Marktraadpleging

Inzake de aanbesteding Resultaatverplichte ICT-opdrachten 2026 (RVICTO 26) op het gebied van Informatiebeveiliging ten behoeve van diverse Ministeries en hun onderdelen, alsmede enkele ZBO's.

Publicatiedatum	: 30 juni 2025
Status	: definitief 1v0
TenderNed-kenmerk	: TN 534872
IUC-registratienummer	: 202409001

Inhoudsopgave

Inhoudsopgave 2
1 Inleiding 3
1.1 Aanleiding marktraadpleging 3
1.2 Wie zijn wij? 3
1.3 Voor de aanbesteding voorgenomen scope van de opdracht 3
1.3.1 Penetratietesten 4
1.3.2 Red Teaming 4
1.3.3 SOC-diensten 4
1.3.4 Overige IB-diensten 5
1.4 Raamovereenkomsten en Nadere overeenkomsten 7
1.5 Aanbestedingsprocedure 8
1.6 Nationale veiligheid en ABRO 8
2 Procedure marktraadpleging 10
2.1 Algemeen 10
2.2 Communicatie en indienen antwoorden marktraadpleging 10
2.3 Planning 10
2.4 Vragen over de marktraadpleging 10
2.5 Aanvullende voorstellen 11
2.6 Resultaten van de marktraadpleging 11
2.7 Rechtsverhouding 11
3 Vragen marktraadpleging 12
3.1 Penetratietesten 13
3.2 Red Teaming 20
3.3 SOC-diensten 25
3.3.1 Monitoring & Detectie (M&D) 26
3.3.2 Kwetsbaarheden scanning & reporting (KS&R) 28
3.3.3 Aanpalende Diensten 30
3.3.4 Overig 30
3.4 Overige IB-diensten 37
3.4.1 Incident response 38
3.4.2 (Cyber) Threat Intelligence 41
3.4.3 (Social) Awareness 45
3.4.4 (Digitaal) Forensisch Onderzoek 47
3.4.5 IB-consultancy 48

1 Inleiding

1.1 Aanleiding marktraadpleging

De inkoopcategorie ICT-professionals Rijk, ondergebracht bij het Inkoop Uitvoering Centrum van het ministerie van Economische Zaken (IUC-EZ), heeft in 2021 na een marktraadpleging [TN324409] ten behoeve van de diverse ministeries raamovereenkomsten voor Resultaatverplichte ICT-opdrachten (RVICTO) aanbesteed [TN332318]. De hieruit voorgekomen raamovereenkomsten eindigen op 14 maart 2026 (Perceel 1 - Werkzaamheden aan maatwerkapplicaties) en op 14 juli 2026 (Perceel 2 - Informatiebeveiligingsdiensten).

Het IUC-EZ is momenteel de Europese aanbestedingen voor opvolging van deze raamovereenkomsten aan het voorbereiden en wil via deze marktraadpleging de kennis en ervaring van de markt betrekken in het inrichten en vormgeven van de

- verdeling in afzonderlijke onderwerpen/domeinen,
- opdrachtformulering, en
- aanbestedingsprocedure.

De doelgroep van de marktraadpleging is een ieder die meent een bijdrage te kunnen leveren aan deze marktraadpleging en in het bijzonder partijen die overwegen om in te schrijven op de voorgenomen aanbestedingen.

De uitkomsten van de marktraadpleging neemt het IUC-EZ mee in verdere voorbereiding van de aanbesteding.

1.2 Wie zijn wij?

Het IUC-EZ is de inkooporganisatie voor de ministeries van EZ, KGG en LVVN. Het is organisatorisch ondergebracht bij de Rijksdienst voor Ondernemend Nederland (RVO), een baten-/lastendienst onder het ministerie van Economische Zaken (EZ). Naast de reguliere inkopen voor de ministeries van EZ/KGG/LVVN begeleidt het IUC-EZ ook de Europese aanbestedingen voor de rijksbrede categorie ICT-Professionals Rijk. Deze categorie richt zich op aanbestedingen en raamovereenkomsten voor alle rijksonderdelen waarin de inzet van externe ICT/IV-professionals centraal staat. De daaruit voortvloeiende raamovereenkomsten worden door de categorie namens en in opdracht van de deelnemers gesloten.
De rijksonderdelen (de deelnemers) doen zelf hun nadere offeraanvragen en sluiten zelf de eventueel daaruit voortvloeiende Nadere Overeenkomsten voor concrete opdrachten c.q. diensten binnen deze raamovereenkomsten.

Deze marktraadpleging wordt door het IUC-EZ uitgevoerd ten behoeve van de categorie ICT-Professionals Rijk.

1.3 Voor de aanbesteding voorgenomen scope van de opdracht

RVICTO 26, als opvolger c.q. voortbouwend op de twee huidige raamovereenkomsten die in 2021 zijn aanbesteed onder TenderNed-nummer 332318, is verdeeld in meerdere onderdelen. De huidige raamovereenkomst (aangeduid als “Perceel 1”) voor maatwerkapplicaties omvat type opdrachten volgens alle profielen van het KwIV, met uitzondering van regel 4.1 Informatiebeveiliging. In RVICTO 26 is dit een separate aanbesteding met een in

beginsel ongewijzigde scope. Dit onderdeel wordt niet meegenomen in deze marktraadpleging.

De andere huidige raamovereenkomst (aangeduid als "Perceel 2") betreft enkel type opdrachten volgens de KwIV-profielen onder 4.1 Informatiebeveiliging. In RVICTO 26 is een onderverdeling gemaakt in verschillende typen IB-dienstverlening:

- Penetratietesten
- Red Teaming
- SOC-diensten
- Overige IB-diensten (Incident response, threat intelligence, Forensisch onderzoek, Awareness, IB-consultancy)

Het idee is om voor deze typen IB-dienstverlening aparte raamovereenkomsten te sluiten. De vragen in deze marktraadpleging zien op deze IB-dienstverlening.

1.3.1 Penetratietesten

Handmatige controle waarbij men zo diep mogelijk wil binnendringen in een digitaal systeem om zwakke plekken te vinden en de gevolgen hiervan te kennen. Men gebruikt de zwakke plekken om nog wat dieper in het systeem te komen. Doel van de test is niet om zoveel mogelijk zwakke plekken te vinden, maar om te onderzoeken of een systeem zwakke plekken kent. Het zoeken naar zoveel mogelijk zwakke plekken gebeurt wel bij een vulnerability scan.

1.3.2 Red Teaming

Een red teamingtest is een geavanceerde securitytest waarbij een cyberaanval op 1 of meerdere kritieke functies van een organisatie wordt uitgevoerd. Dit gebeurt op basis van reële dreigingen. Het doel van een red teamingtest is om de beveiligingsmaatregelen van een organisatie (of keten van organisaties) te testen en de organisatie hiervan te laten leren. Op basis van de bevindingen uit een red teamingtest kun je verbeterplannen opstellen om de digitale weerbaarheid van de organisatie te verbeteren. De Rijksoverheid organiseert Red Teaming via TIBER en ART. TIBER staat voor Threat Intell Based Ethical Redteaming. Binnen TIBER testen instellingen hoe weerbaar ze zijn tegen geavanceerde cyberaanvallen. Dit gebeurt met testaanvallen, die zijn gebaseerd op realistische dreiging. ART staat voor Advanced Red Teaming. Het verschil met een TIBER is dat binnen ART meer keuzeopties zijn voor de inrichting van de test door de modulaire opbouw.

1.3.3 SOC-diensten

In deze markconsultatie bedoelen we met SOC-diensten de volgende twee type dienstverlening:

a) Monitoring & Detectie:
   Het monitoren van ICT-systemen en detecteren van ongebruikelijke of ongewenste activiteiten en deze aan de IT-organisatie melden opdat daarop passende actie kan worden genomen. Ook afnemen, implementeren en gebruiken van operationele Cyber Threat Intelligence informatie, de zogenaamde CTI-feeds, zijn onderdeel van Monitoring & Detectie.

b) Kwetsbaarheden Scanning & Reporting
   Het in kaart brengen van ICT-assets en kwetsbaarheden, het evalueren van bevindingen, hierover rapporteren inclusief het verstrekken van duiding en handelingsperspectief, het adviseren van de organisatie met het verhelpen

van bevindingen en het bewaken en rapporteren over de opvolging om kwetsbaarheden weg te nemen.

Incident Response als omschreven in 1.3.4. wordt in deze marktraadpleging niet tot SOC-diensten gerekend. Er wordt onderkend dat deze dienstverlening samen kan hangen met de SOC-diensten. Vanuit oogpunt van rolscheiding en marktdifferentiatie verdient het echter de voorkeur dit in een ander RVICTO-deel onder te brengen, te weten "Overige IB-diensten".

1.3.4 Overige IB-diensten

Dit deel is een verzameling losse Informatiebeveiligingsdiensten. Voor iedere dienst moet nog worden bepaald op welke wijze deze het beste kan worden gecontracteerd en onder welke contractvorm.

1.3.4-a. Incident response - Het reageren op een cyberincident. Het is een (gestructureerde) aanpak op alle niveaus: operationeel, tactisch en strategisch. Ook preparatie wordt tot incident response gerekend. Preparatie omvat het voorbereiden van een organisatie om adequaat op incidenten te reageren. Denk bijvoorbeeld aan het opstellen van responseplannen en het oefenen op cyberincidenten.

1.3.4-b. Threat Intelligence (dreigingsinformatie) - Inlichtingen en analyses over dreigingen. Het is een discipline onder cybersecurity, die zich richt op de gestructureerde verzameling, analyse en verspreiding van gegevens over potentiële of bestaande cyberdreigingen. Het afnemen, implementeren en gebruiken van dreigingsinformatie kan in de vorm van de zogenaamde CTI-feeds zoals het NCSC deze beschikbaar stelt ten behoeve van monitoring en detectie als onderdeel van SOC-diensten, als ook dreigingsscenario's voor Red teaming, als ook generieke dreigingsbeelden en TI-onderzoek.

Tevens valt onder deze dienstverlening additionele en verrijkte operationele dreigingsinformatie, evenals strategische- en tactische dreigingsanalyses.

1.3.4-c. Awareness – bewust maken, trainen en/of opleiden van eindgebruikers van cyberveiligheid en hoe men daaraan kan bijdragen.

1.3.4-d Forensisch Onderzoek – verzamelen en analyseren van bewijsmateriaal en proberen zo vragen te beantwoorden over een aanval.

1.3.4-e IB-consultancy – Diverse adviesopdrachten op het gebied van Informatiebeveiliging.

<u>Buiten scope</u>

De volgende onderwerpen vallen buiten de scope van de te sluiten Raamovereenkomsten:

- Opdrachten met inspanningsverplichting c.q. inhuur van personen (tenzij het een ondergeschikt, bijkomend c.q. accessoir deel is bij een Nadere overeenkomst uit hoofde van de onderhavige aan te besteden Raamovereenkomst);

- Opdrachten waarvoor de Deelnemers andere (raam)overeenkomsten hebben, ook in het geval van een vernieuwing, namelijk:
  - Datacenter hardwarecomponenten, daaraan gerelateerde software en geïntegreerde oplossingen. Raakvlak met deze raamovereenkomsten bestaat bij diensten op het gebied van beheer, onderhoud en veiligheid;
  - ERP-oplossingen en ERP-dienstverlening (zoals uitbesteding van systeemintegratie en managed services). Deze vallen onder een andere aanbesteding.
  - Standaardprogrammatuur, de implementatie van deze software bij de Deelnemer(s), alsmede het bij de aanschaf gecontracteerde beheer en onderhoud van deze software (gericht op de kwaliteit van het systeem). Raakvlakken met deze raamovereenkomsten bestaan op de gebieden implementatie-, beheer- en onderhoudsactiviteiten die het gevolg zijn van een toenemende complexiteit, zoals het toevoegen van functionaliteiten, het verzorgen van systeemintegratie, het specifiek configureren van de software en/of het oplossen van problemen die niet ondervangen worden door de standaardvoorziening. Op deze gebieden is opdrachtverlening binnen de scope van de onderhavige raamovereenkomsten mogelijk indien en voor zover Deelnemer daarin niet voorzien wordt door de contracten op het gebied van Standaardprogrammatuur;
  - Hardware voor de vaste werkplek, mobiele werkplek, telefonie/spraak, alsmede hierbij behorende software en telefoniediensten. Raakvlakken met deze raamovereenkomsten bestaan op diensten gerelateerd aan implementatie, configuratie, beheer en onderhoud;
  - Connectiviteitsdiensten, waaronder het leveren van (vaste en mobiele) dataverbindingen, cloudconnectiviteit, aanvullende adviesdiensten en het leveren van diensten en voorzieningen om DDoS aanvallen te detecteren en te mitigeren;
  - IT-research dienstverlening, in het bijzonder de levering van standaard, reeds opgestelde ICT/IV-onderzoeksrapporten, -adviesrapporten en –onderzoeksinformatie, die (al dan niet tegen vergoeding) beschikbaar/toegankelijk is voor een breed publiek, alsmede direct hieraan gerelateerde (advies)dienstverlening gericht op kennisdeling over en juiste interpretatie en toepassing van deze (onderzoeks-)informatie;
  - Strategisch resultaatverplichte ICT-(maatwerk)adviezen. Hieronder vallen bijvoorbeeld strategische adviezen met betrekking tot ICT-vraagstukken over de strategie, besturing, beleid, mens en organisatie, verandermanagement als gevolg van veranderde omstandigheden (op resultaatverplichte basis),
  - Het uitbesteden van juridische, financiële of auditdiensten, waarbij het zwaartepunt van de benodigde kennis, ervaring en vaardigheden en werkzaamheden ligt op deze vakgebieden en niet op ICT/IV-vakgebieden zoals omschreven in het Kwaliteitsraamwerk IV;
  - Interimmanagement, waarvoor geldt dat het zwaartepunt van de taken niet binnen het ICT-werkveld ligt;
  - Inkoop- en contractmanagement, tenzij het zwaartepunt ligt bij het management van ICT-contracten;
  - Campagnes, mediadiensten, communicatieonderzoek, webonderzoek, webanalyse, webredactie, beelddiensten, arbeidsmarktcommunicatie en online-diensten die tegemoet komen aan een generieke communicatiebehoefte van het Rijk;

- ICT-/IV-gerichte trainingen, waarbij de dienstverlening kan bestaan uit zowel open aanbod trainingen, incompany trainingen als doorontwikkeling van incompany trainingen, mits deze trainingen geen volledig maatwerk betreffen (vanaf 'scratch' ontwikkelen). Het leeraanbod kan geleverd worden in diverse werk- en leervormen (klassikaal, online, e-learning, videolearning, microlearning, virtual en augmented reality, serious gaming, web-podcast etc.). O.a. trainingen op het vlak van informatiebeveiliging, cybersecurity en privacy, digitaal forensisch opsporen en cybercrime, architectuur, methodes en technieken voor systeem- en applicatieontwikkeling, ontwikkeltalen en -frameworks, data-analyse en vendorspecifieke trainingen (IBM, Red Hat, Microsoft) vallen hier onder;
- Onderwijskundige diensten, didactische trainingsdiensten en diensten voor het technisch ontwerpen, bouwen, opleveren en optimaliseren van maatwerk digitale leeractiviteiten (zoals e-learnings);
- Raamovereenkomsten voor de uitbesteding van resultaatverplichte ICT-/ IV-opdrachten;
- Raamovereenkomsten op dit gebied waaraan een Deelnemer zich zelfstandig reeds heeft verbonden.

<u>Bijlagen</u>
Dit marktconsultatiedocument heeft vier (4) concept-Programma's van Eisen als bijlage. Ook deze staan open voor uw feedback

1. **PvE Generieke eisen** – dit betreffen algemene eisen die voor alle RVICTO-aanbestedingen. Ze zijn bijgevoegd, opdat u een volledig beeld kunt hebben van de afspraken-set en u bij het lezen niet onnodig algemene afspraken in de specifiek PvE's mist.
2. **PvE Pentesten**
3. **PvE Red Teaming**
4. **PvE SOC-diensten**

1.4 Raamovereenkomsten en Nadere overeenkomsten

Tenzij bijzonderheden zich gaan voordoen, is het algemene voornemen het sluiten van raamovereenkomsten (ROK) voor de duur van 2 jaar + 2x1 jaar verlenging (totale duur maximaal 4 jaar).

De duur van Nadere overeenkomsten (NOK) wisselt sterk per onderwerp en dienst. Daar waar het afgeronde projecten betreft is de duurbepaling zoals die is afgesproken. Pentesten zullen in weken uit te drukken zijn, ART/TIBER Red Teaming testen in gemiddeld 6 tot 9 maanden (inclusief het inkoopproces). Voor dit type nadere overeenkomsten is het niet aan de ROK om deze vooraf te fixeren of te bepalen.

De duur van een NOK voor duurprestaties staat in beginsel open en zal per geval naar de eisen van proportionaliteit worden bepaald. Ook kunnen onder diensten verschillen zijn in het terugverdienen van transactiekosten en transitiekosten (in & exit) per dienst. Een NOK op basis van de beoogde ROK heeft altijd een beperkte duur c.q. een concrete begin- en einddatum (dus nooit: onbepaalde tijd) inclusief verlengingen. Vooraf wordt niet bepaald hoe ver de uiteindelijke einddatum

maximaal van de startdatum mag liggen. Wat in het kader van proportionaliteit een passende duur van een NOK is, is aan de omstandigheden waarin een betreffende organisatie zich bevindt en hoe deze omstandigheden de motivatie voor de passende duur kunnen dragen.

Zo speelt bij SOC-diensten onder meer, dat het (voorbereiden en) inrichten van SOC-diensten aan de kant van Deelnemer veel tijd kan kosten, wat snel veel waardevolle contracttijd 'snoept'. Daarbij is vooralsnog het uitgangspunt dat de inrichting/afname van de SOC-diensten voor veel van onderhavige Deelnemers een 1e stap hierin is en na implementatie partijen moeten kalibreren en een contractperiode zoeken met voldoende tijd om in rust en rendement groei van de SOC te kunnen realiseren. In de praktijk zien we looptijden van relevante SOC-contracten (NOK) van 4, 6 en 8 jaar.

Dienstverlening zelf wordt gecontracteerd aan de hand van een NOK. Een NOK kan gedurende de looptijd van de ROK worden uitgevraagd en afgesloten. Een NOK mag langer duren dan de ROK, dus die zijn in duur niet door de looptijd van de ROK beperkt.

Onderstaand worden bij de onderwerpen ramingen gegeven van het totale opdrachtvolume over vier jaar.

- De ramingen van aantallen en euro's zijn in dit stadium indicatief en sterk afgerond.
- Ze vertegenwoordigen niet het opdrachtvolume voor later in aanbestedingen. Ze worden enkel gegeven om een orde van grootte te duiden, ook al zijn ze herleid op basis van huidige verwachtingen.
- Als zowel aantallen als omvang in euro zijn genoemd, dan zij expliciet vermeldt dat getallen voortkomen uit een inventarisatie onder de verschillende deelnemers en het één niet in een rekenkundige verhouding is uitgedrukt in het ander.
- Ramingen zijn opgegeven onder voorbehoud van onzekerheden die men niet concreet kan voorspellen. Dit omvat elementen als de veranderingen als gevolg van keuzes in het kader van arbeidsrelaties, als ook de huidige geopolitieke dynamiek.

1.5 Aanbestedingsprocedure

Tenzij er reden is om anders te kiezen, zal de Openbare Procedure worden gevolgd. Per type IB-dienstverlening wordt dit nader afgewogen. De resultaten van de marktraadpleging worden in die afwegingen meegenomen.

1.6 Nationale veiligheid en ABRO

Het is met enige zekerheid te stellen dat in de beoogde raamovereenkomsten opdrachten zullen worden gegeven die de te beschermen belangen raken of de nationale veiligheid. Deelnemers zijn verantwoordelijk voor het beoordelen of bij een nadere opdracht mogelijk sprake is van een nationaal veiligheidsbelang. Veiligheidsmaatregelen kunnen zich doen gelden in het inkoopproces, als ook in de

uitvoering. Dit kan de aanbestedingsstrategie voor de Europese Aanbestedingen voor raamovereenkomsten raken, als ook concrete (nadere) opdrachten. Dit brengt een voorbehoud op de mogelijke indrukken en verwachtingen die met dit document gewekt kunnen worden

Zijn er ter zake risico's, dan beoordeelt de betreffende deelnemer met betrekking tot het inkoopproces ook welke wet van toepassing is (Aanbestedingswet 2012 of de Aanbestedingswet op Defensie- en Veiligheidsgebied). Hierbij kan gedacht worden aan gevallen waarin gevoelige informatie in het inkoopproces wordt/moet worden gedeeld, dan wel de identiteit van (een) partij(en) anderszins geheim of vertrouwelijk moet blijven. Het kan ook voorkomen dat een opdracht binnen de scope van een ROK om veiligheidsredenen toch buiten die raamovereenkomst wordt/moet worden uitgezet. Veiligheidsmaatregelen in het inkoopproces moeten gescheiden worden beschouwd van de bepaling of een contractpartij veilig is voor de uitvoering van een opdracht.

In het regeerprogramma van 2024 staat vermeld dat vanaf het tweede kwartaal van 2025 via ABRO (Algemene Beveiligingseisen voor Rijksoverheidsopdrachten) aanvullende beveiligingseisen binnen de Rijksoverheid en politie zullen worden ingevoerd. De vaststelling en het begin van invoering is momenteel beoogd in de 2e helft van 2025. Ongeacht wanneer het daadwerkelijk zal komen, is het vrijwel zeker dat het er aan gaat komen. De ABRO 2025 bouwt voort op de 'Algemene Beveiligingseisen voor Defensieopdrachten 2019' (ABDO) van het ministerie van Defensie, die opgaat in de ABRO. De verwachting is dat de ABRO op de raamovereenkomst voor SOC-diensten in generieke zin van toepassing gaat zijn, maar per opdracht moet wel/geen toepassing van (delen van) de ABRO worden vastgesteld. De raamovereenkomst of opdrachten die hieruit voortkomen raken soms de nationale veiligheid. Opdrachtnemers kunnen of zullen soms in aanraking komen met 'te beschermen belangen' (TBB's) van rijksdiensten. Het waarborgen van een adequaat beveiligingsniveau bij het zakendoen met deze opdrachtnemers is dan essentieel. De ABRO moet hierin voorzien.

De ABRO 2025 wordt tranchegewijs ingevoerd. Medio 4e kwartaal van 2025 starten de eerste ministeries en de politie met de implementatie, die tot medio 2027 loopt. De meeste Deelnemers krijgen dan ook geleidelijk met de ABRO 2025 te maken..

Voor elke opdracht die de nationale veiligheid kan raken, beoordeelt de Deelnemer of ABRO 2025 van toepassing is. Vervolgens wordt een potentiële opdrachtnemer gescreend op de aspecten Bestuur en Organisatie, Personeel, Fysiek, Cyber en Cloud. Deze screening richt zich specifiek op individuele bedrijven en hun medewerkers en vormt een belangrijke schakel in de beveiligingsketen. Met de ABRO 2025 worden specifieke beveiligingsmaatregelen geëist van een geselecteerde opdrachtnemer. Bij inzet op een opdracht die de nationale veiligheid raakt, moet een opdrachtnemer een ABRO-autorisatie hebben. Opdrachtnemer zal dan door het Nationaal Bureau Industrieveiligheid (NBIV) onderzocht worden op de onderwerpen: Bestuur en Organisatie en (voor zover relevant) Personeel, Fysieke beveiliging, Cyber, Cloud. Voor opdrachten die naar het oordeel van de Deelnemer niet de nationale veiligheid raken, is geen ABRO-autorisatie nodig. De raamovereenkomst moet ruimte geven voor beide soorten opdrachten.

2 Procedure marktraadpleging

2.1 Algemeen

U wordt uitgenodigd de in dit document gevraagde informatie zo volledig mogelijk aan te leveren. Deze marktraadpleging maakt uitdrukkelijk geen deel uit van een aanbestedingsprocedure.

2.2 Communicatie en indienen antwoorden marktraadpleging

Procedure

We verzoeken u vriendelijk alle communicatie met betrekking tot deze procedure te laten verlopen via categorie.ictprofs.ea@rvo.nl t.a.v. R. Jagt met in het begin van de onderwerpregel in ieder geval vermelding van "**R26-MC**".

Reactie

Het verzoek is uw reactie in de vorm van gerichte schriftelijke antwoorden op de in deze marktraadpleging gestelde vragen. Daarbij ook het verzoek om de nummering van de vragen onveranderd te hanteren in uw beantwoording.

Er is geen maximum aantal pagina's. Toch vragen we om zoveel als mogelijk 'to the point' te blijven en moet een bijdrage in de vorm van gemiddeld 1/2 A4 toereikend kunnen zijn voor de beantwoording van 1 vraag. Daarbij: hoe gerichter het antwoord, hoe beter uw boodschap overkomt.

Uw reactie ontvangen we graag via de berichtenmodule van dit TenderNed dossier retour.

2.3 Planning

Met betrekking tot deze marktraadpleging geldt het navolgende tijdschema:

30 juni 2025	Publicatie/verzending marktraadpleging
25 augustus 14:00 uur	Uiterste datum voor het indienen van antwoorden door marktpartijen

Wij zullen u bij wijzigingen van de termijnen informeren.

Na de marktraadpleging bespreken we de resultaten daarvan in de projectorganisatie van de voorgenomen aanbesteding(en). Hierin wordt bepaald in hoeverre de uitkomsten van de marktraadpleging worden verwerkt in de aanbesteding(en). Beoogd is de aanbesteding(en) in Q3/4 2025 te starten.

2.4 Vragen over de marktraadpleging

Er is een mogelijkheid tot het stellen van vragen over deze marktraadpleging en dit document. Hiervoor heeft u tot en met 10 juli 2025 te tijd. Na deze datum ontvangen wij geen vragen meer en werken dan aan de antwoorden van de tijdig gestelde vragen en streven ernaar deze 17 juli te publiceren.

10 juli 2025 14:00	Afloop van de termijn om vragen over de marktraadpleging te stellen.
17 juli 2025	Publicatie van de antwoorden op de ontvangen vragen.

Urgente vragen of opmerkingen kunt u altijd doorgeven aan de contactpersoon zoals vermeld in paragraaf 2.2. Deze bepaalt de urgentie en of/welke vragen of opmerkingen beantwoord. Deze vragen/opmerkingen en de bijbehorende antwoorden, zullen in voorkomend geval geanonimiseerd via TenderNed worden gedeeld.

2.5 Aanvullende voorstellen

Heeft u, naast de door ons gestelde vragen en uw reactie daarop, uit eigener beweging nog andere nuttige opmerkingen of voorstellen, dan ziet we die graag tegemoet. Hiervoor is per onderwerp ruimte aan het einde van iedere set vragen.

2.6 Resultaten van de marktraadpleging

Een beknopt, geanonimiseerd verslag van de marktraadpleging wordt gedeeld met de respondenten en wordt te zijner tijd als zelfstandig document als bijlage opgenomen bij de voor deze raamovereenkomst te starten aanbestedingsprocedure.

Het is de bedoeling dat wij de informatie die verzameld is naar aanleiding van deze marktraadpleging kunnen gebruiken bij het opstellen van een opdracht. U moet er dan ook rekening mee te houden dat informatie die u in het kader van deze marktraadpleging verstrekt geacht wordt openbaar (al dan niet in geanonimiseerde vorm) te zijn.

Wij willen de door u verstrekte informatie zo veel als mogelijk zonder voorbehouden kunnen gebruiken. Om deze reden kunnen we uw eventuele algemene claims/voorbehouden over het gebruik van informatie of vertrouwelijkheid niet honoreren. Mocht een deel van uw reactie vertrouwelijke informatie bevatten, dan is het dringende verzoek dat deel eenduidig te merken/markeren of zodanig af te bakenen, dat het zonder interpretatie helder is welke informatie onder die betreffende vertrouwelijkheid valt en welke informatie niet. Alleen dan kunnen we de vertrouwelijke behandeling daarvan toezeggen. Door het deelnemen aan deze marktraadpleging stemt u hiermee in.

Bij een aanbesteding zal geen onderscheid bestaan tussen partijen die wel of niet hebben deelgenomen aan deze marktraadpleging.

Voor deelname aan de marktraadpleging worden geen kosten vergoed.

2.7 Rechtsverhouding

De marktraadpleging is voor alle partijen (de organisatie en de geïnteresseerden) vrijblijvend en houdt op geen enkele wijze een verplichting in om met deelnemers in een bepaalde rechtsverhouding te treden. Er kunnen geen rechten worden ontleend aan deelname aan de marktraadpleging of tijdens de marktraadpleging verstrekte informatie.

3 Vragen marktraadpleging

U wordt uitgenodigd onderstaande gegevens voor uw organisatie in te vullen en de algemene en de onderwerp-specifieke vragen.

Als u een suggestie voor aanpassing heeft, help ons die goed te begrijpen door helder te duiden waarom u die suggestie doet en wat het oplevert.

Naam organisatie:	
Naam contactpersoon en functie:	
Tel. Nummer contactpersoon:	
E-mail contactpersoon:	

In 1.3 is de indeling van IB-onderwerpen gegeven waarvoor per onderwerp een overeenkomst beoogd is. Aanleiding is dat de type IB-diensten zeer verschillend van elkaar kunnen zijn, andere waarborgen en afspraken vergen en zelfs andere markten aanspreken.

Vooralsnog wordt gericht op het sluiten van raamovereenkomsten. Per onderwerp is de afweging hoeveel partijen tot een raamovereenkomst toe te laten om voldoende concurrentie en kwaliteit voor de opdrachtgever te waarborgen en tevens tegemoet komt aan de belangen van de opdrachtnemers.

Er kan/zal overlap zijn qua dienstverlening of in te zetten kennis. De indeling beoogt een aanbesteding voor partijen die specifiek op een onderwerp kunnen excelleren. Daarmee is ook beoogd de drempel voor inschrijven op een onderwerp te verlagen.

A1	Wat vindt u van de voorgenomen verdeling in onderwerpen en de daarin omschreven scope?
Antwoord	
A2	Ontbreken er naar uw beeld nog diensten in de genoemde onderwerpen? Zo ja, welke?
Antwoord	
A3	Wat is naar uw mening een gebalanceerd aantal partijen bij een raamovereenkomst voor een onderwerp en hoe komt dat aantal tegemoet aan de gezochte waarden voor opdrachtgever en de te bieden waarden door de opdrachtnemer? *Zekerheidshalve: er wordt uiteraard niet gevraagd om een antwoord voor onderwerpen die niet van uw gading zijn. Ook: als bij een onderwerp deze vraag ook specifiek wordt gesteld, kunt u uw reactie daar geven en hier weglaten.*
Antwoord	

A4	In de raamovereenkomsten zullen diverse deelnemers afnemen. Hoe is het risico te mitigeren dat de vraag voor u te groot wordt om te kunnen leveren? Waar moeten wij rekening mee houden? Welke voorwaarden zijn voor onze deelnemers relevant? *Zekerheidshalve: er wordt uiteraard niet gevraagd om een antwoord voor onderwerpen die niet van uw gading zijn.*
Antwoord	
A5	Bent u geïnteresseerd om in te schrijven op een of meer onderwerpen van de voorgenomen aanbesteding? Zo ja, welke onderwerpen?
Antwoord	
A6	In hoeverre ziet u het effect van de ontwikkeling in de EU rond digitale autonomie/soevereiniteit in de komende tijd op uw producten en dienstverlening in relatie tot de onderhavig voorgenomen aanbestedingen?
Antwoord	
A7	Bij deelnemers is Nederlands, zowel schriftelijk als mondeling, de voertaal. In hoeverre verwacht u dat het eisen van de Nederlandse taal als voertaal een beperking is voor de gevraagde dienstverlening en mogelijk marktpartijen weerhoudt om in te schrijven?
Antwoord	

3.1 Penetratietesten

Raming jaar 1 t/m 4
€10.000.000 - €50.000.000
800 – 2.500 pentesten

Het vooralsnog grote verschil heeft te maken met een 1 grote deelnemer en het aantal variabelen van de afname, zowel in aantal, als in de diversiteit in omvang van de pentesten zelf.

Scope
Een penetratietest (pentest) is een geautoriseerd, gecontroleerd en doelgericht informatiebeveiligingsonderzoek waarbij ethische hackers – met expliciete toestemming van de systeemeigenaar of opdrachtgever – realistische aanvallen uitvoeren op IT-systemen, netwerken, applicaties of andere digitale componenten. Hierbij maken zij gebruik van dezelfde tools, technieken en methoden als kwaadwillende aanvallers, om kwetsbaarheden op te sporen en – waar mogelijk – te misbruiken. Pentests zijn erop gericht om de effectiviteit van bestaande beveiligingsmaatregelen te beoordelen, de digitale weerbaarheid tegen echte dreigingen te testen en verbeterpunten aan te dragen. Vaak wordt daarbij gezocht naar combinaties van kwetsbaarheden die in samenhang kunnen leiden tot bredere

of diepere toegang dan afzonderlijke zwakheden zouden toelaten, zonder onnodige schade aan systemen of gegevens te veroorzaken.
Doel van een pentest is niet om zoveel mogelijk zwakke plekken te vinden, zoals bij een kwetsbaarheden/vulnerability scan.

Per pentest is relevant welke expertise benodigd is, tot wellicht een gespecialiseerde partij. Ook is de aanname dat het doen van een infrastructuur/web-pentest anders is dan een test op een fysiek apparaat (e.g. mobiele webapp).

Buiten scope

- Red teaming – een geavanceerde en gecontroleerde securitytest waarbij een realistische cyberaanval op 1 of meerdere kritieke functies van een (doelwit)organisatie wordt uitgevoerd. Dit gebeurt op basis van reële dreigingen. Het doel van een red teamingtest is om de beveiligingsmaatregelen van een organisatie te testen en de organisatie hiervan te laten leren[1]. Red teaming is gericht op het testen van de volledige detectie- en responscapaciteit van een organisatie, inclusief technische, menselijke en organisatorische verdediging, waar een pentest een beperktere, technische scope heeft en vooral gericht is op specifieke kwetsbaarheden in systemen, netwerken, applicaties of andere digtale componenten.
- Purple teaming - separate securitytest door Red team en Blue team gezamenlijk om de leerervaringen van de geteste organisatie te vergroten. Purple teaming is onderdeel van Red teaming, maar kan ook als separate securitytest worden ingekocht.
- Gold Teaming - een samenwerkingssessie met de crisismanagementteam van de opdrachtgever met het doel het crisismanagement te valideren, trainen en te oefenen in een gecontroleerde omgeving op basis van een voltooid Red teaming-scenario.
- Hackathon - een evenement waarin teams van deelnemers non-stop bezig zijn om binnen een korte tijd oplossingen voor aangereikte casussen te bedenken.
- Audit op de pentest - auditwaarde is wel onderdeel van de scope en dus het rapport, maar de audit op dit rapport niet. Dit doet een onafhankelijke IT-auditor.
- Fysieke pentest - een test waarbij een organisatie aanvallen simuleert om te ontdekken hoe ze toegang kan krijgen tot een beschermde fysieke locatie/omgeving.

Auditwaarde

Opdrachtgevers hebben belang bij pentesten om inzichtelijk te maken of er kwetsbaarheden zijn en te voorkomen dat kwetsbaarheden in hun IT-systeem/applicatie etc. daadwerkelijk misbruikt kunnen worden door criminele organisaties of statelijke actoren, maar ook 'in control' te zijn over hun cyberbeveiliging en 'compliant' te zijn ingevolge wettelijke en/of beleidsmatige verplichtingen, zoals ingevolge de AVG, NIS2/Cyberbeveiligingswet, Cyber Resilience Act (CRA), de Wet digitale overheid (WDO), normenkaders zoals ISO 27001/BIO of een sectorale standaard zoals de NEN7510 voor de gezondheidszorg.

[1] Gebaseerd op: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cybersecurity/oefenen-en-kennisdelen/gereedschapskist-red-teaming/

In de voorgenomen dienstverlening zitten elementen die de bewijsbaarheid en transparantie rond een uitgevoerde pentest moeten borgen. Het eindresultaat van de pentest (in de vorm van een rapportage en aanvullende documenten/bewijsmateriaal) moet betrouwbaar, reproduceerbaar en transparant zijn en moet (optioneel) door de opdrachtgever of een derde partij (zoals een auditor) gevalideerd kunnen worden. Deze validatie/audit moet de opdrachtgever separaat kunnen laten uitvoeren om extra zekerheid te verkrijgen over de kwaliteit van de uitvoering en resultaten van de pentest. De beoogde uitvoering van een pentest is volgens de gangbare standaarden, waarover een vorm van 'in control' verantwoording kan worden afgelegd.

Op 17 december 2024 heeft de Tweede Kamer een motie van het lid Six Dijkstra aangenomen (26 643 nr 1254). In deze motie wordt de regering verzocht om overheidsbreed toe te werken naar een gestandaardiseerde methodiek voor het opdrachtgeverschap van pentests, zoals de methodiek voor Informatiebeveiligingsonderzoek met Audit Waarde (MIAUW).
Het beoogde programma van eisen is gebaseerd op de Methodiek voor Informatiebeveiligingsonderzoek met Audit Waarde (MIAUW)[2], maar de toe te passen eisen zijn deels gewijzigd en aangevuld om beter tegemoet te komen aan de behoeftes van de deelnemers aan de beoogde raamovereenkomst.

CCV-keurmerk
Het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) is een onafhankelijk schemabeheerder. Het CCV geeft de mogelijkheid aan pentestbedrijven (dienstverleners) zich door geaccrediteerde certificatie-instellingen te laten certificeren voor het uitvoeren van pentesten. Een dienstverlener met het CCV-pentestkeurmerk voldoet aan een set minimale kwaliteitseisen en kan hiermee haar afnemer(s) meer zekerheid geven over het te verwachten kwaliteitsniveau van de uit te voeren pentest. Voor de beoogde aanbesteding/raamovereenkomst pentesten kan het verlangen van een CCV-keurmerk voordelen bieden gelet op de kwaliteitswaarborgen, maar er zijn ook risico's. Het in een Europese aanbesteding vereisen van een dergelijk keurmerk is namelijk uitsluitend mogelijk als inschrijvers die dit keurmerk niet hebben (uit Nederland dan wel uit andere landen) de gelegenheid wordt gegeven om aan te tonen dat zij aan een vergelijkbaar niveau voldoen. Transparantie over de keurmerkvereisten en/of het kunnen beoordelen van alternatieven met gelijkwaardige niveaus is daarom belangrijk. Dienstverleners zonder dit keurmerk kunnen immers ook kwalitatief goede pentesten uitvoeren. Aanbestedende dienst wijst hierbij op het beoogde programma van eisen voor de aanbesteding, dat gebaseerd is op MIAUW en delen van het CCV-keurmerk, maar ook verschillen kent. Het programma van eisen zou naar het beeld van aanbestedende dienst voldoende waarborgen moeten bieden voor het te verwachten kwaliteitsniveau. Aanbestedende dienst is daarom niet voornemens het CCV-pentestkeurmerk te vereisen van beoogde inschrijvers op de aanbesteding.

Raamovereenkomst

[2] GitHub - brennodewinter/Informatiebeveiligingsonderzoek: Methodiek voor Informatiebeveiligingsonderzoek met Auditwaarde

In de context van een raamovereenkomst is de uitdaging om de beloofde kwaliteit ook daadwerkelijk beschikbaar te hebben voor een concrete nadere opdracht (nadere overeenkomst).
Daarbij speelt, gegeven de gemiddelde omvang van een pentest, ook de vraag wanneer/waar een mini-competitie voldoende rendement biedt om aan te bieden en wanneer/waar niet, mede indachtig de inkoop-inspanning versus het resultaat/rendement van de te gunnen opdracht. Hiermee is ook direct verbonden het ideale aantal partijen bij een raamovereenkomst. Een eerste schatting is tussen 5 en 10 partijen.

Prijs
In de raamovereenkomst worden prijseenheden voorzien, zoals mogelijk (maximum) tarieven per uur/testdeel/fase/uur.
Voor de daadwerkelijke uitvoering van een pentest moeten de tijd en prijs vastliggen (time boxed) en alle gevraagde werkzaamheden worden opgenomen, inclusief rapportage en presentatie, maar exclusief een mogelijke hertest.
Mogelijk kan per soort pentest een vast tarief voor de gehele test worden bepaald.
Bij constatering van een tekortkoming/blokkerende bevinding in een pentest, los je dat als organisatie op. Een hertest is standaard optioneel in een opdracht voor een pentest, zodat ook het rapport kan worden aangepast in plaats van helemaal opnieuw te laten opmaken. Het is een vorm van nazorg en wegens de relatief geringe tijdsinspanning is het niet zinvol dit in een opvolgende aanvraag opnieuw in de raamovereenkomst uit te zetten. Een opdracht voor een pentest is dus de test + eventuele hertest.

Vrijwaring
De opdrachtnemer (pentester), opdrachtgever en eventueel nog derden (voor zover te onderzoeken objecten niet in eigendom van de opdrachtgever zijn) komen per Nadere overeenkomst een vrijwaringsverklaring overeen voor het uitvoeren van een pentest. In de vrijwaringsverklaring worden de risico's beschreven die het uitvoeren van het onderzoek met zich meebrengt, wordt toestemming gegeven voor aanval op / toegang tot bepaalde objecten en wordt vrijwaring van aansprakelijkheid met betrekking tot de uitvoering van het onderzoek nader geregeld. De opdrachtgever draagt zorg voor afstemming met eventuele derden en ondertekening en retournering van de vrijwaringsverklaring aan opdrachtnemer voordat het onderzoek start. Veel vrijwaringsverklaringen zijn in eerste lezing helder en gebalanceerd, doch verwijzen veelal naar hetgeen in de opdrachtomschrijving staat en wat in dat kader van de pentester aan activiteit wordt verlangd. Dit betekent dat de vrijwaring, althans wat die in de praktijk echt betekent, voor een belangrijk deel in de opdrachtomschrijving staat en niet zozeer in de vrijwaringsverklaring. Het is niet ongewoon dat bestuurders/managers vanuit hun bestuursaansprakelijkheid huiverig zijn bij het tekenen van vrijwaringsverklaringen van de pentester. Daarbij kan het zijn dat een bepaalde manager niet kan overzien of hij/zij iets dergelijks mag tekenen. Wanneer de productie verstoord raakt en er komen kosten uit voort voor herstel kan men die niet vrijwaren.

AI en Cryptografie
AI kan bij pentesten wel (gaan) voorkomen. Quantum computing is er nog niet (althans niet in regulier gebruik). Desondanks is het zaak dit in het vizier te houden. Ook al verschillen diverse voorspellingen, bestaat de kans dat het sneller zich voor zal doen dan verwacht. Er zijn experts die verwachtingen hebben over 2 tot 5 jaar.

Quantum-protocollen is iets wat moet worden meegenomen als je dit wilt testen. Een pentester moet in toenemende mate in staat zijn om quantum-protocollen te kunnen testen. Veel quantum-beveiliging in producten zitten nu nog in een preview-fase, dus nog niet algemeen verkrijgbaar. De verwachting is niettemin dat dit binnen de contractperiode van RVICTO26 danig zal gaan veranderen.

Onderscheidend vermogen

Het vakgebied pentesten kent keurmerken, raamwerken, kaders uit regelgeving et cetera. Ook kunnen belangrijk skills van en pentester buiten certificaten en formeel vaststellingen liggen. Het ligt voor de hand om te vragen naar kennis en ervaring in/met het werken met standaarden (OWASP, CVSS, CIS benchmarks, PTES); Erkende kwalificaties en toepasselijke certificeringen (e.g. ISO/IEC 27001, ISO/IEC 29147, ISO 30111, NIST 800-115, FedRAMP, FIPS 140-2); certificering eindverantwoordelijke pentester/rapporteur(s) en overige in te zetten professionals (zoals OSCP/OSEP/|OSCE/OSCE/OSWE/ eWPTX, GPEN, GWAPT, GXPEN). De vraag daarbij is in hoeverre certificaten zekerheid geven over de gevraagde skills bij personen. Er zijn bijzonder goede pentesters die wellicht niet over bepaalde certificaten beschikken. M.a.w. hoe verhoudt de gevraagde kwaliteit zich t.o.v. een bewijsmiddel en andere manieren om van de gevraagde kwaliteiten c.q. capaciteiten te kunnen overtuigen? En als iedereen de test op nagenoeg dezelfde wijze volgens nagenoeg hetzelfde raamwerk met checklist uit zal voeren, wat maakt dan de ene pentester/opdrachtnemer beter dan de andere? Er zijn wellicht bedrijven die specifieke gebieden hebben waarop ze zich kunnen onderscheiden, maar is daarvoor een objectieve maatstaf voorhanden? Als die elementen gevonden zijn, welke zijn dan relevant op ROK-niveau en wat blijft dan aan onderscheiden vermogen over op NOK-niveau?

Nummer	Vraag en antwoord
P1	Wat is uw bespiegeling rond het indelen van Penetratietesten en Red Teaming in afzonderlijke raamovereenkomsten en het beoogde effect daarmee op de markt en opdrachtgevers?
Antwoord	
P2	Is binnen het domein van pentesten een binnen de markt algemeen houvast van termen en typen van testen, waarmee de te leveren diensten houvast geboden kan worden, zodanig dat producten concreet in concurrentie kunnen worden uitgevraagd?
Antwoord	
P3	Beoogd is te vereisen dat de pentesten worden uitgevoerd volgens de fasering van de Pentest Execution Standard (PTES) (http://www.pentest-standard.org/index.php/Main_Page) of, na acceptatie door de opdrachtgever, volgens de fasen van een vergelijkbare erkende industriestandaard. De belangrijkste overweging hierbij is de uniformiteit, volledigheid en passendheid van de PTES. Er geldt dus een uitgangspunt van PTES, tenzij... Hiernaast zijn combinaties met andere meer

	inhoudelijke standaarden toegestaan (o.a. OWASP, NIST e.a.). De vraag is of het standaard eisen van de fasering van PTES bezwaarlijk kan zijn en waarom c.q in welke gevallen? Zo ja, welke alternatieve standaard(en) voor de fasering van de pentest stelt u voor, in plaats van of naast de PTES?
Antwoord	
P4	Hoe kan worden ingespeeld op de verwachting van de opdrachtgever rond de in te zetten capaciteit voor een concrete opdracht in relatie tot wat de leveranciers bij inschrijving voor de ROK in het vooruitzicht hebben gesteld?
Antwoord	
P5	Wat is uw beeld bij het aantal partijen bij een raamovereenkomst? Relevante elementen zijn onder andere hoeveel pentesten u zou kunnen uitvoeren, naast wat u nu al doet (dus: wat u beschikbaar zou hebben voor deze ROK), dan wel het maximaal aantal deelnemers dat u (gelijktijdig) kunt bedienen. Het is essentieel dat we beeld hebben van het absorptievermogen in de markt is en hoe daarop evenwichtig kan worden ingespeeld.
Antwoord	
P6	Wanneer is een offertetraject voor u zinvol om in een mini-competitie een aanbieding te doen? Denk hierbij aan overwegingen als: - Inkoop-inspanning vs. resultaat/rendement opdracht? - (Wanneer) past een afroepcontract onder de ROK? - Binnen welke kaders? - Hoe past een opdracht bij het aanbod? - Kans op de opdracht en het aantal opdrachtnemers in de ROK.
Antwoord	
P7	Wat is uw beeld bij prijsmodaliteiten voor pentesten qua eenheid en voorspelbaarheid van totale kosten? We gaan uit van algemeen in markt gebruikelijke prijsmodaliteiten met daarin diverse vaste en verrekenbare elementen. Graag vernemen wij wat daarin voor-/nadelen kunnen zijn, met name ten aanzien van vaste en verrekenbare delen.
Antwoord	
P8	Welke informatie (inzicht) heeft u nodig van deelnemers om voor de aanbesteding van de raamovereenkomst een passende inschrijving te kunnen doen? Houdt er rekening mee dat er binnen de raamovereenkomst nog minicompetities uitgevoerd moeten worden om de concrete opdrachten te kunnen verstrekken. In deze minicompetities kan/moet meer gedetailleerde achtergrondinformatie verstrekt worden.
Antwoord	

P9	Welke ervaring heeft uw organisatie met vrijwaringsverklaringen die nodig zijn bij de start van een pentest, maar door betrokkenen niet tijdig genoeg ondertekend worden en de start van een pentest ophouden? Welke aandachtspunten en/of tips kunt u meegeven?
Antwoord	
P10	Zijn er pentesters/dienstverleners die al rekening houden met AI en Quantum cryptografie componenten bij pentesten? Hoe zou u deze elementen in een marktbenadering (aanbesteding) zinvol ingebed zien?
Antwoord	
P11	Is het vereiste van een CCV-keurmerk of gelijkwaardig nuttig als geschiktheidseis (knock out)? Zo ja waarom, zo nee waarom niet?
P12	Welke subgunningscriteria kunnen naar uw beeld het beste worden ingezet in de keuze van opdrachtnemers voor de raamovereenkomst? En welke subguningscriteria stelt u dan voor mededinging (minicompetities) bij de verstrekking van nadere overeenkomsten voor?
Antwoord	
P13	In bijlage 2 bij dit document treft u een conceptversie van het programma van eisen aan. Bij de totstandkoming van deze versie van het programma van eisen is gebruik gemaakt van de Methodiek voor Informatiebeveiligingsonderzoek met Audit Waarde (MIAUW), waarin suggesties voor inkoopeisen voor pentesten zijn opgenomen, maar zijn ook aanvullingen en aanpassingen op MIAUW gemaakt om beter tegemoet te komen aan de diversiteit van behoeftes van betrokken Deelnemers. Wat vindt u van de voorliggende conceptversie van het programma van eisen? Bij uw beantwoording gaat u bij voorkeur in op de volgende subvragen: a. Welke eisen moeten naar uw mening vervallen of afgezwakt worden om te voorkomen dat u en/of andere potentiële inschrijvers hier niet aan kunnen/willen voldoen (verlagen instapniveau)? Motiveer uw antwoord. b. Welke eisen moeten naar uw mening nog toegevoegd of strikter gesteld worden om risico's voor Deelnemers te beperken/minimaliseren (verhogen instapniveau)? Motiveer uw antwoord. c. Welke andere suggesties wilt u doorgeven?
Antwoord	
P14	Als bijlage 2 bij dit document treft u een conceptversie van het programma van eisen aan. Bij dit programma van eisen is een modelrapportage gevoegd. Deze modelrapportage kent een

	standaard opzet/indeling, gebaseerd op de diverse eisen. Bij toekomstige verstrekking van een opdracht (pentest) wordt verwacht dat een opdrachtnemer op basis van de uitgevoerde pentest een rapportage oplevert, conform de vastgestelde modelrapportage, met standaard hoofd- en paragraafindeling. Dit model moet zorgen voor uniformiteit, transparantie, compleetheid van de rapportage en reproduceerbaarheid van het onderzoek. Opdrachtgever kan nieuwe versies van dit model vaststellen, die opdrachtnemer daarna dient toe te passen. Opdrachtnemer heeft tijdens de looptijd van de raamovereenkomst de mogelijkheid suggesties aan opdrachtgever te geven voor verbetering van het model. Afwijking van dit model is alleen toegestaan na schriftelijke goedkeuring van Deelnemer, overeen te komen in het plan van aanpak (pre-engagement) van een pentest. a. Wat vindt u van de opzet (indeling) van de huidige versie van de modelrapportage? b. Welke wijzigingen moeten naar uw mening in de modelrapportage doorgevoerd worden (toevoegingen, wijzigingen, verwijderingen)?
Antwoord	
P15	Hieronder is ruimte voor uw eventuele aanvullende reactie.
Reactie	

3.2 Red Teaming

<u>Raming jaar 1 t/m 4</u>
€5.000.000 - €44.000.000
48 Red teaming testen volgens ART/TIBER, met daarnaast aanvullende behoefte.

De range heeft te maken met de keuze voor ART of TIBER, waarbij ART modulair is opgebouwd. Er wordt gestreefd naar 12 ART/TIBER Red Teaming testen per jaar. Dit kan minder of meer zijn, afhankelijk van de behoefte en de capaciteit voor ondersteuning en monitoring door het Test Cyber Team Rijk (TCT Rijk), wat een vast onderdeel is in ART en TIBER.

Met betrekking tot Red teaming is onder ministeries overwogen dat Red teaming snel zal raken aan hoge te beschermen belangen (TBB) c.q. 'kroonjuwelen' en ook te dien aanzien het hoogste nut heeft. Omdat 'kroonjuwelen' in het geding zullen komen, worden ter zake Red teaming testen bij ministeries alleen uitgevoerd volgens ART/TIBER, begeleid door het TCT-team van CIO Rijk.

Deelnemende zelfstandige organisaties, zoals ZBO's, maken eigen afwegingen rond methodiek en uitvoering. Ook zij kunnen Red teaming testen volgens ART/TIBER, maar ook kiezen voor andere of lichtere vormen of smallere specifieke scope. Hierbij zal ook gestreefd worden naar eenduidige typering en definities om te bepalen

wanneer en test een Red teaming test is, dan wel opschuift naar penetratiestest, zoals in het ander RVICTO-deel voor pentesten is omschreven.

Scope

Red Teaming is een geavanceerde securitytest waarbij een cyberaanval op 1 of meerdere kritieke functies van een organisatie wordt uitgevoerd. Dit gebeurt op basis van reële dreigingen. Het doel van een red teamingtest is om de beveiligingsmaatregelen van een organisatie te testen en de organisatie hiervan te laten leren. Op basis van de bevindingen uit een red teamingtest kun je verbeterplannen opstellen om de digitale weerbaarheid van de organisatie te verbeteren. Binnen scope is Red Teaming volgens het ART-raamwerk of het TIBER-raamwerk. Binnen Red Teaming volgens TIBER en ART zijn verschillende stakeholders betrokken in de verschillende fases van de test:

- Het Control Team (CT voorheen WT) organiseert en heeft de leiding over de test. Zij zijn de enige mensen binnen de organisatie die weten dat de test plaatsvindt. De Control Team Lead is de trekker van dit team.
- De Testmanager uit het Test Cyber Team (TCT) adviseert het Control Team onafhankelijk over de verschillende stappen van het raamwerk en ziet toe op de uitvoering daarvan. Het Test Cyber Team maakt formeel geen onderdeel uit van het Control Team maar werkt wel nauw samen.
- De Threat Intelligence provider (TIP) voert een brede verkenning uit zoals normaal gesproken ook door een aanvaller uitgevoerd wordt als zij hun aanval voorbereiden. Dit wordt vaak gedaan door een externe provider.
- De Red Team Provider (RTP) voert de test 'aanval' uit en maakt geen onderdeel uit van de entiteit die getest wordt. Veelal wordt hiervoor een externe partij ingeschakeld.
- Het Blue Team (BT) is de security organisatie binnen de instelling die 'aangevallen' wordt tijdens de test. Zij zijn niet op de hoogte van de test.

TCT

Red Teaming volgens ART of TIBER impliceert in beide gevallen de betrokkenheid van het Test Cyber Team (TCT) voor de rijksoverheid, momenteel een cluster binnen CIO Rijk. Het TCT geeft ook de verklaring af aan het Control Team dat een RT-oefening volgens ART of TIBER is verlopen. Het TCT is betrokken in alle fases van de test zoals wordt beschreven in het TIBER en ART-raamwerk.

Gold teaming

Gold Teaming (GT) is een crisismanagementoefening zonder daadwerkelijke aanval en kan plaatsvinden zonder een Red team (als een ad-hoc oefening). Het is ook opgenomen als onderdeel in raamwerken al CORIE en ART. In de praktijk vindt GT meestal plaats na een Red teaming test, zodat geoefend wordt met realistische informatie over mogelijke aanvalsroutes. De resultaten van een Red team test zijn meestal bepalend voor de scenario's die een GT onderzoekt. Deze oefeningen worden doorgaans geleid vanuit CISO, maar er zijn ook leidinggevenden en andere afdelingen betrokken. Het doel is het crisismanagement van een organisatie te valideren, trainen en te oefenen in een gecontroleerde omgeving op basis van een voltooid red teaming-scenario. Betrokkenheid op C-niveau is hierin essentieel. ART onderscheidt drie varianten GT:

- Walkthrough Session: Laagdrempelig en toegankelijke oefening met een daarin de bespreking van alle stappen in het crisisbeheersingsproces van detectie tot sluiting en gaat ook in op de rollen en verwachtingen van Crisismanagement Teamleden als acties en maatregelen die in specifieke crisisscenario's moeten worden genomen. Het is een op discussie gebaseerde sessie.
- Tabletop Session: Ook toegankelijk en op discussie gebaseerde oefening met als doel het oefenen van crisismanagement in een omgeving met weinig stress op basis van een fictief scenario.
- Full Simulation: Meest uitgebreid en uitdagend. Een interactieve crisis simulatie, waarin het crisismanagementteam ervaart hoe het is om met een echte crisis geconfronteerd te worden. Het doel is het oefenen onder (tijd)stress op basis van een realistisch crisisscenario dat zich in realtime ontvouwt met of zonder tegenspel (statisch of dynamisch scenario).

GT-provider kan RT-provider zijn, maar dat hoeft niet. Er zijn bedrijven die zich specifiek op GT richten.

Buiten Scope
- Pentesten – zoals hierboven omschreven in het onderwerp 3.1 Penetratietesten.

Raamovereenkomst
Beoogd is het per Red Teaming test contracteren van een Red Team Provider (RTP) voor de uitvoering van de Red Team test. In een Red Teaming test is ook een Threat Intelligence Provider (TIP) betrokken voor het leveren van de gerichte dreigingsinformatie voor de testfase en indien nodig extra inlichtingen verstrekken tijdens de Red Teaming test. In de praktijk is het voor de onafhankelijkheid goed als dit twee verschillend aangetrokken partijen zijn. Dit sluit echter niet uit dat één provider beide producten (al dan niet met onderaannemer) prima kan leveren als die daar aantoonbaar muren tussen zet. De RTP en TIP zijn dus bij voorkeur twee verschillende opdrachtnemers, maar dat hoeft niet in alle gevallen de keuze te zijn. De TIP zal derhalve altijd optioneel mogelijk zijn bij een RTP-opdracht. Voor separaat aantrekken van de TIP wordt deze uitgewerkt in het RVICTO-deel "Overige IB-diensten".

De keuze voor het aantal dienstverleners in een raamovereenkomst wordt mede bepaald door de aantrekkelijkheid en te behalen rendement. Meer rekenkundige elementen zijn o.a.:
- kans op een opdracht
- acquisitie-kosten ten opzichte van te behalen rendement (marge/winst)
- absorptievermogen van dienstverleners: kan het aantal geselecteerde partijen het verwachte aantal ART/TIBER-trajecten aan?

Minder rekenkundig uit te drukken elementen die pleiten voor afwisseling van partijen zijn o.a.
- nationale veiligheid. Niet alle kroonjuwelen bij één RT-provider, maar ook niet onder teveel i.k.v. beheersbaarheid van de veiligheid en vertrouwelijkheid? In hoeverre wordt deze gedachtegang ondersteund door ABRO en BIO?
- creativiteit. Met afwisseling geeft meer een noodzakelijke creativiteit van partijen en RT testen niet sleets raken.

Voor RT-providers kan gedacht worden aan 10-12 partijen bij de raamovereenkomst.

Aandachtpunt is de beschikbaarheid van partijen bij een concrete aanvraag. Het aantal marktpartijen met ART/TIBER-ervaring is mogelijk gering ten opzichte van de verwachte vraag vanuit de overheid als ook die van andere opdrachtgevers (met name financiële instellingen). Het streven is om tot een modus/mechanisme te komen waarin/waarmee partijen ART/TIBER ervaring kunnen opdoen, zonder compromissen te doen op de te verwachten kwaliteit van uitvoering of de raamwerken ART/TIBER.

Prijs

Elk project zal uniek zijn in termen van kosten, doelstellingen en teamleden. Kosten zijn sterk afhankelijk van arbeidsintensiteit en de bestede middelen (welke risico's zijn aanwezig, welke aanvalssectoren moeten worden uitgewerkt enz.)
In de raamovereenkomst worden prijseenheden voorzien, zoals mogelijk (maximum) tarieven per uur/testdeel/fase/uur. RT-testen zijn niet ongewoon gecontracteerd te worden op basis van Fixed Price + post voor onvoorziene uitgaven (PVOU), niet zijnde stelpost. In principe wordt geen gebruik gemaakt van stelposten. Voor de daadwerkelijke uitvoering van een Red Teaming test is de aanname dat de tijd en prijs vast te leggen (time boxed) en alle gevraagde werkzaamheden moeten daarin worden opgenomen, inclusief rapportage en presentatie.

Onderscheidend vermogen

Punten waarop een offerte van een RT-provider voor een concrete RT-opdracht op kwaliteit beoordeeld kan worden en waarin onderscheidend vermogen kan worden gevonden, zijn:

- Aanpak en planning. Te besteden tijd, argumentatie voor de aanpak, multidisciplinair team, duidelijkheid hoe de test gedaan wordt, beschrijving van verschillende fases, …
- Gevoelige informatie. Helderheid en eenduidigheid van omgang/behandeling (ad hoc en structureel), geheimhoudingsverklaring, verwerkersovereenkomst, bewaartermijn, circles of trust, …. E.e.a. voor zover dat in een offerte zinvol is. Hierin kunnen het reguliere standaard maatregelen zijn, maar ook specifieke maatregelen of voorzieningen voor de betreffende RT-opdracht. Denk hierbij ook aan screening en geheimhouding.
- Kennis & ervaring. Referenties als op opdracht-specifieke elementen daartoe aanleiding geven. Idem voor certificering, opleidingen, en wellicht ook links naar publicaties. Immers, bij een NOK is het team concreet.
- Beschikbaarheid. De houdbaarheid die een aanbieding heeft met betrekking tot de daadwerkelijke beschikbaarheid in de uitvoering van de geoffreerde teamleden.

De Praktische Inkooprichtlijnen voor Red-teaming testen geven veel kenmerken waarmee een RTP in eisen en wens kan worden omschreven, van kennis en ervaring, certificaten, recruitment-proces, mate van 'legs up', risicomanagement, R&D, operationele skills, een en ander gericht op het bedrijf, de RT-manager en het RT-team. De kern draait niettemin om kwalificaties en ervaring. Red Teaming blijft uiteindelijk een door mensen geleid proces. Dat brengt voorzichtigheid in het oordeel over alles wat te maken heeft met diensten en het aanbieden van

statistieken. Dat blijft van betrekkelijke betekenis. Toch moet een gunning op basis van objectieve criteria worden verantwoord, zowel op ROK-niveau en NOK-niveau.

R1	Hoe kunnen we inspelen op verwachting rond in te zetten capaciteit in de uitvoering en dat wat als verwachting door de leverancier is opgegeven voor de ROK, gegeven de schaarste aan ART/TIBER ervaring in de markt en de grote vraag bij organisaties (met name financiële instellingen vanuit DORA-regelgeving)?
Antwoord	
R2	Wat is uw beeld bij het aantal Red Teaming-partijen bij een raamovereenkomst? Relevante elementen zijn onder andere hoeveel ART/TIBER testen u zou kunnen uitvoeren, naast wat u nu al doet (dus: wat u beschikbaar zou hebben voor deze ROK), dan wel het maximaal aantal deelnemers dat u (gelijktijdig) kunt bedienen. Het is essentieel dat we een beeld hebben van het absorptievermogen in de markt is en hoe daarop evenwichtig kan worden ingespeeld.
Antwoord	
R3	Heeft u suggesties op welke wijze de beoogde aanbesteding voor een raamovereenkomst naar uw inzicht kan bijdragen aan het vergroten van het speelveld van marktpartijen die ervaring hebben met het ART/TIBER, voor partijen die dat bij inschrijving op de aanbesteding niet hebben? Wat zijn dan de essentiële kwaliteitsaspecten van een inschrijver zonder ART/TIBER ervaring, die bij eventuele gunning van de raamovereenkomst wel opdrachten van deelnemers voor Red Teaming testen conform ART of TIBER op kwalitatief beoogde wijze moeten kunnen uitvoeren?
Antwoord	
R4	In bijlage 3 bij dit document treft u een conceptversie van het programma van eisen aan op basis van ART/TIBER. Wat vindt u van de voorliggende conceptversie van het programma van eisen? Bij uw beantwoording gaat u bij voorkeur in op de volgende subvragen: a. Welke eisen moeten naar uw mening vervallen of afgezwakt worden om te voorkomen dat u en/of andere potentiële inschrijvers hier niet aan kunnen/willen voldoen (verlagen instapniveau)? Motiveer uw antwoord. b. Welke eisen moeten naar uw mening nog toegevoegd of strikter gesteld worden om risico's voor Deelnemers te beperken/minimaliseren (verhogen instapniveau)? Motiveer uw antwoord. Welke andere suggesties wilt u doorgeven?
Antwoord	

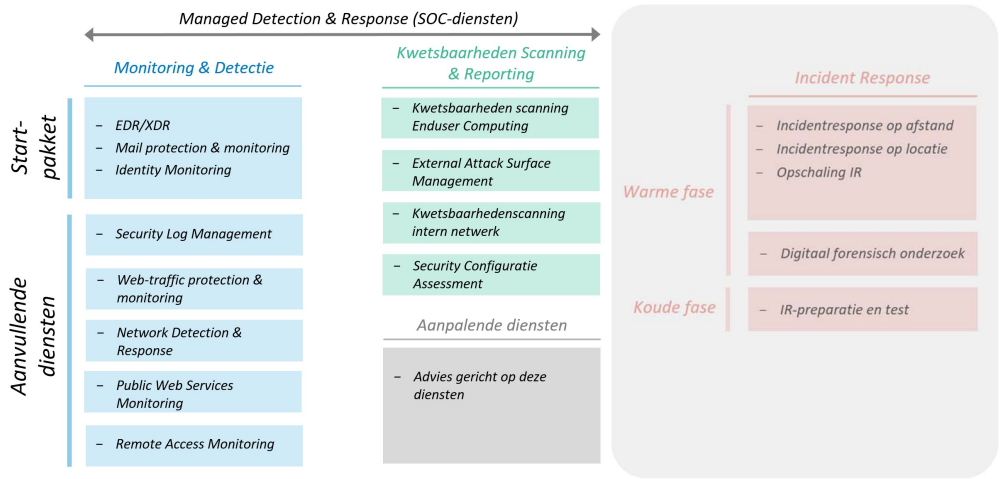
R5	Welke subgunningscriteria dragen volgens u het beste bij aan de keuze van een ROK-partner en welke voor de NOK?
Antwoord	
R6	Welke subgunningscriteria dragen volgens u het beste bij aan de keuze voor een Threat Intelligence Provider?
Antwoord	
R7	Hieronder is ruimte voor uw eventuele aanvullende reactie.
Reactie	

3.3 SOC-diensten

Raming jaar 1 t/m 4
€ 60.000.000

Opdrachtgevers: 30
Werkplekken: 15.000
Mobiele accounts: 10.000
Gebruiker accounts: 15.000
E-mail accounts: 15.000
E5-licenties: 5.000
(aantallen zijn circa en sterk afgerond voor de orde van grootte)

De scope van SOC-diensten betreft hoofdzakelijk Monitoring & Detectie en Kwetsbaarheden Scanning & Reporting.



Naast het volledig zelf doen of volledig uitbesteden zijn er hybride samenwerkingsvormen mogelijk, zoals een rolverdeling tussen een deelnemer en een Managed Security Service Provider (MSSP) op tijdsaspecten (bijvoorbeeld zelf doen 08:00-17:00 uur, MSSP 17:00 – 08:00 uur), op complexiteit (1e lijnsfunctie zelf doen, 2e lijnsvragen voor MSSP), op taken (monitoring en detectie zelf doen,

kwetsbaarheden scanning en reporting voor MSSP) of scope (bepaalde ICT-assets voor eigen SOC, bepaalde assets voor MSSP).
De eventuele randvoorwaarden en complexiteiten bij het leveren van SOC-diensten in hybride samenwerkvormen zullen per opdracht (minicompetitie) expliciet worden gemaakt, omdat deze sterk afhankelijk zijn van het start- en streefbeeld van een deelnemer (wat heeft hij nu, wat wil hij met uitbesteding bereiken).

3.3.1 Monitoring & Detectie (M&D)

M&D omvat alles wat nodig is voor het vaststellen van verdachte gedragingen binnen een ICT-omgeving (gebruikers, netwerk, infrastructuur, applicaties en data) op basis van log data uit de betreffende ICT-omgeving en gespecialiseerde detectietechnologie. Bij detectie van verdachte gedragingen of patronen genereren de detectiesystemen meldingen. Meldingen worden beoordeeld en opgevolgd door monitoring: het continu bewaken van een computer of digitaal netwerk op verdachte activiteiten, bedreigingen, zoals bijvoorbeeld malware, datalekken, phishing, enzovoort. Meldingen uit de detectiesystemen worden continu in de gaten gehouden, beoordeeld en voorzien van opvolging (doorgifte aan Incident Response). De voorgenomen overeenkomst betreft een raamovereenkomst. Deelnemende diensten kunnen via een nadere overeenkomst de dienstenniveaus afstemmen op de specifieke behoefte van de deelnemende dienst. Zo kunnen bepaalde deelnemers een 24/7 dienstverlening afnemen, terwijl andere deelnemers bijvoorbeeld een 5x8 (werkdagen & kantoortijden) dienstverlening wensen. In geval van een hybride SOC kan het juist gewenst zijn dienstverlening buiten kantoortijden af te nemen.

3.3.1-a Modulaire opbouw
De M&D-diensten zijn samengesteld uit een aantal logische bouwstenen die de basis en voor een goed begin c.q. eerste stap naar SOC-diensten zijn. Er is voor deze aanpak gekozen, zodat deelnemers SOC-diensten kunnen implementeren volgens een groeipad dat aansluit op de behoeftes en wensen van de deelnemer.

Een belangrijk onderscheid tussen deze bouwstenen is het startpakket en de aanvullende diensten. Het startpakket omvat alle elementen die nodig zijn om een SOC-dienst te kunnen leveren. Denk hierbij aan zaken als bemensing van een SOC, SIEM-systemen, processen en procedures, etc. Als een Deelnemer geen SOC heeft en SOC-diensten wil uitbesteden, ligt het voor de hand dat de deelnemer eerst het startpakket M&D-diensten afneemt binnen de raamovereenkomst. De afname hiervan is in beginsel een randvoorwaarde om aanvullende M&D-diensten af te kunnen nemen.

M&D-diensten worden eenmalig in minicompetitie uitgevraagd. Aanvullende diensten die later worden ingekocht, gaan naar de in de eerste mini-competitie gekozen dienstverlener. Dit omdat deze diensten dusdanig met elkaar zijn verweven, dat het om meerdere redenen niet voor de hand ligt dit over meerdere dienstverleners te verdelen. Dit laat onverlet hybride situaties. De eerste NOK voor M&D-diensten kent derhalve automatisch de overige aanvullende diensten als optioneel.

Als een deelnemer geen eigen SOC heeft en de M&D-diensten binnen de raamovereenkomst afneemt bij opdrachtnemer X, mag hij de andere opdrachtnemers uitsluiten van mededinging indien hij aanvullende M&D-diensten

wil afnemen. De aanvullende diensten kunnen dan alleen door opdrachtnemer X geleverd worden, omdat zij verbonden zijn aan afname van het startpakket. Idealiter neemt de deelnemer deze opties (om aanvullende diensten af te nemen) gelijk mee bij de opdrachtverstrekking voor het startpakket. Een combinatie van opdrachtnemer X voor het startpakket en opdrachtnemer Y voor aanvullende M&D-diensten kan leiden tot ongewenste risico's/knelpunten en kan om die reden uitgesloten worden.

Als een deelnemer wel een eigen SOC heeft, kan hij ervoor kiezen het startpakket en/of aanvullende M&D-diensten af te nemen in de ROK. Er ontstaan dan hybride samenwerkvormen tussen deelnemer en een opdrachtnemer, waarbij de afbakening gespecificeerd moet worden in de minicompetitie/opdracht.

Er wordt binnen de M&D-diensten een Startpakket samengesteld met enkele diensten die tezamen als eerste logische stap worden beschouwd. Aanvullend op het Startpakket zijn er diensten die per dienst kunnen worden afgenomen. Dit noemen we de aanvullende diensten.
Het is aan deelnemers in hoeverre men gedurende de contractperiode deze aanvullende diensten afneemt en in welke volgorde. Bij een aanvraag voor een Startpakket zal de betreffende deelnemer zich inspannen om een mogelijk te voorziene groeipad geven, zodat het reëel te verwachten opdrachtpotentieel bij aanvang helder is in de context van: alle overige Basisdiensten zijn als optie meegenomen.

Het uitgangspunt is dat het startpakket laagdrempelig is af te nemen. Dit vereist een eenvoudig tariefmodel voor het startpakket.

M&D Startpakket

a. De basis: alle benodigde voorzieningen en capaciteit die nodig zijn om de bewaking van ICT-systemen uit te voeren. Denk hierbij onder andere aan bemensing van een SOC, SIEM-systemen, processen en procedures, etc., als ook het inregelen van processen en procedures bij de betreffende Deelnemer en Opdrachtnemer (voor zover niet al zijn ingericht). Ook omvat deze dienst het onderzoeken en melden van (mogelijke) beveiligingsincidenten.

b. EDR/XDR: Hiermee wordt voorzien in het continu bewaken en beschermen van endpoints (werkplekken en servers). Deze dienst omvat alles wat nodig is om de endpoints te kunnen monitoren en ervoor te zorgen dat de onder (a) genoemde basis de overeengekomen werkzaamheden kan uitvoeren. EDR/XDR functioneert door middel van geïnstalleerde agents op de componenten die bewaakt worden.

c. Mail protection & Monitoring: Deze dienst verzorgt het scannen en monitoren van in- en uitgaand emailverkeer om spam, phishing en malware tegen te houden en datalekken zoveel mogelijk te voorkomen.

d. Identity Monitoring: Met Identity Monitoring worden accounts beschermd en gemonitord om credential breach tegen te gaan of snel te detecteren.

M&D Aanvullende diensten	- Security Log Management: Dit is een dienst die zich richt op het verzamelen, beheren en analyseren van informatiebeveiliging gerelateerde logdata. Het biedt gecentraliseerde mogelijkheden voor logboekbeheer en is ontworpen om organisaties aan wet- en regelgeving te laten voldoen en hun beveiligingspropositie te verbeteren. - Web-traffic protection & Monitoring: Hiermee wordt uitgaand internet browsing verkeer beschermd en gemonitord op het bezoeken van ongewenste web sites en het binnenhalen van ongewenste software. Dit kan worden gedaan op het endpoint of op de centrale internet proxy. - Network Detection & Response: Hierbij wordt in- en uitgaand netwerkverkeer of netwerkverkeer binnen het eigen netwerk continu gemonitord om verdachte gedragingen te detecteren. - Public Web Services Monitoring: Het monitoren van services die organisaties openbaar aanbieden, zoals websites. Met behulp van public web service monitoring worden bijvoorbeeld de logs gemonitord van Web Application Firewalls en Webservers om inbraakpogingen vanaf het internet op publieke services te detecteren. - Remote Acces Monitoring: Dit betreft monitoring van verdacht gedrag op externe toegangsdiensten van een organisatie.

3.3.2 Kwetsbaarheden scanning & reporting (KS&R)

Kwetsbaarhedenbeheer omvat onder andere het bepalen van:
- wat specifieke kwetsbaarheden in digitale systemen zijn;
- hoe deze te zien c.q. te ontdekken zijn;
- wat wordt gedaan als een kwetsbaarheid is geconstateerd;
- wie in dit geheel welke rol speelt; en
- hoe en aan wie wanneer gerapporteerd wordt.

Deze dienst richt zich op het Scannen & Rapportage onderdeel van kwetsbaarhedenbeheer (niet de verwarren met beheer of beheerstaken). Deze 'vulnerability scans' (KS&R) zijn doorgaans in de vorm van duurprestaties c.q. abonnementen voor tijdsperioden waarin continu of periodiek scanning en rapportage wordt uitgevoerd/geleverd. Omdat het inregelen van deze scans veel aansluiting op ICT-assets en voorbereiding betreft, gaan we vooralsnog niet uit van het 'per stuk' afnemen van deze vulnerability scan.

Goed is om hier ook meteen het onderscheid te maken tussen de hier bedoelde 'vulnerability scan' en pentesten waar we hier niet op doelen.

De hier bedoelde kwetsbaarhedenscans hebben als doel om bekende kwetsbaarheden automatisch te identificeren. In tegenstelling tot pentesten

worden kwetsbaarhedenscans snel en geautomatiseerd uitgevoerd, maar hebben minder diepgang dan pentesten. Daarnaast worden kwetsbaarhedenscans met korte intervallen (wekelijks of maandelijks) uitgevoerd, terwijl pentesten minder of met een veel lagere frequentie worden herhaald.

Opdrachtnemers die deze dienst leveren brengen de ICT-assets en kwetsbaarheden bij of namens deelnemer in kaart, evalueren bevindingen en rapporteren hierover aan deelnemer. Meldingen en rapportages worden voorzien van duiding en handelingsperspectief. Daarnaast omvat deze dienst het adviseren van de deelnemer om bevindingen adequaat te verhelpen en het bewaken en rapporteren over de mate waarin opvolging (het wegnemen van kwetsbaarheden) wordt gegeven aan eerdere meldingen en rapportages.

Overige activiteiten in het kader van kwetsbaarhedenbeheer, bijvoorbeeld het daadwerkelijk wegnemen van kwetsbaarheden, zijn aan de deelnemer zelf.

Een deelnemer kan met of zonder eigen SOC ervoor kiezen om de KS&R-diensten in te kopen binnen de raamovereenkomst. Er is geen noodzakelijke relatie met de afname van monitoring- en detectiediensten (M&D-diensten) binnen de raamovereenkomst, oftewel hij kan met of zonder afname van M&D-diensten (startpakket en/of aanvullende diensten) overgaan tot het afnemen van KS&R-diensten. De deelnemer is niet gebonden aan eenzelfde opdrachtnemer als bij de M&D-diensten, dus laat in principe alle opdrachtnemers in de raamovereenkomst meedingen om KS&R-diensten te mogen leveren.

Binnen KS&R wordt onderscheid gemaakt in de volgende onderdelen:

- Kwetsbaarheden scanning End User Computing
  Deze dienst omvat het periodiek in kaart brengen van assets en kwetsbaarheden, het evalueren van bevindingen, en het hierover rapporteren. Tevens omvat de dienst het geven van duiding en handelsperspectief, adviseren van de organisatie met het verhelpen van bevindingen en bewaken en rapporteren over de opvolging (is de kwetsbaarheid opgelost). De scope is van dit onderdeel betreft alleen End-user computing omgevingen.

- Kwetsbaarheden scanning intern netwerk
  Dit omvat het periodiek in kaart brengen van assets en kwetsbaarheden, het evalueren van bevindingen en het rapporteren hierover. Daarnaast adviseert u de organisatie door duiding en handelsperspectief te bieden voor de bevindingen. De scope bevat alles behalve end-user computing en zal vooral bedrijfsapplicaties in datacentra en soortgelijke omgevingen omvatten.

- External Attack Surface Management
  Deze dienstverlening omvat het in kaart brengen van alle toegangspunten die vanaf het internet toegang tot ICT-bedrijfsmiddelen geven. Het in kaart brengen omvat ook het identificeren van bijbehorende kwetsbaarheden en configuratiefouten. De bevindingen worden geëvalueerd en geprioriteerd (beoordelen). De uitkomsten worden met opdrachtnemer gedeeld (rapporteren) zodat deze in staat is om ze op te volgen en op te lossen.

- Security Configuratie Assessment
  Deze dienstverlening omvat het scannen van platformen op correcte inrichting en configuratie op basis van security inrichtingsstandaarden. Daarnaast levert deze dienst op basis van de scans een rapportage aan de opdrachtgever met alle bevindingen met bijbehorende duiding en handelsperspectief.

3.3.3 Aanpalende Diensten

Naast c.q. aanvullend op de SOC-diensten op het gebied van M&D en KS&R kan er behoefte zijn aan diensten die niet als standaarddienst zijn gedefinieerd c.q. bijkomende diensten bij de (implementatie van) SOC-diensten. Deze diensten zijn ex ante onbepaald, maar hebben een directe relatie bij afgenomen of af te nemen SOC-diensten en staan in beginsel niet op zichzelf. Binnen de categorie Aanpalende diensten kan een deelnemer een noodzaak zien om wel of juist niet de dienst exclusief binnen of buiten de raamovereenkomst te laten leveren, al dan niet beperkt tot een exclusieve rol voor of uitsluiting van een huidige opdrachtnemer (SOC-dienstverlener) binnen de raamovereenkomst. De volgende situaties zijn denkbaar:
1. Aanpalende dienst is verbonden met een geleverde SOC-dienst en volgt daarom de betreffende SOC-dienstverlener;
2. Aanpalende dienst is verbonden met een geleverde SOC-dienst en volgt om specifieke redenen (bijv.: onafhankelijkheid) de betreffende SOC-dienstverlener niet;
3. Aanpalende dienst is verbonden met een geleverde SOC-dienst en moet c.q. kan het beste om specifieke redenen (bij een geselecteerde partij) buiten de ROK worden geplaatst;

Zonder de hierboven geschetste verbondenheid zal een deelnemer de opdracht voor Aanpalende diensten in mededinging bij alle opdrachtnemers binnen de raamovereenkomst uitzetten. Qua volume is een grove inschatting voor Aanpalende diensten rond 20% van de SOC-ramingen.

3.3.4 Overig

Aanvraagproces
Het aansluiten en het gemak daarin is essentieel bij 'Off the Shelf'-producten/diensten: hoe eenvoudiger, hoe sneller, goedkoper en kwalitatief zekerder. Het idee is dat deze voordelen kunnen worden behaald met een uniform en simpel proces waarmee de leverancier binnen zeer korte tijd een deelnemer op die dienst kan aansluiten.

De bedoeling is om diensten en dienstenpakketten als 'Off the Shelf' af te kunnen nemen. Hieraan is altijd implementatie en aansluiting (onboarding) verbonden. In dat laatste zitten variabelen per deelnemer en dienst. In de Off-the-Shelf-gedachte is het streven deze zo veel als mogelijk (en zo zinnig als mogelijk) mee te nemen in de implementatie. Bij de aanvraag is het van belang dat daarbij heldere en concrete voorwaarden kunnen worden gesteld aan zowel de dienstverlener, als de deelnemer, dat de dienstverlener de implementatie/aansluiting met een vast bedrag kan prijzen, met eventuele te verrekenen eenheden indien daarvan buiten de verantwoordelijkheid van de dienstverlener van wordt afgeweken.

Exit
Na het eenvoudig en snel aansluiten is uiteraard ook de eenvoud en snelheid van eindigen of overgaan naar een opvolgende dienstverlener een belangrijk aspect van de verbintenis, waaronder overdracht van data c.a.. Bij het beëindigen van de overeenkomst draagt opdrachtnemer alle relevante gegevens die zijn verzameld en/of ontwikkeld tijdens diens inzet over aan de opdrachtgever. De overdracht van gegevens vindt plaats in een gestructureerde, gangbare en machine-leesbare vorm. Na deze overdracht worden alle gegevens vernietigd met uitzondering van gegevens waarvoor een wettelijke grondslag bestaat om deze te bewaren.

E5-Licenties
Diverse deelnemers beschikken over Microsoft E5 licenties. Deze omvatten componenten die voor monitoring en detectie ingezet kunnen worden (o.a. identiteits- en toegangsbeheer, XDR, preventieve eindpuntbeveiliging, monitoring gegevens overdrachten, identiteitsbescherming,…). Dit kan bij deze deelnemers leiden tot een voordeel voor dienstverleners die met Microsoft-oplossingen werken.

Prijs
De bedoeling is om diensten en dienstenpakketten als 'Off the Shelf' af te kunnen nemen. Hieraan is altijd implementatie en aansluiting verbonden (eventuele implementatiekosten kunnen op basis van een éénmalig implementatietarief worden verrekend).

Gedachten gaan nu uit richting een maandtarief per asset en/of per account waarop de M&D-diensten geleverd wordt.

Voor het startpakket zijn geen prijsmodellen gewenst die primair afhankelijk zijn van niet goed voorspelbare dan wel meetbare variabelen.

De prijsmodellen voor aanvullende diensten kunnen mogelijk wel afwijken van bovengenoemd tariefmodel voor het startpakket.

Voorts is het belangrijk dat snel op- en afgeschaald kan worden naar organisatiegrootte en de gehanteerde prijsmodellen hierin voorspelbaar en beheersbaar zijn. Dit met name voor tijdelijke en vraag-gestuurde organisaties. Per uit te voeren regelingen kunnen omstandigheden gedurende de looptijd danig fluctueren. Voor implementatie en aansluiting zijn éénmalige implementatie (lump sum) en éénmalige aansluitkosten (per asset) gehanteerd.

Raamovereenkomst en aantal opdrachtnemers
In de keuze voor het aantal opdrachtnemers in een raamovereenkomst moet een afweging worden gemaakt tussen enerzijds de eenmalige en periodieke kosten van deelnemers en opdrachtnemers (voor de aanbesteding en minicompetities, accountmanagement, etc.) en anderzijds de terugverdienmogelijkheden voor opdrachtnemers (afhankelijk van de kans op gunning van opdrachten) en baten voor de deelnemers als gevolg van gezonde mededinging binnen een raamovereenkomst. Dit zou kunnen leiden tot een ongeveer 4-6 opdrachtnemers binnen een raamovereenkomst.
Daarnaast: wat is het absorptievermogen van opdrachtnemers: hoeveel deelnemers kan men voor een dienst binnen een periode op SOC-diensten aansluiten of kan men in totaal goed bedienen? Hoeveel opdrachtnemers zijn er

nodig om het potentieel van deelnemers aan te sluiten en te bedienen? Dit is primair een vraag aan de markt.

Threat Intelligence
Deelnemers mogen onder voorwaarden gebruikmaken van een zogenaamde CTI-feed die door het Nationaal Cyber Security Centrum beschikbaar wordt gesteld. Deze CTI-feed bevat operationele CTI-informatie, de zogenaamde Indicators of Compromise. De NCSC-feed wordt geleverd per individuele overheidsorganisatie. Opdrachtnemers binnen de raamovereenkomst kunnen onder de aansluitvoorwaarden van NCSC de CTI-feed van deelnemers krijgen, waarvoor zij opdrachten uitvoeren.

AI
Ook binnen SOC-systemen/tooling wordt steeds meer en op diverse manieren gebruik gemaakt van AI-toepassingen, van zoeken tot en met analyse, triage en meldingen (inclusief eventuele oplossingsrichtingen, SOAR). Dit werpt de vragen op als:
- in hoeverre een opdrachtgever c.q. deelnemer met deze dienstverlening daarmee (ook) gebruikt maakt van AI en welke verantwoordelijkheden dat wel of niet met zich brengt,
- hoe dit de verdeling van verantwoordelijkheid tussen opdrachtnemer en opdrachtgever raakt of kan raken,
- hoe de opdrachtgever omgaat met de mogelijkheid dat gevoelige data in AI-systemen belandt als trainingsdata en op welke manier door wie wordt gegarandeerd dat er op geen enkele wijze data voor andere doeleinden wordt gebruikt dan expliciet overeengekomen (dus geen impliciete toestemming, gebruik of het achteraf inroepen van 'fair use'),
- hoe de opdrachtgever omgaat met de mogelijkheid dat gevoelige data in AI-systemen belandt en de geografische locatie waar diens verwerkingen plaatsvinden met het oog op internationale afspraken en beschermingsniveau en toegang voor statelijk actoren en op welke manier door wie wordt gegarandeerd dat mogelijk hieruit voortvloeiende risico's afdoende en op transparante wijze zijn gemitigeerd,
- hoe de opdrachtgever omgaat met de mogelijkheid dat gevoelige data in AI-systemen belandt in relatie tot het in control zijn met betrekking tot vertrouwelijkheid en rubricering van te beschermen belangen.

S1	Is de duiding van type M&D/KS&R-diensten herkenbaar en sluit deze aan op door u te leveren producten? Zijn er ontbrekende diensten?
Antwoord	
S2	Kunt u dienstverlening bieden volgens de opzet van M&D-diensten met daarin een Startpakket en aanvullende diensten en ziet u dit ook als handzame opzet voor organisaties om snel met een SOC te kunnen beginnen met mogelijkheden tot groei? Dit ook ten aanzien van het eenmalig in minicompetitie komen in de context van een raamovereenkomst.
Antwoord	

S3	Wat zijn de meest belangrijke KPI's waarmee de prestaties van M&D en KS&R dienstverlening zijn te meten en aan te tonen?
Antwoord	
S4	Kunt u zich met betrekking tot de gevraagde M&D en KS&R dienstverlening onderscheiden van andere marktpartijen. Zo ja, op welke punten onderscheidt u zich en hoe zijn deze punten meetbaar of aantoonbaar?
Antwoord	
S5	Met betrekking tot het aanvraagproces en het aansluiten van ICT-assets: - Hoe snel en eenvoudig is het aanvragen en aansluiten van het Startpakket voor M&D-diensten? - Welk type informatie heeft u daarvoor nodig van een deelnemer? - Welke inspanningen moet een deelnemer zelf uitvoeren? - Wat zijn overige randvoorwaarden?
Antwoord	
S6	Wat is naar uw inzicht een reëel te verwachten en voor u acceptabele periode van af-/aansluiten waarop een deelnemer kan beslissen tot afname, dan wel van een opdrachtnemer afscheid te nemen? Welke randvoorwaarden zijn hier aan de orde?
Antwoord	
S7	In geval van opvolging van een voorgaande SOC-dienstverlener: maakt dit uw antwoord op S6 anders? Zo ja, hoe?
Antwoord	
S8	Welke (minimale) looptijd van nadere overeenkomsten adviseert u? U kunt hierbij desgewenst onderscheid maken tussen de verschillende diensten die afgenomen kunnen worden binnen de raamovereenkomst. Houd rekening met verschillende implementatietijden, terugverdientijden, exit-/retransitietijden etc. De looptijd van een nadere overeenkomst mag de looptijd van de raamovereenkomst overschrijden. Oftewel als de raamovereenkomst is geëxpireerd, mogen al aangegane Nadere overeenkomsten nog voortduren voor de looptijd (inclusief eventuele opties tot verlenging) die bij aanvang is bepaald.
Antwoord	
S9	Zijn er mogelijkheden – en zo ja welke – om naast de eerstelijns ondersteuning van opdrachtgever en eventuele specialisten ook één of enkele medewerkers van deelnemer in deze rollen te laten meewerken en zo een hybride situatie in te richten?

Antwoord	
S10	Gelden bovenstaande antwoorden voor het Startpakket ook voor de aanvullende M&D-diensten of spelen daar andere aandachtpunten of verschillen?
Antwoord	
S11	Zijn er mogelijkheden of beperkingen of bijzonderheden met betrekking tot het monitoren van Clouddiensten waar in het kader van SOC-diensten rekening mee moet worden gehouden? Zo ja, welke?
Antwoord	
S12	Zijn er mogelijkheden/aandachtspunten met betrekking tot een koppeling met het ticketsystem van een opdrachtgever?
Antwoord	
S13	Welke mogelijkheden biedt u als opdrachtnemer om deelnemers via een uniform dashboard/interface visueel inzicht te geven in loginformatie en events? Het is van belang dat deelnemers alleen de eigen informatie zien en geen inzicht krijgen in informatie van andere deelnemers.
Antwoord	
S14	Zijn er mogelijkheden dat medewerkers van deelnemende diensten ook toegang krijgen tot monitoringsystemen (b.v. SIEM) van opdrachtnemer om zo zelf zaken in te zien en queries te doen? Zo ja, beschrijf op hoofdlijnen welke functionaliteiten toegankelijk zijn.
Antwoord	
S15	Een aantal deelnemende diensten beschikken reeds over Microsoft E5 licenties. Welk effect van deelnemers met Microsoft E5-licenties ziet u op uw dienstverlening, zowel qua verantwoordelijkheden als in de prijsstelling?
Antwoord	
S16	Het ligt in de lijn der verwachting dat de kwaliteit van de dienstverlening toeneemt naarmate een marktpartij gedurende langere tijd diensten levert aan een deelnemer, doordat er ervaring wordt opgebouwd. Onderschrijft u dit beeld? Op welke onderdelen is deze kwaliteitsverbetering volgens u zichtbaar en meetbaar?
Antwoord	
S17	Bij inschrijving op de aanbesteding zullen prijscomponenten opgenomen worden die bepalend zijn op het niveau van de raamovereenkomst (ROK). Deze zullen gelden voor alle nadere offertes (en daarmee nadere overeenkomsten/NOKs) van deze inschrijver binnen de raamovereenkomst. Op basis van welke

	eenheden per dienst kan een beheersbare prijs worden bepaald? Het gaat om prijscomponenten waaruit een prijs wordt opgebouwd en wat de 'drivers' zijn die de prijs kunnen of zullen doen stijgen of dalen. Het doel is te komen tot en veralgemeniseerd prijsmodel waarin diverse inschrijvers kunnen worden vergeleken.
Antwoord	
S18	Heeft u een beeld bij het aantal klanten c.q. welke omvang u kan bedienen om de dienstverlening per klant met zekerheid en op kwalitatief niveau te leveren waarop de klant kan vertrouwen? Dit met name in gevallen van incidenten die (nagenoeg) gelijktijdig meerdere klanten raken of kunnen raken.
Antwoord	
S19	Wat acht u een zinvol aantal opdrachtnemers bij deze Raamovereenkomst en waarom? U kunt denken aan aspecten als transactiekosten, transitiekosten (in/exit); concurrentie versus de kans op een opdracht per mini-competitie, etc. …
Antwoord	
S20	Deelnemers mogen gebruikmaken van een zogenaamde CTI-feed die door het Nationaal Cyber Security Centrum (NCSC) beschikbaar wordt gesteld. Deze CTI-feed bevat zogenaamde Indicators of Compromise. Zijn partijen in staat en bereid om: • deze CTI-feed op te nemen in de Montoring en Detectiesystemen die voor deze dienstverlening worden ingezet? • Alerteringen (sightings) die door deze CTI-feed ontstaan te delen met Opdrachtgever of een door Opdrachtgever aangewezen partij? NB: het NCSC bepaalt welke partijen van deze feed gebruik mogen maken. De implementatie bij opdrachtnemer moet zodanig zijn dat men zich aan de aansluitvoorwaarden van het NCSC houdt.
Antwoord	
S21	In hoeverre speelt AI een rol in uw dienstverlening?
Antwoord	
S22	Welke impact verwacht u van de eisen die voortvloeien uit de invoering van de EU AI-verordening en verwacht u dat u hieraan kunt voldoen?
Antwoord	
S23	Heeft u een visie of activiteiten op het gebied van Quantum Veilige Cryptografie en welk effect dit op (de kwaliteit van) uw dienstverlening heeft? U hoeft geen uitgebreide visie op dit

	onderwerp zelf te geven. U kunt zich beperken tot highlights en relevante punten voor inbedding in een aanbesteding.
Antwoord	
S24	Ingeval een deelnemer van een eigen SOC gebruik maakt en ook SOC-diensten binnen de raamovereenkomst wenst af te nemen, ontstaat er een hybride samenwerkvorm met een opdrachtnemer. Welke randvoorwaarden of aandachtspunten zou u hierbij willen meegeven, naast het logischerwijs goed afbakenen van de verantwoordelijkheden en bevoegdheden?
Antwoord	
S25	In hoeverre is het dienstverleningsconcept (met het startpakket en aanvullende diensten verenigbaar) met een hybride SOC-variant waarin de deelnemende dienst zelf tijdens kantoortijden voorziet in M&D dienstverlening en de leverancier zorgt voor de bewaking daarbuiten. Is een dergelijk model hanteerbaar en welke specifieke aandachtspunten en randvoorwaarden stelt dit?
Antwoord	
S26	In hoeverre is het dienstverleningsconcept (met het startpakket en aanvullende diensten) verenigbaar met een hybride SOC-variant waarin de deelnemende dienst bepaalde M&D-diensten afneemt van een rijksinterne dienstverlener (SSC of anderszins) en de leverancier zorgdraagt voor additionele diensten en/of verhoging van de dekkingsgraad. Is een dergelijk model hanteerbaar en welke specifieke aandachtspunten en randvoorwaarden stelt dit?
Antwoord	
S27	Zijn er voor deelnemers nog niet benoemde randvoorwaarden van belang bij de afname van deze diensten, zoals een relatie met de (eigen en/of externe) SOC die monitoring- en detectiediensten uitvoert?
Antwoord	
S28	In bijlage 4 bij dit document treft u een conceptversie van het programma van eisen aan. Wat vindt u van de voorliggende conceptversie van het programma van eisen? Bij uw beantwoording gaat u bij voorkeur in op de volgende subvragen: a. Welke eisen moeten naar uw mening vervallen of afgezwakt worden om te voorkomen dat u en/of andere potentiële inschrijvers hier niet aan kunnen/willen voldoen (verlagen instapniveau)? Motiveer uw antwoord. b. Welke eisen moeten naar uw mening nog toegevoegd of strikter gesteld worden om risico's voor Deelnemers

	te beperken/minimaliseren (verhogen instapniveau)? Motiveer uw antwoord. Welke andere suggesties wilt u doorgeven?
Antwoord	
S29	Hieronder is ruimte voor uw eventuele aanvullende reactie.
Reactie	

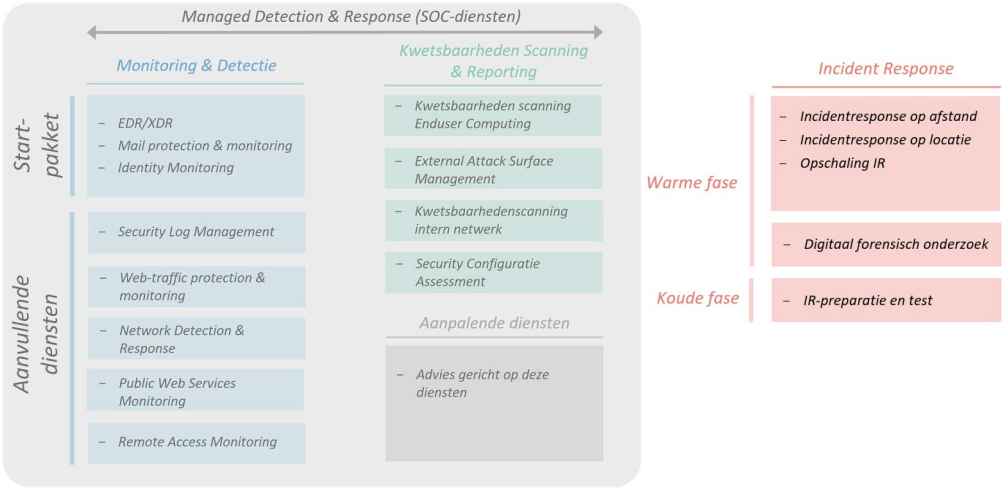
3.4 Overige IB-diensten

Raming jaar 1 t/m 4
€ 20.000.000

In de volgende (sub)paragrafen treft u verschillende onderwerpen aan die gerelateerd zijn aan het domein van informatiebeveiliging (IB) en vooralsnog bewust geen onderdeel zijn van de dienstverlening die binnen de andere raamovereenkomsten is beoogd. Gemakshalve wordt het samenstel van deze diensten 'Overige IB-diensten' genoemd, zonder daarbij impliciet een weging of oordeel te willen geven van het belang van deze afzonderlijke diensten. De behoefte van de deelnemers aan de (gecoördineerde/gezamenlijke) inkoop van deze Overige IB-diensten is op het moment van deze marktraadpleging nog met veel onzekerheden omkleed. Het is daarom nog onzeker of het sluiten van een raamovereenkomst voor (alle) overige IB-diensten, het sluiten van afzonderlijke (raam)overeenkomsten voor een of meer van de verschillende onderwerpen, dan wel het niet gecoördineerd/gezamenlijk inkopen (maar per deelnemer een eigen inkooptraject) van deze Overige IB-diensten een wenselijke route is.

OIB1	Op welke verschillende onderwerpen (zoals genoemd in de subparagrafen) van de Overige IB-diensten kunt en wilt u wel/geen diensten leveren?
Antwoord	
OIB2	Wat is uw advies over het wel of niet als geclusterd geheel aanbesteden van de Overige IB-diensten? Welke onderwerpen zouden beter niet/wel geclusterd kunnen worden aanbesteed c.q. opgenomen in dezelfde (raam)overeenkomst? Waarom?
Antwoord	
OIB3	Hieronder is ruimte voor uw eventuele aanvullende reactie ten aanzien van de mogelijke clustering van inkoopbehoeftes op het gebied van de 'overige IB-diensten'
Reactie	

3.4.1 Incident response



Incident Response (IR) is nauw verbonden met de M&D diensten zoals deze bij de SOC-diensten zijn omschreven. Daar waar de SOC-diensten primair gaan over het zien en melden aan een deelnemer, gaat IR over wat de deelnemer met de melding doet. IR is daarom geen onderdeel van de scope van SOC-diensten en hier separaat ondergebracht in het RVICTO-deel "Overige IB-diensten".

Organisaties die ICT-systemen in gebruik hebben, beschikken in vrijwel alle gevallen over reguliere processen voor incidentmanagement. Deze reguliere processen zijn in de praktijk sterk gericht is op het oplossen van storingsmeldingen van gebruikers en niet altijd voldoende toegespitst op incidentmanagement & response voor beveiligingsincidenten.

Er zijn een aantal belangrijke verschillen tussen regulier incidentmanagement en incidentmanagement & -response in de context van informatiebeveiliging. In het laatste geval is veel meer focus is op inperkende maatregelen (containment), het hebben van draaiboeken (playbook), de relatie met crisismanagement en het uitvoeren van testen. Daarnaast wordt bij (grote) beveiligingsincidenten vaak verwacht c.q. geëist dat er bewijsmateriaal beschikbaar komt die gebruikt kan worden in rechtszaken, het zogenaamde forensisch onderzoek.

Voor onder andere onderdelen van het Rijk wordt bij cyberincidenten hulp verleend door NCSC als sectoraal Computer Security Incident Response Team (CSIRT). Het NCSC ondersteunt, maar vervang geen reguliere cyberbeveiligingsdiensten. Mitigerende maatregelen om het incident te verhelpen moet een Deelnemer, eventueel in samenwerking met een Incident Response partij, zelf treffen (zie de NCSC-factsheet "Ondersteuning bij Cyberincidenten").

Activiteiten in het kader van Incident Response kunnen geheel of gedeeltelijk worden uitbesteed. Grofweg kan als typen IR-diensten worden onderscheiden:

3.4.1-a. Incident response op afstand: Om onverwachte situaties te allen tijde op te kunnen vangen, stelt Opdrachtnemer een 24x7 dienst beschikbaar waarbij

een Deelnemer via een noodhulplijn altijd contact op kan nemen voor eerste hulp bij incidenten. Van Deelnemer wordt verwacht dat een eerste triage wordt uitgevoerd om snel en efficiënt vast te stellen wat de omvang en potentiële impact van het incident is. Op basis hiervan wordt in overleg vastgesteld wat de beste vervolgstappen zijn. Waar nodig kan Opdrachtnemer ondersteuning op afstand blijven bieden gedurende de looptijd van het incident

3.4.1-b. Incident response op locatie: Op basis van de eerste triage kan worden vastgesteld dat Deelnemer ondersteuning op locatie wenst. Opdrachtnemer faciliteert incident response op locatie en kan hierbij binnen korte tijd op locatie binnen Nederland aanwezig zijn. Op locatie geeft Opdrachtnemer op basis van de wens van Deelnemer ondersteuning of leiding aan het onderzoeken en oplossen van incidenten. Waar nodig is Opdrachtnemer 24x7 beschikbaar tot het eind van het incident.

3.4.1-c. Opschaling Incident Response: Opdrachtnemer staat als ondersteunende partij (IR-partij)klaar als een incident groter wordt dan gebruikelijk. Bijvoorbeeld een grote ransomware-aanval, met grote impact voor een Deelnemer, die hij met eigen personeel niet kan oplossen. Een Opdrachtnemer staat dan klaar om deze Deelnemer te helpen, mogelijk op locatie. Dit betekent dat deze Opdrachtnemer altijd klaar moet staan en snel ter plekke moet kunnen zijn.
Betaling voor een dergelijke IR-dienst kan op basis van nacalculatie, met een vast tarief per maand of een mix van deze opties.

3.4.1-d. IR-preparatie en test: Opdrachtnemer organiseert en/of ondersteunt bij het opstellen/prepareren van, het testen en oefenen van incidentresponseplannen, -processen en -procedures. Met deze testen en oefenen gaat het erover dat Opdrachtnemer en Deelnemer oefeningen uitvoeren, bijvoorbeeld tabletops, waarbij er scenario's worden nagespeeld en wordt bekeken of de processen en procedures die zijn ingericht werken zoals ze bedoeld zijn. Het gaat dus niet zozeer over het testen van de beveiliging van informatiesystemen zelf, maar meer testen of de procedures die specifiek voor incidentmanagement en -response zijn ingericht ook werken zoals beoogd.

<u>Voorbeelden van diensten</u>:

- Uitvoeren van een assessment om te controleren of de processen voldoen aan BIO, NIS2/Cbw en eventuele andere van toepassing zijnde normen.
- Ondersteuning bij de inrichting van incidentmanagement & -response in de context van informatiebeveiliging en conform de Baseline Informatiebeveiliging Overheid (BIO), NIS2/Cbw en eventuele andere eisen en normen die voor een organisatie van toepassing zijn. Denk hierbij aan:
    - Ondersteuning bij het opstellen en/of evalueren van beleidsregels voor incident response;
    - Opstellen en/of evalueren van normenkader voor de classificatie van beveiligingsincidenten;
    - Inrichten c.q. optimaliseren en documenteren van het incidentresponseprocedures, inclusief beschrijving van escalatieprocedures en (aanbevelingen voor het) aanstellen van proceseigenaren die verantwoordelijk zijn voor incidentresponse;
    - Inrichten en documenteren van taken, bevoegdheden en verantwoordelijkheden binnen het incidentresponseproces.

- Opstellen van responseplannen, bijvoorbeeld voor Ransomware, Datalekken, supply chain aanvallen, zero day kwetsbaarheden en DDoS.
- Communicatieproces inrichten waarmee voldaan wordt aan communicatieverplichtingen zoals het aantoonbaar maken dat medewerkers, aannemers, dienstverleners en andere belanghebbende op de hoogte zijn van de meldprocedure voor informatiebeveiligingsincidenten;
- Borgen dat processen en procedures van incidentmanagement en -response aansluiten op het bedrijfscontinuïteitsplan.
- Inrichten van processen die nodig zijn om aan de meldplicht te voldoen.
- Het inrichten van rapportageprocessen over de opvolging van beveiligingsincidenten;
- Het inrichten van processen en procedures om van beveiligingsincidenten bewijsmateriaal te identificeren, verkrijgen, verzamelen en bewaren;
- Processen en procedures inrichten voor het evalueren van beveiligingsincidenten en het delen van informatie met andere belanghebbende en zorgen dat er lering getrokken wordt uit eerdere informatiebeveiligingsincidenten.

- Opstellen van draaiboeken (playbooks) voor de (belangrijkste) beveiligingsincidenten.
- Het organiseren en/of ondersteunen bij het testen en oefenen van incidentresponseplannen, -processen en -procedures.
- Operationele ondersteuning bij informatiebeveiligingsincidenten. Op het moment dat er een (grootschalig) beveiligingsincident plaatsvindt, is een organisatie mogelijk niet altijd in staat om zelf adequaat response uit te voeren. Dit omdat er specialistische kennis nodig is om snel en adequaat de gevolgen van het incident te beperken, bewijsmateriaal te verzamelen en om met zo beperkt mogelijke gevolgen tot systeemherstel over te gaan.

IR1	Herkent u bovenstaande indeling in uw producten/diensten portfolio? a) Zijn de diensten bij u als zodanig georganiseerd/ingericht, dan wel andere samenstellingen of dwarsverbanden? b) Wat kunt u meegeven als belangrijke zaken met betrekking tot verantwoordelijkheden en activiteiten binnen een ter zake contract?
Antwoord	
IR2	Moeten we (en zo ja: hoe?) prijstechnisch rekening houden in het onderscheid in prijsmodel en prijsstelling van zaken die met of zonder spoed (Golden Hour) moeten worden opgepakt? a) Als dat onderscheid er is: welke typen zijn daarin en hoe kan hiermee effectief/efficiënt worden omgegaan? b) Is er een generieke kwalificatie waarin u breed in de markt niveaus van dienstverlening herkent? (e.g. Gold/Silver/Bronze, anders…) c) Welke classificaties van reactie-/responstijden of andere 'levertijden' zijn bepalend voor het kunnen leveren van de diensten en wat is het effect van deze classificatie op de prijsstelling? Maak eventueel onderscheid naar verschillende diensten en geeft eventuele randvoorwaarden aan in de samenwerking met een Deelnemer.
Antwoord	
IR3	Welk prijsmodel acht u het meest passend voor deze vormen van dienstverlening, dienstig aan te leveren kwaliteit en besteding van algemene middelen (belastinggeld).

Antwoord	
IR4	Om te bepalen hoeveel Opdrachtnemers bij een raamovereenkomst te kiezen, speelt de vraag hoeveel klanten een Opdrachtnemer 24x7 kan bewaken en hoeveel in 'real time' gelijktijdig bij incidenten kunnen worden ondersteund. In dat kader wordt gevraagd naar uw mogelijke ervaring of uw beelden bij dit vraagstuk, met name bij vragen als : 1. Zijn objectieve gegevens te bepalen die deze verhouding kunnen uitdrukken, zodanig dat deze over diverse opdrachtnemers als benchmark kunnen worden gelezen? 2. Hoe bepaalt u deze verhouding als beheersbaar? 3. Hoe beheert/ondervangt u ter zake risico's?
Antwoord	
IR5	Kunt u de geschetste dienstverlening voor operationele incident response (IR 3.4.1 a t/m c) uitvoeren ingeval een andere leverancier zorgdraagt voor monitoring en detectie? Welke specifieke aandachtspunten ziet u hierbij?
Antwoord	
IR6	Hieronder is ruimte voor uw eventuele aanvullende reactie.
Reactie	

3.4.2 (Cyber) Threat Intelligence

Hier gaat het om verzamelde, verrijkte en geanalyseerde informatie over dreigingen in het digitale domein, die als doel heeft deze dreigingen tijdig te identificeren en de weerbaarheid van de ontvangers te verhogen. De relevante TI-collectie zal per organisatie verschillen en zal afstemming vergen. In beginsel wordt hierin geen onderscheid gemaakt in OSINT, SIGINT of HUMINT. Als dit naar uw mening wel tot relevant onderscheid lijdt in de aanbesteding, dan horen we dat graag.

TI1	Is bovenstaande opsomming dekkend voor de type TI-dienstverlening of zijn er varianten die hierboven niet zijn benoemd, maar wel in het kader van de beoogde raamovereenkomsten relevant zijn?
Antwoord	
TI2	Wat is naar uw beeld de beste strategie van het plaatsen van TI-dienstverlening en scopeafbakening? Als apart aan te besteden raamovereenkomst of als onderdeel van een ander RVICTO-onderdeel? Zie in dit licht ook onderstaande vragen met betrekking tot zinvolle clustering of separatie van diensten.
Antwoord	
TI3	Ziet u de genoemde TI-diensten als logische verzameling die elke TI-dienstverlener standaard kan bieden, of betreffen het (ook) specifieke en dusdanig afwijkende diensten die door verschillende (gespecialiseerde) partijen wordt geleverd?
Antwoord	

TI4	Hieronder is ruimte voor uw eventuele aanvullende reactie.
Reactie	

3.4.2-a. Datafeed ten behoeve van een SOC: Voor Deelnemers die RVICTO SOC-Monitoring & Detectie diensten afnemen (zie hierboven 3.3. SOC-diensten), zal er een CTI-feed vanuit NCSC beschikbaar zijn. Deze is buiten scope van het onderhavige deel "Overige IB diensten". Deelnemers of opdrachtnemers kunnen onverminderd besluiten aanvullende feeds te gebruiken.
Hoofdlijn: het SOC (intern of extern) gebruikt als basis de CTI-feed(s) die door het NCSC beschikbaar wordt gesteld, voldoet aan de aansluitvoorwaarden hiervoor en kan aanvullend eigen feeds gebruiken als verrijking. Een Deelnemer kan besluiten om voor zijn SOC een aanvullende CTI-(data)feeds in te kopen. Dat kan aan de orde zijn als de aanvullende CTI-feed beter aansluit op specifieke dreigingen die (het SOC van) deze Deelnemer (voor)ziet en/of het SOC nieuwe capaciteit/mogelijkheid ziet om deze aanvullende CTI-feed met dreigingen met hun kennis en kunde te analyseren en verwerken in hun SOC-dienstverlening. De volwassenheid van een SOC speelt hierin dus ook een rol.

DF1	Welke CTI-datafeeds voor een SOC onderscheidt u en kunt u leveren? Beschrijf hierbij kort waar deze feeds in voorzien, hoe de data is verzameld (bronnen) en de integriteit (betrouwbaarheid, juistheid, volledigheid) is geborgd.
Antwoord	
DF2	Welke randvoorwaarden stelt u aan de Deelnemers bij het eventuele gebruik van deze CTI-datafeeds? Welke aandachtspunten of adviezen wilt u deze Deelnemers meegeven?
Antwoord	
DF3	Welk prijsmodel hanteert u bij deze CTI-datafeeds? Wat zijn belangrijke kostendrivers (factoren die de hoogte van de prijs voor de Deelnemer bepalen)?
Antwoord	
DF4	Hieronder is ruimte voor eventuele aanvullende reactie.
Reactie	

3.4.2-b. Dreigingsbeeld voor een Pentest:

DP1	Hier is geen vraag. U kunt onverminderd onderstaand desgewenst uw eventuele reactie geven.
Reactie	

***3.4.2-c. Dreigingsbeeld voor Red Teaming*:** Iedere ART/TIBER-test heeft de inschakeling van en TI-team. De samenstelling van het team verschilt naar gelang de scope et cetera. De TI-provider schrijft de scenario's voor een Red Teaming test. Deze kan onderdeel zijn van en RT-opdracht, maar ook kan worden gekozen de TI-provider los van de RT-provider te betrekken. Voor een profiel van de TI-provider voor ART of Tiber, zie o.a. de Praktische Inkooprichtlijnen voor Red-teaming testen. Het volume volgt 3.1 hierboven. Dat brengt een raming jaar 1 t/m 4 voor scenario's voor circa 48 Red Teaming testen volgens ART/TIBER.

DR1	De voornoemde Praktische Inkooprichtlijnen voor Red-teaming testen verwijzen naar kwaliteitseigenschappen van zowel de TI-provider, de TI-manager en het TI-team. Dit gelezen hebbende: welke minimumeisen (ja/nee) en subgunningscriteria kunnen naar uw mening het beste worden ingezet in de keuze van een partner voor de raamovereenkomst en wat resteert daarna aan onderscheidend vermogen voor gunning van een Nadere overeenkomst?
Antwoord	
DR2	Welke vormen van dreigingsbeelden voor Red Teaming test onderscheidt u en kunt u leveren? Beschrijf hierbij kort waar deze dreigingsbeelden in voorzien, hoe de data is verzameld (bronnen), de beelden tot stand komen (analyse) en de integriteit (betrouwbaarheid, juistheid, volledigheid) is geborgd.
Antwoord	
DR3	Welke randvoorwaarden stelt u aan de Deelnemers en de Red Teaming Provider (RTP) bij de aanvraag en het gebruik van deze dreigingsbeelden? Welke aandachtspunten of adviezen wilt u meegeven?
Antwoord	
DR4	Welk prijsmodel hanteert u bij deze dreigingsbeelden voor Red Teaming? Wat zijn belangrijke kostendrivers (factoren die de hoogte van de prijs voor de Deelnemer bepalen)?
Antwoord	
DR5	Hieronder is ruimte voor uw eventuele aanvullende reactie.
Reactie	

3.4.2-d. Generieke/specifieke dreigingsbeelden: Dit betreffen informatiebronnen van TI, anders dan scenario's of datafeeds als in dit deel bedoeld. Dit kunnen algemene en specifieke informatiebronnen zijn, die ofwel met abonnementen of andere periodieke afspraken worden betrokken, dan wel per specifieke informatievraag.

DB1	Heeft u in uw dienstportfolio van informatiediensten het genereren en onderhouden van generieke en (organisatie-) specifieke dreigingsbeelden? Zo ja:

	a) Hoe kunnen die onderscheidenlijk als in de markt breed herkenbare c.q. erkende af te nemen producten worden getypeerd/omschreven? b) Is het beroep op die informatiedienst periodiek, ad hoc? c) Zijn er aanpalende (advies-)diensten verbonden, maar separaat van de informatiediensten? d) Is er een zinvolle clustering of separatie van informatiedienst zoals u die heeft omschreven en waarom?
Antwoord	
DB2	Welk prijsmodel acht u het meest passend voor deze dienstverlening dienstig aan te leveren kwaliteit en besteding van algemene middelen (belastinggeld).
Antwoord	
DB3	Hieronder is ruimte voor uw eventuele aanvullende reactie.
Reactie	

3.4.2-e. TI-onderzoeken: Naast reguliere bestaande TI-collecties is er ook het actief zoeken wat rond een organisatie op het internet te vinden is en of daar aandachtpunten zijn. Bijvoorbeeld: filtering op dark web monitoring, private message groups en TI-feed waarbij een organisatie specifiek wordt genoemd.

TO1	Heeft u in uw dienstportfolio van informatiediensten TI-onderzoeken? Zo ja: a) Hoe kunnen verschillende TI-onderzoeken onderscheidenlijk als in de markt breed herkenbare c.q. erkende af te nemen producten worden getypeerd/omschreven? b) Is het beroep op die informatiedienst periodiek, ad hoc? c) Zijn er aanpalende (advies-)diensten verbonden, maar separaat van de TI-onderzoeken? d) Is er een zinvolle clustering of separatie van informatiedienst zoals u die heeft omschreven en waarom? Indien relevant kunt u ook de relatie leggen met hieronder 3.3.2-d.
Antwoord	
TO2	Welk prijsmodel acht u het meest passend voor deze dienstverlening dienstig aan te leveren kwaliteit en besteding van algemene middelen (belastinggeld).
Antwoord	
TO3	Hieronder is ruimte voor uw eventuele aanvullende reactie.
Reactie	

3.4.3 (Social) Awareness

Eindgebruikers zijn een primaire kwetsbaarheid binnen een netwerk. Het is belangrijk om naast technische middelen ook eindgebruikers c.q. werknemers bewust te maken van veelvoorkomende bedreigingen en hen te trainen hoe ze deze kunnen vermijden of beperken. Hier gaat het om wat en hoeveel eindgebruikers weten over de cyberveiligheid en hoe hun gedrag risico's kunnen beperken of juist vergroten.

Een programma voor eindgebruikers kan bestaan uit een combinatie van meerdere benaderingen:

	BEWUSTZIJN	**TRAINING**	**ONDERWIJS**
Attribuut	"Wat"	"Hoe"	"Waarom"
Niveau	Informatie	Kennis	Inzicht
Doel	Erkenning	Vaardigheid	Begrip
Overdracht via	Media. *(o.a. video, posters, nieuwsbrieven)*	Praktische instructie/oefening. *(o.a. lezing, casestudy-workshop, hands-on)*	Theoretisch onderricht *(o.a. discussieseminar, achtergrondinformatie)*
Effect op	Korte termijn	Middellange termijn	Lange termijn

<u>Bedreigingen in casu</u>
Indringers zoeken meestal naar de gemakkelijkste manier om toegang te krijgen tot een netwerk en dat is vaak het menselijke element:

- Ze benaderen voor hun aanval relevante personen via Social engineering = iemand overtuigen om gevoelige informatie zoals gebruikersnamen en wachtwoorden te geven. Populaire vormen zijn: Scareware, Phishing, Spear phishing, Vishing, Smishing, Tailgating, Piggybacking. Als men via social engineering (al is het maar kort) toegang heeft gekregen, kan kwaadaardige software (Malware) worden geplaatst (o.a. virussen, Trojaanse paarden, wormen, rootkits, spyware, ransomware etc. …).
- Naast Social engineering kan die toegang ook verkregen worden via verwijderbare media (e.q. USB-sticks) of het anderszins verkrijgen of kraken van wachtwoorden, of het 'kapen' van wifi en/of bluetooth verbindingen van met elkaar communicerende apparaten (IoT).
- Bedreigingen kunnen ook binnen een systeem of organisatie zijn, zoals vanuit werknemers of opdrachtnemers die toegang hebben tot de systemen en gegevens van de organisatie met alle risico's van dien (e.g. gegevensdiefstal, sabotage, fraude of spionage).

Met onderwijs en bewustmakingstrainingen kunnen eindgebruikers beter in staat worden gesteld zich te verdedigen tegen cyberdreigingen. Bewust maken, training en onderwijs zijn continuprocessen.

<u>Programmatische benadering</u>
Uitgangspunt van benadering(en) is dat organisaties

1. een nulmeting willen doen (kwetsbaarheden aan de menselijke kant),

2. daar gerichte(re) interventies op nemen en
3. vervolgens daar weer de impact van willen meting (tussen- of eindmeting).

De interventies en activiteiten staan dan niet op zichzelf en zullen vooral gericht zijn op de kwetsbaarheden die uit de nulmeting komen.

Met het oog op hieruit komende wensen tot gedragsverandering kunnen die worden weergegeven in drie factoren:
Weten - wat weten men over de risico's en zijn ze zich bewust van hun/elkaars gedrag en de risico's?
Willen – wat is de motivatie waarom mensen het juiste gedrag willen vertonen?
Kunnen – wat is de gelegenheid waarin men in staat wordt gesteld het gewenste gedrag te vertonen (o.a. door bepaald door cultuur, structuren, instrumenten en processen binnen een organisatie)?
Deze perspectieven kunnen de basis zijn voor de typering van Social awareness opdrachten. Het expliciteren van deze drie perspectieven voorkomt onder meer dat de reikwijdte zich beperkt tot 'het weten', daar waar het zich ook moet richten op de aspecten van 'willen' en 'kunnen'.

De behoefte aan ondersteuning door opdrachtnemer(s) op social awareness programma's kan divers zijn en zich richten op zowel de begeleiding/uitvoering van een volledig programma met herhaalde metingen en interventies, tot alleen heel specifieke ondersteuning bij een meting, interventie/maatregel. Er kan hiernaast gekozen worden voor een generieke aanpak voor een gehele organisatie, maar ook voor een doelgroepgerichte benadering (b.v. (focus op techneuten in datacenters, anders…) of deel van een organisatie (afdeling, team, locatie).

Een andere doorsnede is bijvoorbeeld:
- Brons: voor iedere nieuwe medewerker bij binnenkomst;
- Zilver: jaarlijkse 'fresh up' voor iedere medewerker;
- Goud/Diamant: diepgaander, meer technisch en meer gericht op ontwikkelaars en specifiek techneuten/deskundigen.

Als methoden zijn middelen te gebruiken als surveys, e-learning, gaming, al blijft een belangrijk element hierin ook de menselijke factor.

SA1	In hoeverre onderscheiden type awareness-activiteiten rond informatieveiligheid en doelgroepen zich zodanig dat een bepaalde omvang clustering of separatie van awareness-activiteiten aan te raden is c.q. goed aansluit op de markt?
Antwoord	
SA2	Hoe en in hoeverre kunnen door u gebruikte manieren/methoden en/of de door u hierbij in te zetten expertise en/of in te zette hulpmiddelen bijdragen aan het onderscheidend vermogen tussen aanbieders?
Antwoord	
SA3	Zijn er anders dan manieren/methoden, elementen waarop het succes van uw activiteiten zichtbaar gemaakt kan worden? Bij voorkeur zodanig dat daarmee ook vergelijking tussen marktpartijen mogelijk is.
Antwoord	

SA4	Welke eisen zouden wij op het niveau van een raamovereenkomst moet stellen (geldend voor alle hieronder te verstrekken opdrachten)? Met welke wensen kunnen wij een zinvol onderscheid maken tussen de niveaus van dienstverlening van aanbieders?
Antwoord	
SA5	Welk prijsmodel acht u het meest passend voor deze dienstverlening dienstig aan te leveren kwaliteit en besteding van algemene middelen (belastinggeld) en hoe beïnvloedt dit de vorige vraag V1?
Antwoord	
SA6	Hieronder is ruimte voor uw eventuele aanvullende reactie.
Reactie	

3.4.4 (Digitaal) Forensisch Onderzoek

In specifieke gevallen kan het nodig zijn diepgaand digitaal sporenonderzoek uit te voeren met als doel het verzamelen van juridisch houdbaar bewijsmateriaal. Opdrachtnemer is in staat om op forensische wijze digitale sporen en gegevens te verzamelen. Op basis van deze informatie kunnen gebeurtenissen worden gereconstrueerd. Digitale sporen worden op correcte forensische wijze veiliggesteld en geanalyseerd. De bevindingen worden in een heldere rapportage vastgelegd waarbij de rapportage geschikt is voor gebruiken als bewijsmateriaal in de rechtbank mocht opdrachtgever over willen gaan tot rechtsgang. De rapportage is daarnaast ook geschikt voor het maken van melding bij andere officiële instantie zoals de Autoriteit Persoonsgegevens. Om deze dienstverlening goed te faciliteren, beschikt opdrachtnemer over alle noodzakelijke apparatuur en technische hulpmiddelen voor forensisch onderzoek.

Forensisch Onderzoek is een bijzondere en aparte tak van sport en bij bevindingen vaak ook onderdeel in het opschalen van Incident Response. Wil een onderzoek standhouden in een rechtszaak, dan is een onderzoeker met POB-nummer geboden. Een POB-nummer wordt verstrekt aan een Particulier Onderzoekbureau dat een vergunning heeft gekregen: zonder een vergunning is het in Nederland niet toegestaan om recherchewerkzaamheden te verrichten en zijn rapportages niet rechtsgeldig.

Omdat hier de context van hoge vertrouwelijkheid en onafhankelijkheid geldt, moet nader worden gekeken op welke wijze een aanbesteding tegemoet kan komen aan de bijzondere aspecten van dienstverlening, kwaliteit en waarborgen.

FO1	Heeft u in uw dienstportfolio het uitvoeren van (digitaal) Forensisch Onderzoek? Zo ja: a) Hoe kunnen verschillende vormen van digitaal Forensische onderzoeken onderscheidenlijk als in de markt breed herkenbare c.q. erkende af te nemen diensten worden getypeerd/omschreven? Welke vormen levert u?

	b) Zijn er aanpalende (advies-)diensten verbonden, maar separaat van de Forensische onderzoeken?
Antwoord	
FO2	Hoe en in hoeverre kunnen door u gebruikte manieren/methoden van onderzoek en/of de door u hierbij in te zetten expertise en/of in te zetten hulpmiddelen bijdragen aan het onderscheidend vermogen tussen aanbieders?
Antwoord	
FO3	Welke eisen zouden wij op het niveau van een raamovereenkomst moet stellen (geldend voor alle hieronder te verstrekken opdrachten)? Met welke wensen kunnen wij een zinvol onderscheid maken tussen de niveaus van dienstverlening van aanbieders?
Antwoord	
FO4	Welke randvoorwaarden stelt u aan de Deelnemers bij de aanvraag en het gebruik van deze Forensische Onderzoeken? Welke aandachtspunten of adviezen wilt u meegeven?
Antwoord	
FO5	Welk prijsmodel hanteert u bij deze Forensische Onderzoeken? Wat zijn belangrijke kostendrivers (factoren die de hoogte van de prijs voor de Deelnemer bepalen)?
Antwoord	
FO6	Hieronder is ruimte voor uw eventuele aanvullende reactie.
Reactie	

3.4.5 IB-consultancy

Het betreft hier het op verzoek van een Deelnemer leveren van advieswerkzaamheden op het gebied van:
- IB-aspecten in het algemeen;
- het bedenken, opbouwen en volwassener maken van Incident Response en/of Security Operations;
- Business continuity (planvorming)
- IB-risicoanalyse
- IB-volwassenheidsmeting
- …

Hier kan sprake zijn van losse adviesaanvragen en/of strippenkaart-constructies. Een en ander af te wegen in de verhouding tot kwaliteit, inspanning en rendement.

Quantum veilige Cyptografie

Dit wordt een belangrijk onderdeel in consultancy. Als producten op dit punt gewijzigd moeten worden, is het zaak te weten wat dat betekent. Cryptografie is onder andere op vele plekken aanwezig waar sprake is van communicatie en certificaten. Van telefoons tot systemen.

IB1	In hoeverre wordt bij u al rekening houden met AI en Quantum cryptografie en heeft u daar een visie op? Hoe zou u deze elementen in een marktbenadering (aanbesteding) zinvol ingebed zien?
IB2	Hieronder is ruimte voor uw eventuele aanvullende reactie.
Reactie	

#