te verhelpen;
 - de aanpak en resultaten van de monitoring op naleving van de ISV;
 - informatie over hoe eventueel ontvangen signalen (intern en extern) over schending van de ISV afgehandeld zijn. De rapportage is vormvrij.
- De rapportage is vormvrij, maar moet voor de bruikbaarheid ervan in het Nederlands- of Engels opgesteld zijn.

2.3.5. Diversiteit en Inclusie

Diversiteit gaat over de verscheidenheid aan mensen in een organisatie. Inclusie gaat over hoe diverse mensen tot hun recht komen en gewaardeerd worden. Samen zorgen zij voor een maatschappij met eerlijke kansen voor iedereen, het tegengaan van discriminatie en een representatieve overheid. Aspecten van dit thema zijn:

- Divers personeelsbestand in de (eigen) organisatie;
- Faciliteren van diverse werknemers;
- Representatieve beeldvorming;
- Sociale veiligheid;
- Toegankelijkheid.

Mogelijke prestatie-indicatoren zijn maatregelen die werknemerstevredenheid, de samenstelling of doorstroom van personeel bevorderen.

2.3.6. Social return

Social return is een aanpak om arbeidsparticipatie te stimuleren en meer werkgelegenheid te creëren voor mensen met een afstand tot de arbeidsmarkt. Sociale impact of 'social return on investment' kan je uitvragen door het:

- Stellen van sociale voorwaarden;
- Inkopen bij sociale ondernemingen of SW-bedrijven.

Een mogelijke maatregel is een percentage van de loonsom van een opdracht om personen met een afstand tot de arbeidsmarkt in te zetten.

Inschrijver dient bij de uitvoering van de opdracht aan social return bij te dragen door het creëren van extra werk(ervarings)plaatsen voor mensen met een grote(re) afstand tot de arbeidsmarkt. Voor deze aanbesteding wordt uitgegaan dat minimaal 5% van het totale aantal in te zetten uren van de overeenkomst wordt ingezet voor de doelgroep. De werkzaamheden dienen gerelateerd te zijn aan de opdracht. Voorafgaand aan het sluiten van de overeenkomst wordt afgestemd op welke wijze Inschrijver invulling gaat geven aan social return en hoe de invulling geverifieerd kan worden door de Opdrachtgever.

Bij social return gaat het om de volgende doelgroepen:

- Wet Werk en Bijstand (WWB) gerechtigden, die langer werkloos zijn dan 12 maanden, 50 jaar of ouder zijn en/of die zonder reïntegratieondersteuning of andere begeleiding niet zelfstandig aan werk kunnen komen;
- Werkloosheidwet (WW) gerechtigden, die langer werkloos zijn dan 12 maanden, en/of 50 jaar of ouder zijn;
- Wet Werk en Inkomen naar Arbeidsvermogen (WIA) gerechtigden;
- Regeling Werkhervatting Gedeeltelijk Arbeidsgeschikten (WGA) gerechtigden;
- Wet arbeidsongeschiktheid zelfstandigen (WAZ) gerechtigden;
- Wet arbeidsongeschiktheidsvoorziening Jonggehandicapten (Wajong) gerechtigden;
- Wet Inkomensvoorziening Oudere en gedeeltelijk Arbeidsongeschikte Werkloze werknemers (IOAW) gerechtigden;
- Wet Inkomensvoorziening Oudere en gedeeltelijk Arbeidsongeschikte gewezen Zelfstandigen (IOAZ) gerechtigden;
- Wet Sociale Werkvoorzieningen (WSW) geïndiceerden;
- Leer/werkplekken voor niet uitkeringsgerechtigde werkzoekenden (nuggers);

- Leer/werkplekken voor vroegtijdig schoolverlaters en jongeren met onvoldoende kwalificaties;
- Leer/werkplekken in het kader van BOL/BBL opleidingen, VSO en/of praktijkscholen.

UE 9	Voorafgaand aan het tekenen van de Overeenkomst komen Opdrachtnemer en de Opdrachtgever overeen op welke wijze invulling wordt gegeven aan social return.
GUE 1	Gedurende de looptijd van de overeenkomst besteedt de Inschrijver minimaal 5% van de aantal in te zetten uren van de overeenkomst aan extra werk(ervarings)plaatsen voor mensen uit genoemde social return doelgroepen.
UE 10	Opdrachtnemer stuurt aan de Opdrachtgever elk half jaar, uiterlijk 15 kalenderdagen na ommekomst van deze periode, geheel ingevuld en ondertekend een periodiek verantwoordingsformulier social return (overeenkomstig model toe. Dit periodiek verantwoordingsformulier social return is opgenomen als Bijlage X - Model verantwoording Social Return bij het Beschrijvend document.
UE 11	Wanneer op basis van de periodieke verantwoordingsformulieren de Opdrachtgever constateert dat de Opdrachtnemer gedurende de looptijd van de overeenkomst twee maal achtereenvolgend het percentage haalt genoemd als verplichting in GUE 1, kan de Opdrachtgever in overleg kan treden met Opdrachtnemer. Op basis van dit overleg: - Stellen de Opdrachtgever en de Opdrachtnemer de oorzaken vast voor het niet behalen van het genoemde percentage door de Opdrachtnemer. - Stellen de Opdrachtgever en de Opdrachtnemer maatregelen vast voor het verbeterd nakomen van de verplichting tot social return door de Opdrachtnemer.
UE 12	Bij het niet nakomen van de verplichting genoemd in GUE 1, kan de Opdrachtgever naar rato van de bijdrage social return die de Opdrachtnemer moest doen, betalingen inhouden of storten op de waarde van de overeenkomst, met uitzondering in die situaties dat het voldoen aan de verplichting genoemd in eis GUE 1 buiten de schuld van de Opdrachtnemer om niet lukt(e). De bewijslast rust te allen tijde bij de Opdrachtnemer.

2.3.7. Duurzaamheidsbijdrage opdrachtnemer

W 1	Duurzaamheid Inschrijver wordt gevraagd zijn onderscheidend vermogen te laten zien in een verifieerbare uiteenzetting van zijn bijdrage aan de duurzaamheidsdoelstellingen van de Rijksoverheid bij de uitvoering van de overeenkomst. Inschrijver dient in zijn uiteenzetting inzichtelijk te maken hoe hij aan de hand van gerealiseerde of binnenkort te realiseren acties rondom de bovengenoemde 6 thema's Opdrachtgever helpt in het bereiken van de gestelde doelen. 1) Inschrijver dient per thema aan te geven: - In hoeverre het thema relevant is, op basis waarvan dat wordt geconcludeerd en de mate waarin het thema relevanter is ten opzichte van de overige thema's (uitgedrukt in een relatieve score qua relevantie/rangorde); - Welke concrete acties reeds zijn gerealiseerd; - Welke acties in gang zijn gezet en binnen 6 maanden zullen zijn gerealiseerd alsmede hoe hierop wordt gestuurd; - Welke overige acties worden voorgenomen en welke afhankelijkheden er zijn om deze te kunnen realiseren; - Welke aantoonbare toegevoegde waarde op gebied van duurzaamheid de acties opleveren voor Opdrachtgever; - In welke mate de acties (kunnen) resulteren in een hoger tarief voor Opdrachtgever.
-----	--

	Opdrachtgever laat zich graag positief verrassen door extra (niet genoemde) doelstellingen en thema's op het gebied van duurzaamheid die voor Opdrachtgever van toegevoegde waarde zijn. Inschrijver wordt geadviseerd om bij de beantwoording gebruik te maken van de ambitieweb tool en -handleiding van PIANOo (https://www.pianoo.nl/nl/handreiking-aan-de-slag-met-het-ambitieweb) 2) Op welke wijze Opdrachtgever, zowel voor de gunning als bij de uitvoering van de overeenkomst, in staat is en wordt gesteld om de duurzaamheidsbijdrage van Inschrijver te verifiëren 3) welke algemene (niet op een thema betrekking hebbende) duurzaamheidsresultaten of -prestaties u kunt noemen die ter zake van toegevoegde waarde zijn. Denk bijvoorbeeld aan - een milieumanagement tool dat inschrijver in gebruik heeft zoals ISO 14001, EMAS of vergelijkbaar - doorgevoerde duurzaamheid in de eigen bedrijfsvoering bijvoorbeeld aan de hand van beoordelingsaspecten als: • Wat het huidige niveau is van de prestaties van de eigen bedrijfsvoering (waar mogelijk kwantitatief gemaakt a.d.h.v. CO2-emissies • De reeds behaalde resultaten in de afgelopen drie jaar t.a.v. het verbeteren van prestaties ondersteund met verifieerbare prestatie informatie; • De doelstellingen die de organisatie heeft m.b.t. de verduurzaming van de eigen bedrijfsvoering; Een plan van aanpak waarin de doelstellingen worden onderbouwd, al dan niet met beleidsdocumenten. Zie in de beantwoording toe op volledigheid, onderbouwing (concreetheid), realiseerbaarheid en toegevoegde waarde. Maximaal te behalen punten voor deze wens: 20 punten.
--	--

Vormvereisten

Bij de beantwoording van deze Wens gelden de volgende vormvereisten:

- De beantwoording dient in een anoniem en neutraal format aangeleverd te worden (zonder direct herleidbare informatie als een logo, bedrijfsnaam, namen van werknemers, et cetera).
- De beantwoording dient zowel in MS Word als in PDF formaat te worden geüpload.
- De beantwoording dient maximaal 4 A4 (enkelzijdig, inclusief afbeeldingen, Arial 9,5, regelafstand enkel, marges 2,5) te bevatten. Na het maximale aantal pagina's wordt de informatie niet meer meegenomen in de beoordeling. Als er meer pagina's nodig zijn, dit graag aangeven in de Nota van Inlichtingen.

Beoordelingskader

Bij de beoordeling van de beschreven Wens wordt rekening gehouden met:

- Volledigheid: De beantwoording is volledig en laat geen aspecten van de Wens onbeantwoord.
- Concreetheid: De beantwoording is onderbouwd en berust op betrouwbare informatie. Wollig taalgebruik is vermeden en de beoordelaar hoeft geen moeite te doen het antwoord te doorgronden. Waar nodig is deze toetsbaar.
- Realistisch: De plannen en adviezen uit de beantwoording zijn haalbaar. Zowel technisch als in de tijd.
- Toegevoegde waarde: De beantwoording draagt daadwerkelijk bij aan het behalen van de geformuleerde doelen/ gewenste resultaten.

Voor de beoordeling maken de beoordelaars gebruik van onderstaand beoordelingsschema Tabel 1.

Daarbij geldt dat een beoordelaar alleen een hogere waardering kan geven wanneer volledig aan de criteria van de lagere waardering is voldaan.

Waardering	Score	Meerwaarde	Criteria
Onvoldoende	0%		De beantwoording is niet of nauwelijks aanwezig
Matig	20%		- De beantwoording is in enige mate aanwezig - De beantwoording is in enige mate concreet - De beantwoording is niet realistisch - De beantwoording is niet van toegevoegde waarde
Voldoende	55%		- De beantwoording is volledig - De beantwoording is concreet - De beantwoording is in enige mate realistisch - De beantwoording heeft enige mate van toegevoegde waarde
Goed	80%		- De beantwoording is volledig - De beantwoording is concreet - De beantwoording is realistisch - De beantwoording is van toegevoegde waarde
Uitstekend	100%		- De beantwoording is volledig - De beantwoording is concreet - De beantwoording is realistisch - De beantwoording heeft een grote mate van toegevoegde waarde en overtreft de geformuleerde doelen / gewenste resultaten

Tabel 1 - Beoordelingsschema Wens 1

Hoofdstuk 3. Integriteit

3.1 Business Etiquette

Opdrachtgever maakt graag gebruik van de kennis en innovatieve kracht uit de markt. Daarvoor werkt de Opdrachtgever samen met leveranciers. In deze samenwerking speelt u dus een essentiële rol. Opdrachtgever vindt onpartijdigheid en transparantie belangrijk. Daarom maken we afspraken hierover: onze Business Etiquette.

UE 13	Opdrachtnemer conformeert zich aan de Business Etiquette zoals opgenomen in Bijlage 4 van het Beschrijvend Document.
-------	--

Hoofdstuk 4. Financiële afspraken

4.1. Prijsmodel

GUE 2	Inschrijver vult de Prijzen voor de Diensten in in het Prijzenformulier, Bijlage VII.
GUE 3	Inschrijver zal de ingediende Prijzen in de gehanteerde formule niet frustreren, bijvoorbeeld door "met Prijzen te schuiven", zodanig dat voor het ene prijsonderdeel onrealistisch hoge Prijzen worden geboden en voor het andere prijsonderdeel onrealistisch lage Prijzen.
GUE 4	Inschrijver zal geen negatieve Prijzen of Prijzen van €0,- invullen in het Prijzenformulier, Bijlage VII. Inschrijver hanteert ingevulde Prijzen, die realistisch en marktconform zijn.
GUE 5	Alle met de Diensten gemoeide kosten zijn verwerkt in de Prijzen, tenzij anders vermeld.
GUE 6	Bedragen die niet in de Inschrijving genoemd worden en niet verdisconteerd zijn in de Prijzen, maar toch noodzakelijk blijken te zijn voor het goed uitvoeren van de Diensten, conform de in de Aanbestedingsstukken gestelde eisen en in de Inschrijving opgenomen beantwoording van de wensen, zijn voor rekening van de Opdrachtnemer.

4.2. Indexering Prijs

De door Inschrijver geoffreerde Prijzen: het uurtarief, zoals opgegeven in het spreadsheet Prijzenformulier, Bijlage VIII, mogen vanaf 2025 jaarlijks en steeds per 1 januari geïndexeerd worden op basis van de CBS tabel 'CAO-lonen, contractuele loonkosten en arbeidsduur, indexcijfers (2010 = 100)'; onderwerp: CAO- lonen incl. bijz. beloningen; SBI2008: M-N Zakelijke dienstverlening, conform de volgende webpagina:

<https://opendata.cbs.nl/statline/#/CBS/nl/dataset/82838NED/table?dl=9454A>

Prijsaanpassingen dienen uiterlijk voor 1 december van enig jaar aan de contractmanager ter goedkeuring te worden aangeboden, waarbij het op dat moment – door het CBS – meest recent beschikbare en gepresenteerde indexcijfer, Jaarmutatatie per kwartaal, gehanteerd wordt. Het percentage voor de tariefstijging wordt afgerond op één decimaal achter de komma. Inhaalslagen op niet doorgevoerde indexeringen worden niet geaccepteerd. Verder kan het resultaat van achtereenvolgens toegekende indexeringen nooit uitstijgen boven het verloop van de indexering sinds het begin van het contract.

Voorbeeld: als de overeenkomst op 1 juli geïndexeerd had mogen worden, was de prijsindexatie 5,1% geweest (jaarmutatatie DPI 2e kwartaal 2023, meest recent beschikbare indexcijfer).

GUE 7	De door de Opdrachtnemer geoffreerde Prijzen mogen jaarlijks per 1 januari geïndexeerd worden conform paragraaf 4.2 De eerste indexering vindt plaats niet eerder dan na 1 januari 2025.
-------	--

4.3. Elektronisch factureren (e-factureren)

Vanaf 1 januari 2017 stelt de Rijksoverheid elektronisch factureren (e-factureren) verplicht. E-factureren levert voordelen op voor alle factuurstromen tussen leveranciers en overheden. Een e-factuur is een gestructureerd digitaal bestand (geen pdf) waarbij de vereiste Gegevens altijd op een vaste plek met een specifieke codering in het bestand staan. Er zijn 4 mogelijkheden om een e-factuur aan de Rijksoverheid te versturen die nader staan omschreven in Bijlage 5 - Elektronisch bestellen & factureren.

Om elektronisch te kunnen factureren zijn ten minste de volgende gegevens nodig:

- naam en adres van de Opdrachtnemer
- het KvK-nummer van de Opdrachtnemer
- het BTW-nummer van de Opdrachtnemer
- het bankrekeningnummer (en indien van toepassing de BIC- en IBAN-code) van de Opdrachtnemer
- het Overheidsidentificatienummer (OIN) van de Rijksdienst waaraan de factuur wordt gestuurd. De lijst met OIN's wordt bijgehouden door Logius, zie www.logius.nl voor het actuele overzicht.
- het afleveradres (het adres waar de goederen of diensten zijn geleverd)
- het bestelnummer
- contactpersoon (de persoon die de bestelling heeft geplaatst)
- artikelcode (indien van toepassing)
- de omschrijving van de bestelde/geleverde goederen of diensten
- de bestelde/geleverde hoeveelheid
- de prijs per eenheid

UE 14	Opdrachtnemer verzendt toekomstige facturen elektronisch zodat deze, met inachtneming van de door de Aanbestedende dienst gegeven specificaties, elektronisch kunnen worden ontvangen en verwerkt.
UE 15	Opdrachtnemer zorgt na de gunning zo spoedig mogelijk voor de implementatie van 1 van de 4 beschreven mogelijkheden tot e-factureren conform de verplichtingen uit Bijlage 5 - Elektronisch bestellen & factureren en informeert de Aanbestedende dienst over de door u gekozen wijze van aansluiten.
UE 16	De Rijksoverheid berekent geen kosten aan Opdrachtnemers voor aansluiting op en communicatie met DigiPoort. Bij een directe aansluiting op de DigiPoort komen alle kosten vanaf het koppelvlak aan de zijde van de Opdrachtnemer voor rekening van de Opdrachtnemer. De kosten die de Opdrachtnemer daarvoor maakt, zijn voor eigen rekening.
GUE 8	Inschrijver accepteert een betalingstermijn van 30 Kalenderdagen na ontvangst van de factuur door de Aanbestedende dienst.

Hoofdstuk 5. Functionele eisen en wensen

5.1. Algemeen (voor alle Diensten)

5.1.1. Offerteprocedure

Wij hanteren een Offerteprocedure. Deze Offerteprocedure verloopt volgens onderstaande beschrijving:

Binnen Opdrachtgever kan een bepaalde behoefte ontstaan vanuit de ICT-organisatie. De signalering van de behoefte wordt de Klantvraag genoemd. De Klantvraag wordt vertaald naar een Offerteaanvraag. De contractmanager van de Opdrachtgever ontvangt een aanvraag van de interne klant voor het uitvoeren van Diensten door Opdrachtnemer. Dit resulteert in een Offerteaanvraag, die gericht is aan de Opdrachtnemer. De Opdrachtnemer, die volgens het verdeelsysteem (zie paragraaf 2.4.4 van het Beschrijvend Document) aan de beurt is, ontvangt de Offerteaanvraag.

In geval van spoed vraagt de Contractmanager van de Opdrachtgever telefonisch/per mail aan de Opdrachtnemer, die aan de beurt is volgens het verdeelsysteem, of hij de Diensten binnen de gestelde termijn kan vervullen. Is dit niet het geval? Dan wordt de volgende Opdrachtnemer benaderd, die aan de beurt is volgens het verdeelsysteem. Uit historie blijkt dat 5% van de Offerteprocedure van de Opdrachtgever spoed waren.

Opdrachtnemer maakt een concept offerte, heeft een intake met de Contactpersoon zoals genoemd in de Offerteaanvraag (hetzij telefonisch hetzij in een intakegesprek). Dit gesprek maakt het mogelijk om eventuele onduidelijkheden (o.a. inhoud, technische vragen, aantal dagen, beschikbaarheid systemen, etc.) weg te nemen en de details af te stemmen.

Opdrachtnemer maakt van het intakegesprek een verslag met daarin de afgesproken aspecten van de Opdracht.

Opdrachtnemer stuurt op basis van de intake en de Offerteaanvraag een Offerte binnen de genoemde termijn in de Offerteaanvraag.

De Offerte wordt na ontvangst beoordeeld. Indien de Offerte aansluit op de Offerteaanvraag en de prijs ten minste marktconform is, kan de Opdrachtgever besluiten de Opdracht te verstrekken.

Om zowel de kwaliteit als de prijs gedurende de contractperiode optimaal te stimuleren, heeft de Opdrachtgever binnen de Offerteprocedure de mogelijkheid om de Offerteaanvraag naar meerdere Opdrachtnemers te versturen. Dit zal steekproefsgewijs gebeuren. Bij deze Offerteaanvraag wordt de Opdrachtnemer niet op de hoogte gesteld van deze "mini-competitie". De ingediende Offerte met de laagste prijs krijgt de Opdracht verstrekt.

GUE 9	Inschrijver verklaart akkoord te gaan met de Offerteprocedure zoals beschreven in paragraaf 5.1.1.
-------	--

5.1.2. Sleutelfiguren van de Opdrachtnemer

Het personeel van de Opdrachtnemer dat belast is met de daadwerkelijke levering van de Diensten en waarvoor geldt dat zij over voldoende deskundigheid en ervaring beschikt om op een goede wijze invulling te geven aan de opdracht, worden gezien als Sleutelfiguren.

Het is te verwachten dat gedurende looptijd van de Overeenkomst en/of Nadere Overeenkomst er veelvuldig contact is tussen personeel van de Opdrachtnemer en Opdrachtgever. Om de samenwerking optimaal te stimuleren is het noodzakelijk dat er vanuit de Opdrachtnemer een beperkt vast aantal contactpersonen contacten heeft met de Opdrachtgever. Daarmee verwachten wij dat in de samenwerking efficiënter en effectiever gehandeld gaat worden.

GUE 10	Inschrijver verklaart akkoord te gaan bij uitvoering van de Overeenkomst aan bovenstaande paragraaf 5.1.2.
UE 17	Opdrachtnemer dient bij aanvang van de Overeenkomst de Sleutelfiguren op te geven inclusief vermelding van de specialismen per Sleutelfiguur en levert daartoe de CV's aan van de Sleutelfiguren. De CV's bevatten cumulatief minimaal hetgeen gesteld is in GUE 14 en GUE 15.
UE 18	Opdrachtnemer informeert Opdrachtgever tijdig bij voorgenomen vervanging van Sleutelfiguren.
UE 19	Opdrachtnemer is verplicht om bij vervanging en uitbreiding van Sleutelfiguren de competenties van de Sleutelfiguren op minimaal hetzelfde niveau te behouden. Opdrachtgever zal voorafgaand aan vervanging en uitbreiding een CV-toets uitvoeren alvorens akkoord te gaan met de vervanging/uitbreiding. Opdrachtnemer rapporteert periodiek aangaande de vervanging en uitbreiding.
UE 20	Sleutelfiguren van de Opdrachtnemer dienen bij iedere uit te voeren Opdracht in het bezit te zijn van een recente Verklaring Omtrent Gedrag (VOG) voor Natuurlijke Personen welke niet ouder is dan 12 maanden en waaruit blijkt er geen bezwaren zijn voor de uitvoering van de opdracht. Opdrachtnemer zal periodiek rapporteren aangaande de VOG.
UE 21	Sleutelfiguren van Opdrachtnemer dienen bij iedere uit te voeren Opdracht waarbij sprake is van Gegevens geclassificeerd als Staatsgeheim Confidentieel minimaal een Verklaring van Geen Bezwaar (VGB) niveau C (van de AIVD/MIVD) welke niet ouder is dan 12 maanden en waaruit blijkt er geen bezwaren zijn voor de uitvoering van de opdracht. Opdrachtnemer zal periodiek rapporteren aangaande de VGB.
W 2	Screening Hoe heeft Inschrijver de eis aangaande de minimale verklaring van geen bezwaar niveau C (van de AIVD/MIVD) in geval van Staatsgeheim Confidentiële Gegevens in zijn organisatie geborgd? Beoordeling vindt o.a. plaats op: - reeds aanwezige screening van personeel op dit vlak. - aantal Sleutelfiguren die deze verklaring van geen bezwaar niveau C reeds in bezit hebben. - proactieve houding om deze screening te verkrijgen. Maximaal te behalen punten voor deze wens: 90 punten.

5.1.3. Eisen en wensen uit te voeren Opdracht(en)

GUE 11	Inschrijver gaat akkoord dat de Diensten ook (deels) op locatie(s) (van de Opdrachtgever) plaatsvinden.
--------	---

GUE 12	Inschrijver garandeert strikte vertrouwelijkheid ten aanzien van de uit te voeren Opdracht(en) voor Opdrachtgever.
UE 22	Rapportage(s) worden elektronisch opgeleverd aan de Opdrachtgever en aan de Contractmanager van Opdrachtgever.
UE 23	De Opdrachtnemer levert altijd elektronisch de definitieve versie van een Onderzoeksrapport op aan de Opdrachtgever en het Security Operations Center.
W 3	Geef een beschrijving van de door u gebruikte allianties, samenwerkingsverbanden en overige connecties voor (meest recente) kwetsbaarheden in de IB-wereld. Beoordeling vindt o.a. plaats op inzicht in uw netwerk op het gebied van kwetsbaarheden, het door u aangegeven belang van deze allianties, samenwerkingsverbanden en overige connecties, wat is de toegevoegde waarde voor Opdrachtgever en de kwaliteit van de Diensten. Maximaal te behalen punten voor deze wens: 60 punten.
W 4	Geef een beschrijving van de door u gehanteerde testtooling. Gebruikt u alleen gangbare producten zoals Nessus en Burp suite of heeft u ook zelf tools ontwikkeld (zegt iets over uw ontwikkelings- of volwassenheidsniveau; bent u leidend of volgend). Beoordeling vindt o.a. plaats op aard van de tools, hoeveelheid tools, gebruik van de tools, recente versie van tools, participatie bij ontwikkeling tooling, wat is de toegevoegde waarde van de door u gebruikte tool(s) voor Opdrachtgever en de kwaliteit van de Diensten. Maximaal te behalen punten voor deze wens: 110 punten.
W 5	Geef een beschrijving van de door u gebruikte bronnen voor (meest recente) kwetsbaarheden. Wat is uw informatie-positie? hoe verzekert u zich van de meest recente kwetsbaarheden, hoe actueel en betrouwbaar is de beschikbare info over kwetsbaarheden en maak daarbij onderscheid tussen open bronnen en gesloten bronnen. Beoordeling vindt o.a. plaats op betrouwbaarheid van de bron en de snelheid waarbinnen de informatie beschikbaar is, wat is de toegevoegde waarde van de door u gebruikte bronnen voor Opdrachtgever en de kwaliteit van de Diensten. Maximaal te behalen punten voor deze wens: 110 punten.

5.1.4. Eisen en wensen ten aanzien van kennisdeling

GUE 13	Inschrijver dient bereid te zijn om gevonden bevindingen en verbetervoorstellen aan medewerkers van Opdrachtgever (bijvoorbeeld programmeurs of architecten) te presenteren. Het tarief dat Inschrijver daarvoor maximaal in rekening mag brengen is het door Inschrijver geoffreerde tarief voor het type Dienst waaruit de behoefte tot het presenteren van de bevindingen en verbetervoorstellen voortvloeit.
W 6	Geef een beschrijving van de wijze waarop u Opdrachtgever van kennis kunt voorzien zodat Opdrachtgever een robuuste en veilige ICT omgeving in stand kan houden.

	Beoordeling vindt o.a. plaats op basis van de mate waarin de kennisdeling op specifieke doelgroepen binnen Opdrachtgever is gericht, de vorm en de frequentie. Maximaal te behalen punten voor deze wens: 60 punten.
W 7	Geef een beschrijving van uw kennissysteem. Hoe houdt u de kennis van uw medewerkers op peil en hoe voorziet u in voortdurende bijscholing? Op welke wijze werd per medewerker geïnvesteerd aan kennis in de jaren 2020-2021-2022 (met bewijs)? Hoe wisselt men kennis uit, bijvoorbeeld 'capture the flag events'. Beoordeling vindt o.a. plaats op basis van de mate waarin uw kennissysteem is uitgewerkt op specifieke doelgroepen binnen uw organisatie, de vorm en de frequentie van kennisuitwisseling. Maximaal te behalen punten voor deze wens: 60 punten.

5.2. A&P testen

5.2.1. Sleutelfiguren

Het team van Sleutelfiguren van de Opdrachtnemer dienen minimaal te beschikken over de volgende competenties:

- Geschoold op HBO of universitair niveau,
- In het bezit zijn van drie certificaten gericht op het uitvoeren van A&P testen op Advanced niveau gelijkwaardig aan: OSCP, OSCE, GPEN, GXPEN.
- Minimaal kunnen voldoen aan level 2 Application Security Verification Standard 4.0 (owasp).
- Gecertificeerd zijn en werkervaring hebben op het (technisch-) domein waarop A&P testen wordt uitgevoerd zoals: Windows, AIX, Linux, Netwerken, Web hosting, databases, etc.
- Te beschikken over minimaal drie jaar relevante werkervaring in het zelfstandig uitvoeren van A&P testen en vijf jaar werkervaring in het (technisch-) domein waarop de A&P test wordt uitgevoerd zoals: Windows, AIX, Linux, Netwerken, Web hosting, databases, Java, .net;
- Beheersing van de Nederlandse en/of Engelse taal in woord en geschrift;
- Beschikken over communicatieve skills, om in een contact, bijvoorbeeld bij gesprekken met klant, eindgebruiker, of medewerkers van Opdrachtgever, een correcte houding aan te nemen en is in staat de juiste bewoordingen te kiezen;
- In staat om constructief met overige projectdeelnemers samen te werken om het vooraf bepaalde resultaat te realiseren;
- In staat om zijn beperkte beschikbaarheid zo doelmatig en efficiënt mogelijk in te zetten ten behoeve van de projectdoelstellingen.

GUE 14	Inschrijver gaat akkoord met de bovenstaande gevraagde competenties (paragraaf 5.2.1.) voor het team van Sleutelfiguren en zal enkel Sleutelfiguren inzetten die voldoen aan bovenstaande eisen (paragraaf 5.2.1.).
W 8	Beschikbaarheid testcapaciteit Welke garanties kan Inschrijver afgeven met betrekking tot de beschikbare testcapaciteit zonder dat een jaarplanning beschikbaar is wanneer, welke A&P testen plaats dienen te vinden? Beoordeling vindt o.a. plaats op: uw beschikbare testcapaciteit en uw garanties voor normale en spoedopdrachten. B.v. Op basis van een 'normale' opdracht voor een A&P test kan gegarandeerd binnen 14, 21 en 28 kalenderdagen met de daadwerkelijke test worden aangevangen na ontvangst van de opdracht daarvoor. B.v. Spoedopdracht kan binnen 7 kalenderdagen met de test worden aangevangen na ontvangst van de opdracht daarvoor. Maximaal te behalen punten voor deze wens: 90 punten.

GUE 15	Inschrijver gaat akkoord met de volgende annuleringsregeling: tot 5 werkdagen voor aanvang van de A&P test kan Opdrachtgever de opdracht kostenloos annuleren.
W 9	Annulering / verplaatsen test Op welke wijze denkt u mee in de situatie dat Opdrachtgever bij annulering/ verplaatsen van de opdracht binnen 5 werkdagen voor aanvang van de A&P test niet de volledige kosten in rekening gebracht wenst te krijgen? Beoordeling vindt o.a. plaats op: - herinzet van ingepland Personeel, denk aan inzet bij andere opdrachtgevers, inzet ten behoeve van opleiding van Opdrachtgever. - welke aantoonbaar te maken kosten krijgt Opdrachtgever maximaal in rekening gebracht voor Personeel dat niet heringezet kan worden. Maximaal te behalen punten voor deze wens: 50 punten.

5.2.2. Plan van Aanpak

Voorafgaand aan de A&P test verwacht de Opdrachtgever in de Offerte een Plan van Aanpak waarin de Opdrachtnemer aangeeft welke benodigdheden voor de test geregeld moeten worden, de gekozen aanpak, methodiek (scripts en tools), het intake-gesprek met de Opdrachtgever en baseline die wordt toegepast bij de uitvoering van de A&P test. Gebruikte scripts worden voorafgaand altijd door de Opdrachtgever op werking beoordeeld in de testomgeving van Opdrachtgever alvorens deze op zijn ontwikkel- en productiesystemen mogen worden gebruikt.

UE 24	Opdrachtnemer conformeert zich bij de uitvoering van de Overeenkomst aan bovenstaande (paragraaf 5.2.2.).
-------	---

5.2.3. Onderzoeksrapport

Kwetsbaarheden die zijn gevonden worden in de Rapportage als bevindingen gerapporteerd. Van bevindingen in de categorie hoog en midden worden niet alleen gerapporteerd welke kwetsbaarheden zijn vastgesteld, maar wordt tevens aangetoond dat de kwetsbaarheid daadwerkelijk uitgevoerd (geëxploiteerd) kan worden.

Tevens dienen minimaal de volgende zaken in de Rapportage opgenomen te worden:

- Management samenvatting met daarin tenminste opgenomen:
 - Beoordeling en standpunt van de Opdrachtnemer over de algehele veiligheid van de service zoals in de opdrachtoomschrijving en scope staan beschreven;
 - Onderscheid maken of bedreiging vanuit een intern dan wel extern perspectief een bedreiging vormt.
- Detailoverzicht van geconstateerde bevindingen met minimaal:
 - Bevinding, onderbouwing en mogelijke risico's;
 - Aanbeveling om de risico's te mitigeren.
 - Voor welke systemen/applicatie/op welke plekken binnen de applicatie, de bevinding van toepassing is.
 - Per bevinding een uniek volgnummer voor traceerbaarheid in het ticketing systeem;
 - Score opbouw volgens het Common Vulnerability Scoring System (CVSS) 3.0;
 - Beschrijving van de gebruikte methodiek en techniek om bevinding te reproduceren.
- De onderzoeker wordt gevraagd in de Rapportage antwoord te geven op de onderzoeksvragen die in de Offerteaanvraag staan beschreven;
- Beschrijving van de gekozen aanpak, methodiek en baseline die is toegepast bij de uitvoering van de A&P test.
- Om de volledigheid van het onderzoek aan te tonen, bevat de Rapportage een totaaloverzicht van alle getoetste kwetsbaarheden, ook als het getoetste aan de gestelde eisen voldoet.

6. Opgeleverde rapporten mogen zowel in de Nederlandse als in de Engelse taal worden opgesteld maar mogen geen documentbeveiliging bevatten zodat relevante teksten naar het ticketing systeem en memo's gekopieerd kunnen worden.

UE 25	Opdrachtnemer conformeert zich bij de uitvoering van de Overeenkomst aan bovenstaande (paragraaf 5.2.3.).
UE 26	Gerapporteerde bevindingen dienen voorzien te zijn van een onderbouwing en reproduceerbaar te zijn door Opdrachtgever. Eventuele keylogging, screenshots en networktraces dienen onderdeel te zijn van de onderbouwing. Indien voor het reproduceren van bevindingen speciale scripts of programmatuur noodzakelijk is dan dienen deze door Opdrachtnemer om niet ter beschikking te worden gesteld aan Opdrachtgever.

5.2.4. Evaluatie

Na afloop van een A&P test moet er ook een Evaluatie gedaan worden. Deze Evaluatie bestaat uit twee punten.

1. Na afloop van een A&P test worden de bevindingen altijd met de betrokkenen geëvalueerd voordat de Rapportage definitief wordt gemaakt. Indien nodig kan de Opdrachtgever de Opdrachtnemer uitnodigen om mondeling, indien niet anders overeengekomen, op locatie van Opdrachtgever, toelichting over het rapport te geven en richting te geven bij een gewenste oplossing.
2. Bij iedere bevinding in de categorie hoog en midden wordt aangetoond dat de kwetsbaarheid praktisch is te misbruiken door middel van een proof of concept (POC). Hierbij wordt onderscheid gemaakt vanuit een extern- én intern perspectief. Extern is een ongeautoriseerde derde, niet zijnde een medewerker van Opdrachtgever. Intern is medewerker van Opdrachtgever.

UE 27	Opdrachtnemer conformeert zich bij de uitvoering van de Overeenkomst aan bovenstaande (paragraaf 5.2.4.).
W 10	Geef een beschrijving inclusief voorbeelden van de deliverables op basis waarvan u zich conformeert aan de UE 24 tot en met UE27. Beoordeling vindt o.a. plaats op: - volledigheid van uw beschrijving - de mogelijkheid tot handmatig en geautomatiseerd rapporteren - de mate van aansluiting van de voorbeeldrapportage van een blackbox audit van een webbased programma aan de gestelde eisen - de mate van aansluiting voorbeeldrapportage van een crystalbox audit van een webbased programma aan de gestelde eisen - de mate van aansluiting van de voorbeeldrapportage van een code review aan de gestelde eisen - Max. 8 pagina's (A4) NB de kwaliteit van de overlegde deliverables wordt maatstaf voor de kwaliteit van de uitgevoerde opdrachten na gunning Maximaal te behalen punten voor deze wens: 200 punten.

5.3. IB kaders

UE 28	Opdrachtnemer heeft een inspanningsverplichting om Opdrachtgever proactief te informeren aangaande mogelijke bedreigingen en/of beveiligingsissues, met betrekking tot de Diensten inclusief eventuele risico's en de mogelijke oplossingen, of te nemen maatregelen met de eventueel daarmee gemoeide kosten.
-------	--

De Belastingdienst verwerkt fiscale en financiële Gegevens van particulieren en ondernemingen. De omgang met deze Gegevens vraagt van Opdrachtgever een werkwijze die de vertrouwelijkheid en integriteit van deze Gegevens waarborgt. De Baseline Informatiebeveiliging Overheid, bevat het normenkader voor informatiebeveiliging voor de overheid. Het Voorschrift informatiebeveiliging Rijksdienst – bijzondere informatie 2013 is van toepassing op de beveiliging van bijzondere informatie. Zie hiervoor Bijlage 7 & 8 (BIO en VIR-BI 2013) van het Beschrijvend Document.

Bij het betrekken van Diensten uit de markt zal een deel van de verantwoordelijkheden ingevuld worden door de Opdrachtnemer. Van de Opdrachtnemer wordt verwacht dat de aangeboden Diensten het beveiliging niveau, zoals beschreven in Bijlage 7 & 8 van het Beschrijvend Document – BIO en de VIR-BI 2013, niet aantast. De BIO sluit aan op de actuele, internationale standaard voor informatiebeveiliging (NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002).

UE 29	Inschrijver committeert zich aan de inhoud van Bijlage 7 & 8 van het Beschrijvend Document – BIO en VIR-BI 2013 en draagt er zorg voor dat tijdens de looptijd van de Overeenkomst de Diensten die worden aangeboden het basis beveiliging niveau, zoals beschreven in het BIO en de VIR-BI 2013, niet aantasten.
UE 30	(BIO 5.1.2, 15.1.2.6, 18.2.1.1) De Opdrachtgever heeft het recht om zelf (een deel van) de dienstverlening aan een Audit te onderwerpen. Basis van de Audit is deze Specificatie van de Opdracht.

5.3.1. Gegevens

Gegevens van de Opdrachtgever worden gescheiden Verwerkt van andere klanten van Opdrachtnemer: de Opdrachtgever heeft geen zicht in Gegevens van andere klanten, andere klanten hebben geen zicht in die van de Opdrachtgever.

Verwerken: een bewerking of een geheel van bewerkingen in het kader van de Opdracht met betrekking tot Gegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen.

Medewerkers van Opdrachtnemer hebben alleen toegang tot de Gegevens van de Opdrachtgever voor zover dat noodzakelijk is voor het uitvoeren van de Overeenkomst.

UE 31	Gegevens van de Opdrachtgever worden gescheiden opgeslagen van de gegevens van andere klanten. Toegang tot deze Gegevens is beperkt tot de Opdrachtgever en –voor zover noodzakelijk voor het uitvoeren van de Overeenkomst- Opdrachtnemer.
W 11	Geef aan in hoeverre Opdrachtnemer in staat is om Gegevens gescheiden van andere klanten van Opdrachtnemer te Verwerken. Als er meerdere mogelijkheden zijn, geef dan aan per alternatief wat de functionele verschillen zijn. De Opdrachtgever verwacht van het antwoord van de Opdrachtnemer dat: • De beantwoording volledig is conform de hierboven genoemde aspecten. • Het antwoord overtuigend, samenhangend en logisch is. <u>Beoordeling</u> De beoordeling vindt plaats op basis van de hierboven beschreven verwachting en de mate waarin uw antwoord daaraan voldoet. Maximaal te behalen punten voor deze wens: 50 punten.

Gegevens van en over de Opdrachtgever zijn vertrouwelijk en niet zonder expliciete toestemming van de Opdrachtgever te gebruiken voor eigen gebruik of te delen met Derde partijen. Gegevens worden door Opdrachtnemer alleen Verwerkt voor de doelen waarover afspraken gemaakt zijn.

UE 32	Opdrachtnemer zal geen Gegevens voor eigen doeleinden delen dan wel verwerken, behalve na expliciete toestemming van de Opdrachtgever. Opdrachtnemer openbaart welke Gegevens als strikt noodzakelijk worden beschouwd voor de uitvoering van de Overeenkomst.
--------------	--

Gegevens die te relateren zijn aan de Opdrachtgever of zijn medewerkers mogen zonder expliciete toestemming van de Opdrachtgever niet buiten de organisatie van Opdrachtnemer verwerkt worden. Dat geldt uiteraard ook voor Persoonsgegevens.

De Opdrachtgever maakt bij voorkeur gebruik van versleutelde Gegevens bij opslag (encryption-at-rest). Eén van de voordelen is dat als de Gegevens op ongecontroleerde wijze buiten zijn invloedssfeer terecht komen, Derden geen gebruik kunnen maken van deze Gegevens.

UE 33	Op Gegevens van de Opdrachtgever wordt encryption-at-rest toegepast.
--------------	--

W 12	Geef aan in hoeverre de Opdrachtnemer in staat is om Gegevens versleuteld op te slaan. In uw beschrijving dient u in ieder geval de volgende aspecten uit te werken: • Welke Gegevens versleuteld kunnen worden opgeslagen; • Wat de gevolgen van versleuteling zijn; • Op basis van welke encryptie-algoritmes Gegevens versleuteld worden; • Hoe de versleuteling ook in de toekomst aangesloten blijft bij marktconforme encryptie-algoritmes; De Opdrachtgever verwacht van het antwoord van de Opdrachtnemer dat: • De beantwoording volledig is conform de hierboven genoemde aspecten. • Het antwoord overtuigend, samenhangend en logisch is. Maximaal te behalen punten voor deze wens: 100 punten.
-------------	--

5.3.2. Personeel

Beschikbaarheid, integriteit en vertrouwelijkheid van Gegevens van de Opdrachtgever mogen op geen enkele manier gecompromitteerd raken. Van medewerkers van Opdrachtnemer met toegang tot Gegevens is de achtergrond gecontroleerd. Voor Nederlandse ingezetenen wordt gebruik gemaakt van de VOG. Voor niet-ingezetenen kan een gelijkwaardige verklaring worden overlegd. De Opdrachtgever oordeelt over de bruikbaarheid hiervan.

UE 34	(BIO 7.1.1.1) Opdrachtnemer heeft van alle medewerkers met toegang tot de Gegevens de achtergrond geverifieerd conform relevante wet- en regelgeving. Voor Nederlandse ingezetenen wordt gebruik gemaakt van de VOG. Voor niet-ingezetenen kan een gelijkwaardige verklaring worden overlegd.
--------------	---

5.3.3. Informatiesystemen

Beschikbaarheid, integriteit en vertrouwelijkheid van Gegevens van de Opdrachtgever mogen op geen enkele manier gecompromitteerd raken. De informatiesystemen waar Opdrachtnemer gebruik van maakt bij de uitvoering van de Diensten, zoals bijvoorbeeld het portal van waaruit de onderzoeksrapporten worden gedeeld met Opdrachtgever, zijn te dienaangaande voldoende beveiligd.

UE 35	• Opdrachtnemer zal informatie en/of data van Opdrachtgever op welk medium dan ook aan geen ander beschikbaar stellen of openbaar maken dan aan door Opdrachtgever aangewezen personen of organisaties; • Opdrachtnemer verbindt zich ten aanzien van de data van Opdrachtgever die onder hem berusten, waaronder ook begrepen transporten, het overeengekomen niveau van informatiebeveiliging in acht te nemen ter voorkoming van diefstal of onbevoegde wijziging en/of kennisneming daarvan; • Opdrachtnemer zal alle kennis omtrent toegangsregels en –codes welke in verband met de uitvoering van de opdracht worden gehanteerd, geheim houden en alle benodigde voorzieningen treffen teneinde te voorkomen dat deze kennis in handen van onbevoegden raakt; • Opdrachtnemer conformeert zich aan het huishoudelijk reglement kritische ruimtes (datacenters); • Opdrachtnemer zorgt ervoor dat haar Personeel en door haar ingeschakelde derden schriftelijk tot geheimhouding zijn verplicht; • Opdrachtnemer zegt toe dat indien geconstateerd wordt dan wel een vermoeden bestaat dat er sprake is van schending van vertrouwelijkheid, integriteit en beschikbaarheid, hiervan door Inschrijver onmiddellijk melding wordt gedaan bij Opdrachtgever en hierover tevens apart schriftelijk gerapporteerd zal worden aan Opdrachtgever; • Opdrachtgever is gerechtigd een kwaliteitstoetsing ten aanzien van de uitvoering van de opdracht door Inschrijver, op basis van de Overeenkomst, alsmede ten aanzien van vertrouwelijkheid, integriteit en beschikbaarheid van de door Opdrachtnemer ter beschikking gestelde Diensten, door een onafhankelijke deskundige te laten uitvoeren; • De Opdrachtnemer is bereid mee te werken aan een voorgenomen toetsing zoals hierboven beschreven. De Inschrijver is bereid door de deskundige aangegeven aanbevelingen ter verbeteringen, voor zover redelijkerwijze mogelijk, uit te voeren. Opdrachtnemer conformeert zich bij de uitvoering van de Overeenkomst aan bovenstaande.
-------	--

5.3.4. Veilige informatie-overdracht

UE 36	Opdrachtnemer stelt aan Opdrachtgever een medium (bij voorkeur een portal met MFA) beschikbaar waarop op een veilige manier documenten (zoals Plan van Aanpak en Rapportages) en gegevens uitgewisseld kunnen worden.
UE 37	Opdrachtnemer draagt er middels zijn e-mail systeem zorg voor dat alle e-mails tussen de Opdrachtgever en Opdrachtnemer standaard versleuteld worden uitgewisseld.

Hoofdstuk 6. Contractmanagement en Rapportage

6.1. Inleiding

De Opdrachtgever heeft contractmanagement ingericht inzake de beoogde Overeenkomst. Contractmanagement wordt omschreven als het op tactisch en operationeel niveau managen van alle contractueel vastgelegde verantwoordelijkheden, verplichtingen, procedures, afspraken, voorwaarden en tarieven rond een bepaalde overeenkomst plus het managen van alle onduidelijkheden.

De Opdrachtgever heeft haar ambitie op het gebied van contractmanagement vertaald in de navolgende activiteiten:

1. het sturen op de Resultaten van de Diensten door Opdrachtnemer middels het beoordelen van de kwaliteit van de Diensten volgens paragraaf 6.2, alsmede van de rapportages (zie paragraaf 6.2.2) en het evt. nemen van passende maatregelen daaromtrent
2. het proactief managen van alle afspraken, verplichtingen, voorwaarden, aannames, verwachtingen en doelstellingen met betrekking tot het contractueel bepaalde tussen Opdrachtgever en Opdrachtnemer;
3. het elimineren van gebreken, hiaten, onduidelijkheden en verschil van interpretatie in de onder 1 genoemde aspecten;
4. het volgens afspraak of op verzoek tijdig (laten) verschaffen van zo correct mogelijke informatie met betrekking tot status, voortgang, financiën, risico's, besluiten, acties en openstaande issues tussen Opdrachtnemer aan Opdrachtgever;
5. het organiseren, voeren en administreren van het noodzakelijke overleg tussen Opdrachtgever en Opdrachtnemer;
6. het managen van niet contractueel vastgelegde, maar voor partijen wel belangrijke aspecten of nevendoelestellingen.

Contractmanagement kan pas tot goede resultaten leiden als Partijen op een proactieve en transparante wijze invulling geven, respectievelijk bijdragen, aan deze activiteiten.

6.2. Beoordeling kwaliteit Diensten

Opdrachtgever verwacht van Opdrachtnemer dat de (Resultaten van de) uit te voeren Diensten van voldoende kwaliteit zijn. Om Opdrachtnemer te stimuleren een zo hoog mogelijke kwaliteit te leveren en een optimale samenwerking tot stand te laten komen zal de volgende beoordelingssystematiek worden gehanteerd.

6.2.1. A&P testen

Bij A&P testen kunnen de volgende aspecten worden onderscheiden:

- Offerteaanvraag
- concept offerte
- intake
- offerte met Plan van Aanpak
- inkoopopdracht
- planning en voorbereiding
- uitvoering
- rapportage
- evaluatie
- definitieve rapportage

Na de definitieve rapportage geven contractmanagers van zowel Opdrachtgever als Opdrachtnemer per aspect aan waar zij voor zichzelf en voor de ander verbeterpunten zien. Deze verbeterpunten worden via mail door de contractmanagers uitgewisseld. Afhankelijk van de ernst en urgentie van de bevindingen rondom deze verbeterpunten kunnen de contractmanagers van Partijen besluiten voor de bespreking ervan een separaat operationeel overleg te beleggen. Indien de verbeterpunten daar geen aanleiding voor geven worden de verbeterpunten in het eerstvolgende geplande operationeel overleg doorgesproken. Van de

verbeterpunten wordt bepaald hoe deze worden opgepakt, wie ze oppakt en wanneer deze tot de gewenste verbetering moeten leiden.

Opdrachtgever zal, indien de kwaliteit van de Diensten daartoe aanleiding geeft, aanpassingen doorvoeren in het verdeelsysteem genoemd in paragraaf 2.4.4 van het Beschrijvend Document.

6.2.2. Rapportage

Opdrachtnemer levert per kwartaal een Service Level Rapportage op aan de Contractmanager van de Opdrachtgever conform de in Bijlage A1 - Service Level Rapportage opgenomen aspecten.

UE 38	Opdrachtnemer conformeert zich bij de uitvoering van de Overeenkomst aan bovenstaande (paragraaf 6.2.2.).
-------	---

Hoofdstuk 7. Lijst van Bijlagen en Verklaringen

Bijlagen bij de Specificaties van de opdracht:

Bijlage	Inhoud
Bijlage A1	Service Level Rapportage