



Programma van Eisen

Resultaatverplichte ICT/IV-Opdrachten

Informatiebeveiligingsonderzoeken

(RVICTO-PT-II)

TenderNed-kenmerk : 620596
IUC-registratienummer : 202510196
Versie : D1.1

Revisie tabel

Dit document is een voortzetting van versie 1.0 uit de ingetrokken aanbesteding met TenderNed -kenmerk 609833. Voor de heraanbesteding met TenderNed-kenmerk 620596 zijn in versie 1.1 wijzigingen aangebracht ten opzichte van versie 1.0. Deze wijzigingen worden hieronder toegelicht en, waar van toepassing, rood gemarkeerd.

Versie	Datum	Toelichting
1.0	03 september 2026	Publicatie
1.1	30 oktober 2026	<ul style="list-style-type: none">• Wijziging eis A3;• Wijziging eis A5;• Correctie dubbele AI.2 en vervolgnummering;• Afbakening AI-informatieverplichtingen;• Wijziging eis nummering AI3 t/m AI6;• Wijziging AP.1.1 en AP.1.2; behoud toerbeurtpositie bij herclassificatie na intake toegevoegd;• Wijziging eis AP3;• Wijziging eis AP5.2;• Wijziging eis AP8;• Wijziging eis AP18;• Wijziging eis K1;• Wijziging eis K10;• Wijziging eis K11;• Wijziging eis K14; nummering gewijzigd;• Tekstcorrectie (typo) K.25;• Wijziging eis K31;• Wijziging eis K32; verwijzing gewijzigd;• Correctie kop K.33 en inhoudsopgave;• Wijziging eis M1; tabel gewijzigd;• Wijziging eis M2; waarden gewijzigd;• Wijziging eis M6; nummering gewijzigd;• Toevoeging bijlage 1 verduidelijking bewijslast audit-proof;• Wijziging P.5: gecertificeerde inzet in uren;

Versie	Datum	Toelichting
		<ul style="list-style-type: none"> • Wijziging P.30 en P.35; • Wijziging P.43; • Wijziging P.94; • Wijziging P170; • Toevoeging toepassingskader PQC.1–PQC.4 en aanpassing van de bepalingen over niet-toepasselijkheid en rapportage. • Wijziging T.3; • Hernummering T.8.

Inhoudsopgave

Hoofdstuk 1 - Algemene eisen	5
Vertrouwelijkheid en integriteit	5
Taal.....	5
ICT/IV-kaders.....	5
Veiligheid	6
Hoofdstuk 2 – Specifieke eisen	8
Algemeen.....	8
Interacties voor betrokkenheid	10
Executie van een onderzoek	14
Standaardrapport.....	15
Artificiële Intelligentie (AI).....	20
De eisen AI.1 tot en met AI.6 gelden voor AI-functionaliteit die wordt gebruikt bij de uitvoering van de betreffende Nadere overeenkomst of die van invloed is op het te leveren resultaat. Algemeen beschikbare kantoorfunctionaliteit en uitsluitend intern gebruikte hulpmiddelen vallen buiten de reikwijdte voor zover zij geen informatie van Deelnemer verwerken en geen materiële invloed hebben op de uitvoering of het resultaat. Opdrachtnemer verstrekt relevante, proportionele en redelijkerwijs beschikbare informatie over zijn eigen AI-gebruik. Iedere partij blijft verantwoordelijk voor de eigen verplichtingen op grond van toepasselijke wet- en regelgeving.....	20
Post Quantum Cryptografie.....	21
Generiek toepassingskader PQC.1 – PQC.4.....	21
PQC.1 tot en met PQC.4 zijn van toepassing op ieder Informatiebeveiligingsonderzoek, tenzij Opdrachtgever in de Aanvraag uitdrukkelijk bepaalt dat PQC niet aan de orde is. Het ontbreken van een expliciete verwijzing naar post-quantumcryptografie, quantumveiligheid of cryptografie geldt niet als uitsluiting. Opdrachtnemer beoordeelt actief of PQC redelijkerwijs relevant is en wijst Opdrachtgever onverwijld op een mogelijke omissie of onjuiste uitsluiting. Bij twijfel zijn PQC.1 tot en met PQC.4 van toepassing.....	21
Hoofdstuk 3 - Eisen aan het aanvraagproces	23
Hoofdstuk 4 - Eisen aan prijs en facturering	28
Hoofdstuk 5 - Eisen aan organisatie en beheer.....	30
Centraal en decentraal contractmanagement	30
Klantoverleg.....	30
Hoofdstuk 6 - Eisen aan rapportages (ROK niveau)	31
Hoofdstuk 7 - Eisen met betrekking tot prestatie management (ROK niveau)	33
KPI-1 Kwaliteit van de dienstverlening NOK	33
KPI-2 Rapportages	34
PI-1 Percentage gegunde Opdrachten	35
M-1 Aanbiedingspercentage Offertes	35
Sturingsmechanisme 1 sanctiemogelijkheden KPI-1 en KPI-2.....	36
Sturingsmechanisme 2 rouleren RVICTO-PT-veld en RVICTO-PT-bank	37
Van RVICTO-PT-veld naar RVICTO-PT-bank, primair rouleren op basis van KPI-1	37
Van RVICTO-PT-veld naar RVICTO-PT-bank, secundair rouleren op basis van PI-1.....	37
Van RVICTO-PT-veld naar RVICTO-PT-bank, rouleren door loting IUC-EZK/LVVN	38
Rouleren van RVICTO-PT-bank naar RVICTO-PT-veld	38
Achterwege blijven sanctie/gele kaart sturingsmechanisme 1 en/of rouleren van RVICTO-PT-veld naar RVICTO-PT-bank sturingsmechanisme 2	39
Programma van Eisen RVICTO-PT-II versie D1.1	

Hoofdstuk 8 - Eisen aan Maatschappelijk Verantwoord Ondernemen.....	40
Specifieke voorschriften met betrekking tot social return (SR)	40
Specifieke voorschriften met betrekking tot diversiteit en inclusie	46
Bijlage 1 - Classificatiematrix.....	48
Bijlage 2 – Model standaardrapport.....	51

Hoofdstuk 1 - Algemene eisen

Vertrouwelijkheid en integriteit

- A.1** Opdrachtnemer heeft zich voorafgaand aan de uitvoering van de Raamovereenkomst dan wel de Nadere overeenkomst ervan vergewist en garandeert dat door hem in te zetten Personeel geen integriteitsrisico's met zich meebrengen.
- Opdrachtnemer en diens Personeel zullen bij de uitvoering voor zover daarvoor aan de orde, de Gedragscode Integriteit Rijk (GIR) in acht nemen [Gedragscode Integriteit Rijk | O&P Rijk P-Direkt](#), dan wel de gedragscode voor integriteit van Deelnemer daar waar deze stringenter is dan de GIR. Deelnemer behoudt zich het recht voor om ondertekening te verlangen van een verklaring omtrent de naleving van de bedoelde gedragscode/verklaring.
 - Opdrachtnemer en diens Personeel zullen, indien zij gebruik maakt van de digitale faciliteiten van het Rijk, de (Rijksbrede) Gedragsregeling voor de digitale werkomgeving [Gedragsregeling voor de digitale werkomgeving | O&P Rijk P-Direkt](#) in acht nemen en/of, indien van toepassing, een specifieke regeling van Deelnemer.
 - Deelnemer kan van het door Opdrachtnemer ingezet Personeel een verklaring omtrent gedrag (VOG NP) verlangen of (doen) aanvragen of een vergelijkbare verklaring uit het land van herkomst voor personeel met buitenlandse nationaliteit en geeft dit aan in de Aanvraag. De VOG wordt bekostigd door Opdrachtnemer.
 - Deelnemer kan van het in te zetten Personeel een Verklaring van Geen Bezwaar (VGB) verlangen. In voorkomend geval wordt dit in de Aanvraag aangegeven. De VGB wordt bekostigd door de Deelnemer.
 - Specifiek voor AFM is voorafgaand aan de inzet van Personeel bij AFM een screeningsprocedure van toepassing. Hieronder valt onder andere een antecedentenonderzoek, ondertekening van een geheimhoudingsverklaring, ondertekening en akkoord op de Compliance Regeling die bij AFM geldt, evenals het doorgeven van eventuele nevenwerkzaamheden.

Taal

- A.2** Documenten worden opgeleverd in de Nederlandse taal, tenzij expliciet anders aangegeven in de Aanvraag of op voorhand een Opdracht of schriftelijke toestemming door de Deelnemer is verstrekt. Zie specifiek voor het standaardrapport van een beveiligingsonderzoek ook eis P.34.
- A.3** Het door Opdrachtnemer in te zetten Personeel beheerst de Nederlandse taal, ~~tenzij expliciet anders aangegeven in de Aanvraag.~~ met dien verstande dat binnen een onderzoeksteam niet alle leden de Nederlandse taal hoeven te beheersen, mits het team wordt aangestuurd door een Nederlandstalige rapporteur die de klantcommunicatie voert en de professionele eindverantwoordelijkheid draagt conform eis P.4/P.5.

ICT/IV-kaders

- A.4** Deelnemers hanteren een aantal ICT-/IV-kaders waaraan de Opdrachtnemers zich bij Nadere overeenkomsten dienen te conformeren. Opdrachtnemer is bereid om voor uitvoering van Opdrachten af te stemmen over de (referentie)architecturen, technologie standaarden, principes en bouwstenen binnen het ICT-/IV-domein van de Deelnemer(s), alsmede over mogelijke wijzigingen daarin, om de informatiebehoefte van de klant voor de betreffende Nadere overeenkomst(en) goed in te kunnen passen binnen de ICT-/IV-kaders. Waar relevant zal Deelnemer dit al in de Aanvraag specificeren.

De belangrijkste (bronnen van en hun opvolgers) standaarden (niet limitatief) worden hieronder opgesomd:

- a. Informatiebeveiliging: het Besluit voorschrijft informatiebeveiliging rijksdienst (VIR) 2007, het Besluit voorschrijft informatiebeveiliging rijksoverheid – bijzondere informatie (VIRBI) 2025, de Baseline Informatiebeveiliging Overheid (BIO2), zie ook eis A.10
- b. Pentest execution standard, zie eis P.6

c. Standaarden zoals genoemd in eis P.28

A.5 ~~In het geval van een vermoedelijk of geconstateerd incident, waarin bij de uitvoering van een Nadere overeenkomst niet voldaan wordt aan de daarvoor geldende ICT/IV kaders, wetgeving of de beveiligingsnormen zoals genoemd in A.10, dient Opdrachtnemer dit onverwijld te melden aan de Deelnemer. Opdrachtnemer meldt ook ieder incident dat de beschikbaarheid, integriteit of vertrouwelijkheid van bij de Opdracht verwerkte/te verwerken gegevens raakt binnen 24 uur na ontdekking aan Deelnemer, inclusief aard, omvang en getroffen maatregelen.~~

Opdrachtnemer treft onverwijld alle maatregelen die binnen zijn bevoegdheden en feitelijke macht liggen om Incidenten te beëindigen en de gevolgen te beperken. Voor de melding en vervolgrapportage van Incidenten, Bijna-incidenten en dreigingen gelden de definities, informatievereisten en termijnen van artikel 4 van het Addendum Cyberbeveiligingswet en Wet weerbaarheid kritieke entiteiten bij de ARBIT-2022.

Incidenten worden uiterlijk binnen twaalf uur na kennisname gemeld, tenzij significantie op dat moment redelijkerwijs kan worden uitgesloten overeenkomstig artikel 4.1. Bij twijfel wordt gemeld. Voor uitgezonderde Incidenten geldt de verzamelrapportage van artikel 4.2a, met onverwijldde escalatie zodra mogelijk sprake is van significantie. Deze uitzondering laat de verplichting tot onmiddellijke risicobeperkende maatregelen onverlet.

Bij samenloop met een Inbreuk geldt overeenkomstig artikel 5.1 de kortste toepasselijke meldtermijn. Na activering van artikel 6 geldt voor Verstoringen tevens artikel 7. De toepasselijke meldroutes en contactpersonen worden vooraf per Nadere overeenkomst vastgelegd; de betrokken Deelnemer wordt in de melding betrokken.

A.6 Opdrachtnemer zorgt voor actuele kennis van ontwikkelingen in het vakgebied en opkomende technieken (emerging technologies) die relevant zijn binnen het domein van Nadere overeenkomst(en) die Opdrachtnemer uitvoert voor de Deelnemer(s). Deze kennis is aanwezig binnen de organisatie van Opdrachtnemer.

A.7 Alle voor de Prestatie(s) van de Nadere overeenkomsten benodigde data die door of namens Deelnemer wordt verwerkt buiten de omgevingen van Deelnemer(s), vinden plaats binnen de Europese Economische Ruimte (EER) en dienstverlening en dataverwerkingen vallen uitsluitend binnen Europese jurisdictie of nationale jurisdictie van lidstaten van de Europese Unie. Deelnemers kunnen per Opdracht verlangen dat de Nederlandse jurisdictie van toepassing is. Dit geldt standaard voor verwerkingen van gegevens die door Deelnemer als staatsgeheim zijn gerubriceerd. Opdrachtnemer garandeert voor elke Opdracht dat gegevens buiten de omgevingen van Deelnemer(s) niet worden overgedragen aan partijen buiten deze jurisdictie zonder schriftelijke toestemming van de Deelnemer.

A.8 Opdrachtnemer zal als onderdeel van de Prestatie die activiteiten verrichten die beschreven zijn in de Nadere overeenkomst (dus inclusief de Aanvraag, Nota's van Inlichtingen, prijsopgaven et cetera). Dit omvat ook activiteiten en voorzieningen die daaruit volgen of noodzakelijk zijn om de Prestatie conform de Nadere overeenkomst te verrichten, ook als die activiteiten of voorzieningen niet expliciet zijn beschreven.

Veiligheid

A.9 Certificeringen die nodig zijn voor het uitvoeren van de Nadere overeenkomst (w.o. kwalificaties van het Personeel die de Opdrachten uitvoeren) dienen tijdens de uitvoering actueel te zijn.

A.10 Opdrachtnemer dient alle gegevens die hij verwerkt bij het onderzoek aantoonbaar adequaat te beveiligen, conform de relevante maatregelen uit de meest actuele versie van de BIO, ISO 27001/2 of gelijkwaardig. Onder de verwerkte informatie vallen o.a. de gegevens van gevonden kwetsbaarheden, gebruikte aanvalsmethoden die succesvol zijn geweest en de daarbij vergaarde gegevens.

Indien Opdrachtnemer bij het onderzoek in aanraking kan komen met bijzondere (gerubriceerde) informatie die valt onder het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIRBI) 2025 of gevoelige informatie die volgens Deelnemer een vergelijkbaar niveau

van veiligheidsclassificatie krijgen, houdt hij zich aan de VIRBI 2025 en toepasselijke (aanvullende) bindende voorschriften/voorwaarden die Deelnemer of een door Deelnemer aangewezen beveiligingsautoriteit hieraan stelt.

Voor de maatregelen van veilige verwerking (w.o. opslag, inzage en uitwisseling) van gerubriceerde of gevoelige informatie zullen Deelnemer en Opdrachtnemer nadere (bindende) voorwaarden overeenkomen. Als Opdrachtnemer (deels) niet kan of wil voldoen aan de VIRBI 2025 en eventuele aanvullende bindende voorschriften/voorwaarden, proberen Deelnemer en Opdrachtnemer tot een oplossing te komen waarin het onderzoek wel volgens de noodzakelijke veiligheidsvoorschriften kan worden uitgevoerd. Gedacht kan worden aan het onder voorwaarden gebruikmaken van bestaande voorzieningen van Deelnemer, het door Deelnemer zorgdragen en faciliteren van nieuwe voorzieningen die Opdrachtnemer hiervoor moet gebruiken, dan wel het op andere wijze mitigeren van veiligheidsrisico's.

- A.11** De Opdrachtnemer hanteert regels voor medewerkers en andere verwerkers, die buiten Nederland persoonsgegevens of authenticatiemiddelen (voor de toegang tot persoonsgegevens vanuit het buitenland) met zich meedragen of in hun bezit hebben, ongeacht of deze informatie versleuteld is, waarbij deze regels schriftelijk zijn vastgelegd en aantoonbaar aan medewerkers zijn gecommuniceerd.
- A.12** De verwerking door Opdrachtnemer wordt op verwerkers/persoonsniveau gelogd, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens de medewerker heeft opgevraagd, ingezien en aangepast. Logging wordt beveiligd opgeslagen, is uitsluitend toegankelijk voor geautoriseerde personen en wordt bewaard conform de relevante BIO-maatregelen voor monitoring en logging.

Hoofdstuk 2 – Specifieke eisen

Algemeen

- P.1** Deelnemers kunnen aan Opdrachtnemer een Opdracht verstrekken tot het uitvoeren van een informatiebeveiligingsonderzoek. Deelnemer en Opdrachtnemer bereiken dan overeenstemming over de scope, uitvoering en op te leveren eindresultaat van en eventueel te verlenen nazorg bij dit onderzoek. Het eindresultaat is in beginsel een standaardrapport, al dan niet voorzien van aanvullende documenten en/of toelichting. Het eindresultaat is betrouwbaar, reproduceerbaar en kan (optioneel) door Deelnemer of een derde partij (zoals een auditor) gevalideerd worden. De validatie kan uitgevoerd worden om extra zekerheid te verkrijgen over de kwaliteit van uitvoering en resultaten. Ingeval Opdrachtnemer een onderaannemer/derde wil inzetten voor het uitvoeren van een deel van het onderzoek, blijft Opdrachtnemer eindverantwoordelijk en gelden voor deze onderaannemer/derde dezelfde eisen aan de dienstverlening. Opdrachtnemer ziet erop toe dat deze eisen door de onderaannemer/derde worden nageleefd.
- P.2** Opdrachtnemer zal binnen de Opdracht een (mondelinge) toelichting geven op het uitgevoerde onderzoek en hetgeen hij aan Deelnemer (in de vorm van een rapportage of anderszins) heeft opgeleverd, inclusief zijn bevindingen en adviezen. In zijn adviezen doet Opdrachtnemer suggesties voor mogelijke opvolging en verantwoordelijken voor de opvolging van gegeven adviezen. Opdrachtnemer staat hierbij open voor interactie met door Deelnemer aan te wijzen contactpersonen, die belang hebben bij de uitkomsten en eventuele opvolging van het onderzoek.

Het standaardrapport wordt digitaal verstrekt

- P.3** Het standaardrapport wordt digitaal verstrekt. Opdrachtnemer hanteert hiervoor het format in Bijlage 2 PvE – Model standaardrapport. Deelnemer en Opdrachtnemer kunnen na aanvang van de Opdracht nadere afspraken maken over zowel opzet van het rapport, aanvullend te verstrekken documenten als wijze van verstreking, mits deze rapportagevereisten niet strijdig zijn met dit Programma van Eisen.

Aanwijzing en beschrijving rapporteur, opsteller of hoofdonderzoeker

- P.4** In het op te leveren rapport is de naam van een persoon (of meerdere personen) genoemd, die de professionele eindverantwoordelijkheid draagt (of dragen) voor de uitvoering van het informatiebeveiligingsonderzoek en het betreffende rapport. Deze persoon (of personen) is (of zijn) in het rapport als rapporteur(s) aangemerkt.

Beschrijving van de verplichte certificering, waarover de rapporteur beschikt

- P.5** Het onderzoeksteam, bestaande uit de rapporteur(s) en de overige voor uitvoering van het informatiebeveiligingsonderzoek in te zetten professionals, beschikt als geheel over de voor het onderzoek relevante geldige certificering(en). Het is toegestaan dat een of meerdere leden van het onderzoeksteam niet aantoonbaar beschikken over relevante geldige certificering, mits andere leden hier gezamenlijk wel aantoonbaar over beschikken. Bovendien moeten de niet-gecertificeerde leden van het team onder inhoudelijke supervisie werken van een of meerdere leden met relevante geldige certificering(en), waarbij een gecertificeerd lid maximaal twee niet-gecertificeerde leden onder zijn/haar inhoudelijke supervisie mag hebben. ~~De rapporteur is hiervan uitgezonderd, maar is (eind)verantwoordelijk voor het borgen van voldoende inzet van gecertificeerde leden van het onderzoeksteam en de kwaliteit van het onderzoek.~~ **De rapporteur is uitsluitend uitgezonderd van de supervisieverhouding van maximaal twee niet-gecertificeerde leden per gecertificeerd lid. Een niet-gecertificeerde rapporteur werkt wel onder inhoudelijke supervisie van een lid met relevante geldige certificering(en). De rapporteur blijft (eind)verantwoordelijk voor het borgen van voldoende inzet van gecertificeerde leden van het onderzoeksteam en de kwaliteit van het onderzoek.** ~~De hoeveelheid inzet van gecertificeerde leden van het onderzoeksteam is ten minste de helft van de totale inzet van het onderzoeksteam voor het onderzoek.~~ **Ten minste de helft van het totale aantal uren dat door het onderzoeksteam aan het onderzoek wordt**

besteed, wordt besteed door professionals die beschikken over de voor het onderzoek relevante geldige certificering(en).

Een relevante geldige certificering genoemd in de meest recente versie van de lijst kwalificaties voor pentesters, als appendix van het CCV-keurmerk Pentesten, voldoet hier in elk geval aan. Zie deze hyperlink voor de meest recente versie: <https://hetccv.nl/keurmerken/cybersecurity/pentest/documenten/>.

Ook certificeringen die niet genoemd zijn in de lijst kwalificaties voor pentesters, als appendix van het CCV-keurmerk Pentesten, kunnen als geldig en gelijkwaardig worden gezien. De eisen die het CCV stelt aan trainingen en examens om erkend te worden als (gelijkwaardige en) geldige certificering en passende kwalificatie voor pentesters, gelden dan ook hier:

1. Het certificaat geeft een goede indicatie dat de kandidaat beschikt over uitgebreide kennis en vaardigheden op het gebied van penetratietesten. Instapcertificaten kunnen niet aan deze criteria voldoen.
2. Om het certificaat te behalen, ondergaat de kandidaat een examen waarbij hij/zij minimaal 23 uur zelfstandig hackt in een labomgeving.
3. Na afloop van het examen stelt de kandidaat een rapport op dat daadwerkelijk wordt beoordeeld door een examinerator.
4. Er zijn adequate maatregelen genomen om fraude tijdens het examen te voorkomen.
5. Er is minimaal 2 jaar een examen voor persoonscertificering voor pentesters beschikbaar om in aanmerking te komen voor deze lijst (voldoende trackrecord om aan de overige criteria te voldoen).

Als het CCV gedurende de looptijd van de Raamovereenkomst nieuwe eisen hieraan stelt (via een nieuwe versie van het appendix van het CCV-keurmerk Pentesten, zie eerdere hyperlink), kunnen Deelnemer en Opdrachtnemer zich ook hierop beroepen om te bepalen of certificaten als geldig en gelijkwaardig kunnen worden gezien. Bij eventuele tegenstrijdigheid tussen versies prevaleert de lagere vereiste of uitleg in het voordeel van de Opdrachtnemer.

Pentest Execution Standard

P.6 Het onderzoek wordt in beginsel uitgevoerd volgens de zeven fasen van de Pentest Execution Standard (PTES) (http://www.pentest-standard.org/index.php/Main_Page) of, na voorstel door Opdrachtnemer en na acceptatie door Deelnemer, volgens fasen van een andere vergelijkbare erkende industriestandaard voor het uitvoeren van informatiebeveiligingsonderzoeken. De zeven fasen van PTES zijn:

1. Interacties vóór de betrokkenheid (Pre-engagement Interactions);
2. Informatie verzamelen (Intelligence Gathering);
3. Modelleren van bedreigingen (Threat Modeling);
4. Kwetsbaarheidsanalyse (Vulnerability Analysis);
5. Exploitatie (Exploitation);
6. Post-exploitatie (Post Exploitation);
7. Rapportage (Reporting).

In het Plan van Aanpak kunnen Deelnemer en Opdrachtnemer een afwijkende fasering van het onderzoek overeenkomen of een of meer fasen van de toe te passen standaard voor het onderzoek buiten toepassing verklaren (met name bij kleinere onderzoeken). De voor de fasering toe te passen standaard kan gecombineerd worden met andere voor de uitvoering van het onderzoek te gebruiken standaarden en methodieken.

P.7 Deelnemer kan, nadat Opdrachtnemer het (initiële) onderzoek heeft uitgevoerd en de rapportage heeft opgeleverd, de aanbevelingen opvolgen en maatregelen treffen om de in de rapportage geconstateerde risico's te minimaliseren. Hierna kan Deelnemer aan Opdrachtnemer vragen een herhalingsopdracht (ook: hertest) uit te voeren. De herhalingsopdracht ziet in beginsel uitsluitend op eerder gevonden kwetsbaarheden of bevindingen. Hiermee beoogt Deelnemer uitsluitel te krijgen of de maatregelen doeltreffend zijn doorgevoerd en de risico's tot een volgens Deelnemer acceptabel niveau zijn verminderd. Een herhalingsopdracht doorloopt dezelfde fasering. Een herhalingsopdracht wordt in beginsel als optie bij een initieel onderzoek overeengekomen, eventueel met een maximale termijn na oplevering van

het initiële onderzoeksrapport, maar kan ook op basis van een nieuwe Offerte van Opdrachtnemer aan hem worden verstrekt.

- P.8** Als de Opdracht een optie bevat tot het uitvoeren van een herhalingsopdracht en Deelnemer wil daarvan gebruikmaken, dan kan Deelnemer zonder minicompentie of toerbeurtschema aan Opdrachtnemer een timeboxed herhalingsopdracht verstrekken. De toepasselijke uurtarieven van Opdrachtnemer op grond van de originele Opdracht zijn hierop ook van toepassing, waarbij Deelnemer een maximum aantal te vergoeden uren en zodoende een vaste prijs voor uitvoering van de herhalingsopdracht voorschrijft.

Opdrachtnemer mag de uitvoering van deze herhalingsopdracht weigeren. Na weigering zal Deelnemer de Aanvraag voor het uitvoeren van een herhalingsopdracht in minicompentie of toerbeurtschema uitzetten met het verzoek hiervoor een (nieuwe) Offerte uit te brengen.

Interacties voor betrokkenheid

- P.20** Opdrachtnemer garandeert dat hij uitsluitend werkzaamheden uitvoert die binnen de reikwijdte van de opdrachtoomschrijving/scope van de Aanvraag vallen. De intake die na start van de Nadere overeenkomst plaatsvindt is niet bedoeld om de scope van de Opdracht en de voorwaarden hieraan wezenlijk te wijzigen. In de intake kunnen Deelnemer en Opdrachtnemer nadere werkafspraken maken over de onderwerpen die al in de Aanvraag, de Offerte of Nadere overeenkomst zijn beschreven, dan wel hier nog niet zijn beschreven maar verdere afstemming/detaillering behoeven en in het Plan van Aanpak vastgesteld worden.

Beschrijving intakegesprek

- P.21** Het intakegesprek is onderdeel van de Opdracht en wordt binnen 10 werkdagen na start van de Opdracht uitgevoerd, tenzij Deelnemer en Opdrachtnemer akkoord gaan met een andere termijn of moment voor het intakegesprek. Deze termijn start op de eerste werkdag na start/ondertekening van de Nadere overeenkomst of afroep binnen een Nadere overeenkomst. Het intakegesprek vindt plaats voordat enige testactiviteiten worden gestart.
- P.22** Opdrachtnemer maakt een verslag van het intakegesprek. Dit verslag bevat de besproken onderwerpen die nodig zijn om een Plan van Aanpak te maken voor uitvoering van het onderzoek (zie eis P.24), de datum van het intakegesprek, de deelnemers aan het intakegesprek en welke informatie er nog verstrekt moet worden voor het informatiebeveiligingsonderzoek.
- P.23** Voorafgaand aan het onderzoek, bijvoorbeeld in het intakegesprek, benoemen Deelnemer en Opdrachtnemer elkaars contactpersonen die met elkaar tijdens de uitvoering van de Opdracht kunnen afstemmen, waarover en (indien van toepassing) onder welke voorwaarden. Indien van toepassing benoemt Deelnemer ook contactpersonen van rechthebbende derde partijen die voor het onderzoek relevant zijn.

Opdrachtnemer en Deelnemer bespreken voorafgaand aan het onderzoek eventuele door hen geziene risico's met betrekking tot de beschikbaarheid en/of deskundigheid en/of bevoegdheid van alle door partijen voorgestelde contactpersonen en kunnen waar gewenst mitigerende maatregelen nemen om beschikbaarheid en/of deskundigheid en/of bevoegdheid beter te borgen.

Plan van Aanpak

- P.24** Na het intakegesprek levert Opdrachtnemer een definitief voorstel Plan van Aanpak op voor het uitvoeren van de gevraagde Opdracht. Het definitieve Plan van Aanpak omvat ten minste:
- een omschrijving van de scope, doelstelling(en) van de Opdracht, te onderzoeken objecten, eigenaarschap en fysieke locaties (land) van objecten inclusief gevolgen voor naleving relevante wet- en regelgeving
 - optioneel (indien verzocht door Deelnemer): de locatie(s) van uitvoering van het onderzoek
 - te gebruiken methodiek(en), standaarden, aanvalsperspectief (black/grey/whitebox, evt. toepassing van het "assume breach" principe), aanvalsscenario's (op grond van eventuele applicatie- of klantspecifieke (dreigings)scenario's), toe te passen hulpmiddelen (tools)
 - een planning (w.o. datums/tijden/attack window van onderzoek), verwachte inzet en afspraken hierover

- voorwaarden en garanties van Opdrachtnemer en/of deelnemer t.a.v. de planning
- afspraken over hoe om te gaan met eventuele risico's en incidenten die zich tijdens de uitvoering kunnen voordoen
- indien testen in productie plaatsvindt, worden vooraf expliciete risico's, randvoorwaarden en eventuele beperkingen schriftelijk overeengekomen.
- overige voorwaarden voor uitvoering onderzoek
- namen van de rapporteur(s) en overige in te zetten professionals, inclusief de relevante en geldige individuele certificeringen
- afspraken over communicatie en contactpersonen tussen Opdrachtnemer, Deelnemer en eventuele derden
- afspraken over de distributiekring van het onderzoeksrapport of informatie over het onderzoek, inclusief mogelijke vertrouwelijkheid van informatie
- afspraken over het al dan niet versleutelen en het hashen van documenten/bestanden
- afspraken over het al dan niet opleveren van (ruwe) scanresultaten, bewijsmiddelen, checklists, lijsten met gedeelde bestanden en documenten
- als bijlage het verslag van het intakegesprek

Het definitieve Plan van Aanpak dient door Deelnemer schriftelijk te worden goedgekeurd. Het Plan van Aanpak benoemt de uitgangspunten voor uitvoering van het onderzoek. Opdrachtnemer start het onderzoek pas nadat het Plan van Aanpak door Deelnemer is goedgekeurd.

Deelnemer en Opdrachtnemer kunnen voorafgaande aan het onderzoek overeenkomen hoe Opdrachtnemer tijdens het uitvoeren van het onderzoek dient om te gaan met risico's, mogelijke incidenten en bevindingen die boven een nader te bepalen risiconiveau komen (wie dient waarover geïnformeerd te worden, wordt het onderzoek vervolgd of gestaakt). Dit wordt besproken in het intakegesprek en vastgelegd in het Plan van Aanpak. Opdrachtnemer adviseert Deelnemer hierbij desgewenst al direct (voorafgaand aan de rapportage) over effectieve maatregelen om de risico's (al dan niet tijdelijk) te mitigeren. Ook benoemt Opdrachtnemer welke risico's niet tijdelijk gemitigeerd kunnen worden.

Scope

- P.25** Er is een beschrijving van de scope van het onderzoek. Deze bevat de relevante selectie van onderdelen en objecten (volgens sub 2.2.1 t/m 2.2.8 hieronder). Opdrachtnemer verifieert in het intakegesprek of de scopebeschrijving overeenkomt met de behoeftes uit het intakegesprek en past binnen de afgesproken tijdspanne. Opdrachtnemer verwerkt nieuwe inzichten over de scope in het Plan van Aanpak, mits deze niet leiden tot een wezenlijke wijziging.

Scope - Aanvalsperspectieven

- P.26** In de scopebeschrijving is opgenomen welk aanvalsperspectief is afgesproken, wat gevalideerd wordt door de Deelnemer en Opdrachtnemer. Opdrachtnemer voert op verzoek van Deelnemer een onderzoek uit op basis van blackbox, greybox of whitebox:

1. Black box: er worden vooraf geen gegevens beschikbaar gesteld over of toegang tot het te onderzoeken object. De test wordt uitgevoerd vanuit een ongeautoriseerd perspectief en benadert de realiteit van cyber criminelen het meest.
2. Grey box: er worden beperkte gegevens over de applicatie(s) en infrastructuur beschikbaar gesteld. Ook kunnen er (test) login credentials beschikbaar worden gesteld. De penetratietest wordt uitgevoerd vanuit het perspectief van iemand die normale toegang heeft (bemachtigd), waarbij geprobeerd kan worden buiten de gestelde kaders van dat account te treden.
3. White box: de onderzoekers krijgen voor het onderzoek volledige (expliciete en substantiële) kennis van de interne werking van de applicatie(s) en infrastructuur, inclusief de broncode, implementatiedetails, configuraties en architectuurdocumentatie. Additionele gegevens over de applicatie(s), netwerkdigrammen en infrastructuur worden beschikbaar gesteld. Ook kunnen er (test) login credentials beschikbaar worden gesteld.

In het intakegesprek kunnen nadere afspraken gemaakt worden over het niveau van voorkennis.

Scope - Objecten

- P.27** De objecten die onderzocht worden, zijn onderdeel van de scope. Indien er sprake is van een scope object met een specifiek versienummer dient deze te worden vastgelegd als onderdeel van het object. Per scope object wordt aangegeven conform welke bijbehorende kaders/standaarden onderzoek wordt gedaan. Alle kaders/standaarden die van toepassing kunnen zijn op het betrokken object, zijn in de scopebeschrijving opgenomen.

Standaarden

- P.28** Opdrachtnemer voert zijn Opdrachten uit conform de meest recentelijk gepubliceerde en erkende industriestandaards, gerelateerd aan de objecten in de scope. De belangrijkste zijn:
- bij webapplicaties: OWASP Web Security Testing Guide (WSTG);
 - bij Internet of Things (IoT) apparaten: OWASP IoT Security Testing Guide (ISTG);
 - bij API: conform de standaard WSTG hoofdstuk 12 API Testing;
 - bij firmware: OWASP Firmware Security Testing Methodology (FSTM);
 - bij mobiele applicaties: OWASP Mobile Application Security Testing Guide (MASTG);
 - bij operationele technologie / industriële automatiserings- en besturingssystemen: ISA/IEC 62443.

In het intakegesprek kunnen Deelnemer en Opdrachtnemer nadere afspraken maken over het gebruik van overige standaarden, normenkaders, richtlijnen of referentiebronnen, zoals de Google Hacking Database (GHDB), Open Source Security Testing Methodology Manual (OSSTMM), National Institute of Standards and Technology (NIST), Information System Security Assessment Framework (ISSAF), MITRE ATT&CK, de CWE top 25, CIS-controls (Center for Internet Security), SOC2, de ICT-beveiligingsrichtlijnen voor webapplicaties (van NCSC), overige beveiligings- of beheersingsrichtlijnen van het NCSC.

Hiernaast conformeert Opdrachtnemer zich aan de fasering van de Penetration Testing Execution Standard (PTES), tenzij anders overeengekomen.

Deelnemer en Opdrachtnemer leggen alle afspraken over de in het onderzoek toe te passen standaarden en eventuele afwijkingen hierop vast in het Plan van Aanpak.

Vaststelling scope en objecten

- P.29** Alle binnen de scope vastgestelde objecten worden getest.

Voorafgaand aan het onderzoek verifieert Opdrachtnemer bij Deelnemer of de objecten in een acceptatie-omgeving moeten worden getest en moeten worden gevalideerd in de productie-omgeving of dat direct in de productie-omgeving moet worden getest. De afspraken hierover worden vastgelegd in het Plan van Aanpak.

Eigenaarschap scope

- P.30** Voorafgaand aan de start van het onderzoek (bijvoorbeeld bij het intakegesprek) heeft Opdrachtnemer geverifieerd dat de lijst aan objecten toebehoort aan de Deelnemer of toestemming is gegeven door de rechthebbende derde partij voor het uitvoeren van het onderzoek.

~~Het proces en de verantwoordelijkheid om tijdig tot toestemming van de rechthebbende derde partij te komen, stemmen Opdrachtnemer, Deelnemer en eventueel deze derde partij indien nodig nader af, voorafgaand aan de uitvoering van het onderzoek.~~

Deelnemer draagt zorg voor het tijdig verkrijgen van de noodzakelijke toestemmingen van rechthebbenden en betrokken derden. Opdrachtnemer draagt er vanuit zijn deskundigheid aan bij dat tijdens de intake wordt vastgesteld welke toestemmingen voor de voorgenomen uitvoering noodzakelijk zijn. Het proces wordt waar nodig met de betrokken derde partij afgestemd, voorafgaand aan de uitvoering van het onderzoek. Indien deze rechthebbende derde partij nadere voorwaarden stelt, die noodzakelijk zijn om het onderzoek te kunnen uitvoeren, stemmen Deelnemer, Opdrachtnemer en deze derde partij af of en in hoeverre hieraan voldaan kan worden bij de uitvoering van het onderzoek. De afspraken hierover worden opgenomen in het Plan van Aanpak en de rapportage. Indien Opdrachtnemer en/of Deelnemer besluiten zich niet aan deze nadere voorwaarden van de rechthebbende derde partij te kunnen of willen

committeren, geeft dit het recht aan Deelnemer en Opdrachtnemer om de betreffende Opdracht eenzijdig te beëindigen.

Jurisdictie scope-objecten

- P.31** Voorafgaand aan start van het onderzoek (bijvoorbeeld bij het intakegesprek) stelt Opdrachtnemer vast wat de fysieke locaties zijn van de te onderzoeken objecten en welke relevante wet- en regelgeving hier van toepassing is. De Deelnemer levert waar nodig de informatie aan over de fysieke locatie van een object, laat deze door de eigenaar(s) van het object aanleveren of bevestigt deze. Het beveiligingsonderzoek wordt uitgevoerd onder Nederlandse jurisdictie. Indien objecten zich buiten Nederland bevinden, wordt vooraf schriftelijk vastgelegd welke aanvullende juridische of technische maatregelen noodzakelijk zijn.
- P.32** Opdrachtnemer voert op verzoek van Deelnemer het onderzoek uit vanaf een nader te benoemen externe en/of interne locatie (een door Deelnemer gebruikte locatie of vanaf een locatie van een rechthebbende derde partij). Indien remote testen plaatsvindt, worden beveiligingsmaatregelen voor de verbinding vooraf overeengekomen.

Accordering scope

- P.33** Er is schriftelijke overeenstemming tussen een bevoegde functionaris van de Deelnemer en Opdrachtnemer over het Plan van Aanpak, waaronder de uit te voeren scope van onderzoek.

Taal rapport

- P.34** Voorafgaand aan start van het onderzoek (bijvoorbeeld bij het intakegesprek) heeft Opdrachtnemer geverifieerd wat de taal van het standaardrapport moet zijn. De standaard is Nederlands, maar Deelnemer kan op voorhand een opdracht of schriftelijke toestemming geven om delen van het standaardrapport (exclusief de managementsamenvatting) in het Engels te laten opstellen. Het rapport bevat altijd een Nederlandstalige managementsamenvatting.

Vrijwaringsverklaring

- P.35** Opdrachtnemer, Deelnemer en eventueel nog derden (voor zover te onderzoeken objecten niet in eigendom van Deelnemer zijn) komen per Nadere overeenkomst een vrijwaringsverklaring overeen voor het uitvoeren van het informatiebeveiligingsonderzoek. ~~Partijen kunnen hierbij gebruikmaken van het model in NOK bijlage 3 — Model vrijwaringsverklaring. Partijen gebruiken hiervoor het voorgeschreven Model Vrijwaringsverklaring, opgenomen als Bijlage 15 bij het Aanbestedingsdocument. De voor het betreffende onderzoek ingevulde verklaring wordt als Bijlage 3 bij de Nadere overeenkomst gevoegd.~~ 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. ~~Deelnemer en, indien van toepassing, de Onderzochte Partij vrijwaren Opdrachtnemer tegen aanspraken van rechthebbenden of andere derden die voortvloeien uit de uitvoering van het onderzoek binnen de overeengekomen scope, verleende toestemmingen en instructies. Deze vrijwaring geldt niet voor zover de betreffende aanspraak voortvloeit uit een aan Opdrachtnemer toerekenbare tekortkoming.~~ Deelnemer draagt zorg voor afstemming met eventuele derden en ondertekening en retournering van de vrijwaringsverklaring aan Opdrachtnemer voordat het onderzoek start. Een door bevoegde functionaris(sen) ondertekende vrijwaringsverklaring wordt dan onderdeel van de betreffende Nadere overeenkomst.
- ~~Opdrachtnemer vangt niet aan met uitvoering van het onderzoek zonder schriftelijke goedkeuring door Deelnemer van genoemde documenten dan wel een afwijking hierop. Opdrachtnemer vangt niet aan met het onderzoek voordat de noodzakelijke toestemmingen zijn verkregen, de vrijwaringsverklaring door de bevoegde functionaris(sen) is ondertekend en Deelnemer schriftelijk goedkeuring voor de uitvoering heeft verleend.~~
- P.36** In de Aanvraag kan Deelnemer eisen dat een door betrokken partijen getekende Verwerkersovereenkomst een noodzakelijke voorwaarde is voor het starten van de Opdracht. Dat zal geëist worden als Opdrachtnemer bij de uitvoering van het onderzoek toegang kan krijgen tot persoonsgegevens, als hij voor dit onderzoek

verwerker is en er een juridische noodzaak is afspraken over de verwerking van de (persoons)gegevens vast te leggen.

Opdrachtnemer vangt dan niet aan met uitvoering van het onderzoek zonder een door betrokken partijen getekende Verwerkersovereenkomst.

Executie van een onderzoek

- P.40** Opdrachtnemer voert het onderzoek uit conform het definitieve Plan van Aanpak, waarbij een wederzijds overeengekomen latere versie bij tegenstrijdigheid prevaleert boven een eerdere versie. Deelnemer en Opdrachtnemer kunnen tijdens de uitvoering van het onderzoek aanpassingen op het Plan van Aanpak overeenkomen, mits deze ook expliciet worden vastgelegd en beargumenteerd in het standaardrapport. De aanpassingen mogen geen wezenlijke wijzigingen zijn.
- P.41** Voor zover dit in het Plan van Aanpak is overeengekomen, informeert Opdrachtnemer vlak voordat het attack window van het onderzoek begint de hiervoor aangewezen contactpersoon/contactpersonen van Deelnemer.

Assume breach

- P.42** De standaard bij een onderzoek (behalve bij black box) is dat er getest wordt op basis van het "assume breach" principe, waarbij ervan uit wordt gegaan dat een aanval/uitvoerder reeds toegang heeft tot de netwerkomgeving/objecten. Hierdoor kan de robuustheid/kwetsbaarheid van het object 'as is' beter worden getest, zonder invloed van andere mitigerende maatregelen (zoals firewalls etc.). Partijen stemmen dan af welke maatregelen nodig zijn om dat mogelijk te maken.
- Deelnemer en Opdrachtnemer kunnen ook nader overeenkomen dat/wanneer er niet wordt getest op basis van het "assume breach" principe.

CVSS-scores

- P.43** Aan iedere bevinding wordt een score toegekend volgens de standaard van het Common Vulnerability Scoring System (CVSS). ~~De CVSS-scores dienen te worden berekend op basis van de relevante metriekgroepen: Base Metrics, aangevuld met de Supplemental Metrics, Environmental (Modified Base Metrics – Vulnerable System Impact Metrics, Subsequent System Impact Metrics) en Threat Metrics. De CVSS-scores worden berekend op basis van de Base Metrics en vastgelegd met de bijbehorende vector string. Toepassing van Supplemental Metrics, Environmental Metrics en Threat Metrics is niet verplicht.~~

Bewijslast

- P.44** Opdrachtnemer dient de rapportage versleuteld op te slaan. Indien dat in het Plan van Aanpak is overeengekomen, dient Opdrachtnemer ook de scanresultaten, producties en andere resultaten versleuteld op te slaan en op eerste verzoek van Deelnemer ter beschikking te stellen.

De integriteit van alle scanresultaten, producties en overige resultaten is gewaarborgd. Indien dat in het Plan van Aanpak is overeengekomen, heeft Opdrachtnemer alle resultaten gehasht, zodat de inhoud en integriteit van de bestanden geverifieerd kan worden.

Er geldt een minimale bewaartermijn van 3 maanden, berekend vanaf datum van het definitieve standaardrapport. Voor (gerubriceerde) informatie die te beschermen belangen (TBB's) raakt met een rubricering TBB1, 2 of 3 (staatsgeheim) geldt een minimale bewaartermijn van 6 maanden. Partijen maken afspraken over eventueel langere bewaartermijnen. Na afloop van de bewaartermijn verwijdert Opdrachtnemer de gegevens aantoonbaar en op veilige wijze en maakt hier schriftelijk melding van aan Deelnemer.

Validatie scanresultaten

- P.45** Opdrachtnemer levert voor zover redelijkerwijs mogelijk en vast te stellen, op eerste verzoek van Deelnemer, bewijs aan waaruit blijkt dat de scans/testen zijn uitgevoerd op de scope objecten en niet tegen andere beschermende maatregelen (zoals firewalls), die buiten werking gesteld hadden moeten worden om een versturende werking op de scanresultaten te voorkomen. Opdrachtnemer levert dan ook, voor zover redelijkerwijs mogelijk, bewijs aan dat met andere parameters (bijvoorbeeld

IP-adres of intensiteit van scanning) is gevalideerd dat extra beschermende maatregelen voor het onderzoek niet functioneerden tijdens het onderzoek.

Documenteren toegangswegen

- P.46** Opdrachtnemer dient op eerste verzoek van Deelnemer bewijs te kunnen leveren van de gedetecteerde en geïdentificeerde toegangswegen waarmee verbonden kan worden met een onderzocht scope object, ook indien deze niet direct tot een kwetsbaarheid hebben geleid.
- P.47** De rapporteur(s) en overige bij het onderzoek in te zetten professionals van Opdrachtnemer handelen tijdens het onderzoek integer en zoals van een bekwaam beroepsbeoefenaar verwacht mag worden. Als dat niet het geval is, heeft Deelnemer het recht verdere inzet van deze de persoon te weigeren en vervanging te verlangen, zonder dat de Opdrachtnemer aanspraak kan maken op enigerlei schadevergoeding in de breedste zin des woords. De rapporteurs en overige in te zetten professionals proberen onderbrekingen of verstoringen die het gevolg zijn van hun handelen, met ongewenst gevolgen voor de Deelnemer, zoveel als mogelijk te voorkomen.
- P.48** Wanneer Opdrachtnemer tijdens het onderzoek een onvoorziene onderbreking of verstoring veroorzaakt op een scope-object als gevolg van zijn handelen, met ongewenste gevolgen voor de productie-omgeving, staakt hij het onderzoek en maakt hij hiervan direct melding bij de voor dit onderzoek aangewezen contactpersoon van Deelnemer onder vermelding van alle relevante informatie. De contactpersoon van Deelnemer verzorgt de interne communicatie, Opdrachtnemer herstelt de situatie zo spoedig mogelijk. Opdrachtnemer stemt met Deelnemer af of en onder welke voorwaarden het onderzoek kan worden vervolgd.
- P.49** Het is Opdrachtnemer bij een onderzoek niet toegestaan om wijzigingen aan te brengen in de scope-objecten, productiegegevens of systeemconfiguraties die hij aantreft en/of deze te verwijderen, op een manier die de operationele integriteit kan aantasten, tenzij Deelnemer hiervoor expliciete schriftelijke toestemming heeft verleend. Het volgens een tussen Deelnemer en Opdrachtnemer overeengekomen Plan van Aanpak uitvoeren van het onderzoek en daarmee wijzigen van bijvoorbeeld een logbestand als gevolg van automatische registratie van inlogpoging, het wijzigen van sessietokens of uploaden van webshells moet wel mogelijk zijn.
- P.50** Opdrachtnemer laat ten minste de belangrijkste bevindingen die uit geautomatiseerde tests volgen nog handmatig verifiëren of reviewen door de rapporteur(s), door overige bij het onderzoek in te zetten professionals dan wel door ter zake deskundige en gecertificeerde externe reviewer(s). De rapporteur(s) en overige professionals bepalen de eventuele keuze (welke bevindingen wel/niet belangrijk en handmatig verifiëren) op basis van hun expert oordeel over het risico en de impact van de kwetsbaarheid en/of de betrouwbaarheid van de gemelde bevindingen of anders een representatieve steekproef.
- P.51** Opdrachtnemer stemt met Deelnemer af of en welke bevindingen van kwetsbaarheden gemeld worden als CVE-aanvraag (Common Vulnerabilities and Exposures aanvraag) via een Coordinated Vulnerability Disclosure (CVD) formulier/procedure bij een geautoriseerde instantie die als CVE Numbering Authority (CNA) fungeert, zoals het NCSC in Nederland. Opdrachtnemer ondersteunt Deelnemer op verzoek bij deze CVD-melding/CVE-aanvraag. Als de kwetsbaarheid gevonden is in een systeem of product dat niet van Deelnemer maar een rechthebbende derde is, dan stemt Opdrachtnemer met Deelnemer af en ondersteunt hij op verzoek van Deelnemer bij het melden van deze kwetsbaarheid bij deze derde.

Standaardrapport

Rapporteur, opsteller of hoofdonderzoeker

- P.60** In het op te leveren standaardrapport is de naam van een persoon (of meerdere personen) genoemd, die de professionele eindverantwoordelijkheid draagt (of dragen) voor de uitvoering van het informatiebeveiligingsonderzoek en de betreffende rapportage. Deze persoon (of personen) is (of zijn) in het standaardrapport als rapporteur(s) aangemerkt.

Hiernaast vermeldt het standaardrapport de namen van de overige personen die betrokken zijn (geweest) bij de uitvoering van het onderzoek. Indien het standaardrapport kan of zal worden verspreid naar derden (niet zijnde een auditor),

mag Opdrachtnemer hiernaast een inhoudelijk gelijkwaardige 'publieke versie' van het standaardrapport opleveren, waarin hij de namen van deze overige betrokken personen heeft weggelakt of gepseudonimiseerd/geanonimiseerd. Deze publieke versie zal dan voor bredere distributiedoeleinde worden gebruikt. De distributiekring en mate van vertrouwelijkheid van informatie in het standaardrapport hebben Deelnemer en Opdrachtnemer al eerder in het Plan van Aanpak afgesproken. Het toepasselijke rubriceringsniveau wordt in het standaardrapport vermeld.

- P.61** In het standaardrapport wordt bij de rapporteur(s) en de overige professionals die betrokken zijn bij de uitvoering van het onderzoek benoemd over welke relevante en geldige individuele certificeringen zij beschikken.

Opdrachtnemer mag deze informatie uitsluitend in het standaardrapport achterwege laten indien deze al in het Plan van Aanpak is benoemd, de samenstelling van het onderzoeksteam (rapporteur(s) en overige professionals) sindsdien niet veranderd is en Deelnemer goedkeuring heeft gegeven voor het niet laten vermelden van deze informatie in het standaardrapport. In het standaardrapport wordt dan vermeld dat informatie over de individuele certificeringen bij Deelnemer bekend is en in het Plan van Aanpak is opgenomen (of soortgelijke bewoording).

- P.62** Op verzoek van Deelnemer vermeldt Opdrachtnemer in het standaardrapport hoe Deelnemer de aanwezigheid van geclaimde geldige certificering middels inzage in bewijsstukken kan vaststellen. Dat kan bijvoorbeeld door vermelding van (1) een digitale vindplaats met link naar een platform/portaal of bestand of (2) contactgegevens van een persoon die op fysieke of digitale wijze inzage kan geven. Opdrachtnemer mag hierbij kiezen voor het vermelden van een vindplaats met besloten en beveiligde toegang, voor in elk geval de Deelnemer en eventueel een auditor. Opdrachtnemer werkt op eerste verzoek van Deelnemer mee aan het geven van inzage in bewijsstukken. Indien Opdrachtnemer in bezit is van een geldig CCV-keurmerk, kan dit als geldige vervanging van voorgaande bewijsstukken worden gezien.

Versie

- P.63** Het standaardrapport beschikt over een versienummer.

Handtekening

- P.64** Het standaardrapport wordt voorzien van een tekst, waaruit blijkt dat:

1. de rapportage accuraat en naar waarheid is opgesteld;
2. er een review op deze versie van het document heeft plaatsgevonden en welke ter zake deskundige personen (welke onderdelen) hebben gereviewd. Niet-gerubriceerde (niet gevoelige) informatie kan door niet bij het onderzoek betrokken personen worden gereviewd, bij gerubriceerde informatie moet betrokkenheid van externe reviewers door Deelnemer vooraf worden goedgekeurd en kunnen extra maatregelen nodig zijn om vertrouwelijkheid te borgen.

Deze tekst is voorzien van een handtekening van de rapporteur (niet per se ook de reviewers). Deze handtekening kan een fysiek gezette handtekening zijn of een digitale handtekening. Deelnemer kan ook een geavanceerde of gekwalificeerde digitale handtekening verlangen (AES- of QES-authenticatieniveau).

Vertrouwelijkheid

- P.65** Opdrachtnemer legt in beginsel aan het op te leveren standaardrapport en onderliggende documenten geen belemmeringen aan Deelnemer op met betrekking tot het beschikbaar stellen, verspreiden, opslaan en distribueren. Bijvoorbeeld aan rechthebbende derde partijen die eigenaar zijn van onderzochte systemen of applicaties of door Deelnemer ingeschakelde auditors. Deelnemer draagt in zo'n geval de verantwoordelijkheid voor het verder verspreiden van deze informatie en de vertrouwelijkheid hiervan. Eventuele door Deelnemer en Opdrachtnemer gemaakte afspraken over vertrouwelijkheid worden in de rapportage benoemd en gerespecteerd, bijvoorbeeld over het niet verspreiden van financiële informatie over de Opdracht. Opdrachtnemer deelt het standaardrapport niet zonder expliciete toestemming van de contactpersoon van Deelnemer met anderen.
- P.66** Indien van toepassing, vernietigt Opdrachtnemer de gegevens van het standaardrapport en/of onderliggende bestanden na een bepaalde bewaartermijn, volgens de specifieke afspraken die Deelnemer en Opdrachtnemer daarover hebben

gemaakt. Anders gelden hiervoor de wettelijke bewaartermijnen. Vernietiging vindt aantoonbaar en op veilige wijze plaats.

Review

- P.67** Deelnemer kan verlangen dat Opdrachtnemer het standaardrapport in (laatste) conceptvorm aan een of meerdere contactpersonen van Deelnemer ter review aanbiedt, om vast te stellen of het standaardrapport voldoet aan rapportagevereisten en de afspraken in het Plan van Aanpak. Deelnemer onthoudt zich van commentaar waarmee de onafhankelijkheid en integriteit van het standaardrapport kan worden aangetast. Zolang het commentaar niet ziet op het nakomen van eerder overeengekomen rapportagevereisten of afspraken in het Plan van Aanpak, is (zijn) de rapporteur(s) eindverantwoordelijk voor de keuze welk commentaar wel of niet overgenomen wordt in het standaardrapport. Na review en verwerking van aanpassingen kan het standaardrapport worden opgeleverd als definitief.

Hoofdstukindeling

- P.70** Inhoudsopgave - Opdrachtnemer levert op basis van het uitgevoerde onderzoek het standaardrapport op, conform het door Opdrachtgever vastgestelde model in bijlage 2 PvE – Model standaardrapport met standaard hoofd- en paragraafindeling. Dit model moet zorgen voor uniformiteit, transparantie, compleetheid van het standaardrapport en reproduceerbaarheid van het onderzoek. De Opdrachtgever kan nieuwe versies van dit model vaststellen, die Opdrachtnemer daarna dient toe te passen. Opdrachtnemer heeft 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.

- P.71** Methodologie – Het standaardrapport bevat een hoofdstuk methodiek waarin beschreven wordt langs welke fasen en lijnen het onderzoek uitgevoerd is. De fasering van de Pentest Execution Standard (PTES) wordt hierbij als standaard gebruikt, tenzij Deelnemer en Opdrachtnemer expliciet in het Plan van Aanpak een andere, vergelijkbare erkende industriestandaard zijn overeengekomen, welke in de methodiek beschreven is.
- P.72** CVSS - Het standaardrapport bevat een subhoofdstuk binnen het hoofdstuk methodiek - waarin beschreven wordt dat de bevindingen welke door onderzoekers gedaan worden, geclassificeerd worden middels het Common Vulnerability Scoring System en worden voorzien van een zogenoemde CVSS-vector string teneinde terug te kunnen leiden hoe de calculatie van de score tot stand gekomen is. De gebruikte CVSS-versie wordt expliciet vermeld.
- P.73** Documentbeheer - Het standaardrapport bevat een (sub)hoofdstuk over het document (documentbeheer) - in dit hoofdstuk wordt tenminste gedefinieerd: Deelnemer, projectnummer/naam, start- en einddatum van project, rapporteurs, reviewers, document classificatie, rubricering, versie-nummer van het document en de handtekening van de verantwoordelijke rapporteur.
- P.74** Versiebeheer - Het standaardrapport bevat een (sub)hoofdstuk over versie-beheer, in dit hoofdstuk wordt tenminste gedefinieerd (per versie): versie, datum, auteur en versie-omschrijving.
- P.75** Distributielijst - Het standaardrapport bevat een (sub)hoofdstuk inzake de distributielijst - in dit hoofdstuk wordt tenminste gedefinieerd: versie, datum, naam, organisatie en verspreidingsmethode. Indien een publieke versie wordt opgesteld, wordt dit expliciet vermeld.
- P.76** Aanleiding - Het standaardrapport bevat een (sub)hoofdstuk waarin de aanleiding van het onderzoek beschreven is, hierbij wordt minimaal beschreven: of er sprake is van een timeboxed test en indien dit het geval is, wat de maximering van de uren betreft, welke onderdelen niet (volledig) konden worden getest en waarom niet, een algemene beschrijving van de te testen omgevingen van Deelnemer.
- P.77** Doelstelling - Het standaardrapport bevat de doelstelling(en) die overeenkomt (overeenkomen) met wat tijdens de intake is besproken en is opgenomen in het definitieve Plan van Aanpak.

P.78 Bevindingenlijst en bevindingen - Het standaardrapport bevat een genummerde lijst van bevindingen en verwijst naar de individuele bevindingen. Zie ook de eisen P.90 tot en met P.97.

P.79 Managementsamenvatting - Het standaardrapport bevat een managementsamenvatting. Deze is als volgt opgebouwd:

- Start/einddatum - De managementsamenvatting bevat een start- en einddatum van het onderzoek.
- Gebruikte standaarden - De managementsamenvatting bevat een overzicht van de gebruikte standaarden tijdens het onderzoek.
- CIA-scores - Op verzoek van Deelnemer bevat de managementsamenvatting een overzicht van de CIA-scores per scope-object.
- RCA - De managementsamenvatting bevat - indien zinvol en met voldoende context beschikbaar - een root-cause analyse op basis van de informatie verkregen uit het onderzoek en de bevindingen.
- Overige bevindingen - De managementsamenvatting bevat een overzicht van de door rapporteur aangetroffen kwetsbaarheden (aantal bevindingen per risico-categorie) - op basis van het Common Vulnerability Scoring System - CVSS - waarbij de volgende categorieën worden gehanteerd: Kritiek, Hoog, Gemiddeld, Laag en Informatief (zoals gedefinieerd door FIRST).
- Opdrachtnemer geeft een samenvatting van de belangrijkste bevindingen en zijn aanbevelingen aan Deelnemer voor verbetering.

P.85 Scope - Het standaardrapport bevat:

- Een overzicht van de scope-objecten, waarbij per scope-object aangegeven wordt of deze getest is en indien er afwijkingen zijn wordt er per scope-object beschreven wat deze afwijkingen behelzen.
De scope die is besproken in het intakegesprek en is vastgelegd in het definitieve Plan van Aanpak.

P.87 Assume breach - Het standaardrapport bevat een (sub)hoofdstuk waarin beschreven is of er middels het assume breach principe getest wordt en hoe de validatie van het toepassen van het principe vastgesteld is door Opdrachtnemer.

P.88 Locaties - Het standaardrapport bevat de fysieke locaties (land) van de onderzochte objecten, de fysieke locaties van uitvoering van het onderzoek en vaststelling dat het onderzoek volgens de aldaar van toepassing zijnde wet- en regelgeving is uitgevoerd.

P.89 Tijdslijn - Het standaardrapport bevat een tijdslijn waarin aangegeven wordt welke acties er op welk moment in de tijd (tijdens de testperiode) uitgevoerd zijn, zodat op een later moment de acties en impact daarvan geverifieerd en kan worden, bijvoorbeeld voor een audit of forensisch onderzoek. Deelnemer en Opdrachtnemer stemmen af welke detailniveau hierbij wenselijk is. Kritieke acties worden in beginsel op de tijdslijn vermeld.

Hoofdstuk - Bevindingen

P.90 Het standaardrapport bevat een hoofdstuk waarin de bevindingen van het onderzoek zijn beschreven.

P.91 In het standaardrapport dient er per opgenomen bevinding een scope-object te worden gedefinieerd - dit scope-object dient direct herleidbaar te zijn naar het systeem, de omgeving of applicatie (of directe URL) waarbinnen de kwetsbaarheid zich bevindt.

P.92 In het standaardrapport dient er per opgenomen bevinding een CVSS-score te worden gedefinieerd, tezamen met een CVSS-classificatie, bij voorkeur volgens de meest recente standaard (<https://www.first.org/cvss/v4.0/specification-document> - 6. Qualitative Severity Rating Scale).

P.93 In het standaardrapport dient er per opgenomen bevinding een CVSS-vector string te worden verstrekt, bij voorkeur volgens de meest recente standaard (<https://www.first.org/cvss/v4.0/specification-document> - 7 Vector String).

P.94 In het standaardrapport dient er per opgenomen bevinding een beschrijving van de kwetsbaarheid te worden opgenomen, waarbij indien beschikbaar gerefereerd wordt naar externe bronnen (zoals bijvoorbeeld CVE-nummers, public advisories).

~~In het standaardrapport worden indien van toepassing ook AI-gegenereerde kwetsbaarheden gesignaleerd. In het standaardrapport worden, indien van~~

toepassing, ook met behulp van AI-tooling geïdentificeerde kwetsbaarheden gesignaleerd.

- P.95** In het standaardrapport dient er per opgenomen bevinding een bevestiging van de kwetsbaarheid te worden opgenomen, waarbij expliciet opgenomen staat hoe de kwetsbaarheid kan worden gereproduceerd, of er gebruik gemaakt is van een publieke exploit, of er door middel van misbruik van de kwetsbaarheid toegang is verkregen tot het systeem en/of beschikbare informatie.
- P.96** In het standaardrapport dient er per opgenomen bevinding een mogelijke impact te worden beschreven, inclusief mogelijke uitbuiting van de kwetsbaarheid (exploitability). Daarbij dient ook rekening te worden gehouden met de impact op omliggende omgevingen/systemen en ketens welke een relatie hebben tot het scope-object.
- P.97** In het standaardrapport dient er per opgenomen bevinding een aanbeveling te worden geschreven inzake hoe een kwetsbaarheid kan worden opgelost. Daarbij dient er (indien deze van toepassing is) een klikbare (link) te worden opgenomen naar een individuele toevoeging in de Common Weakness Enumeration (CWE) database welke bij de kwetsbaarheid hoort.

Bijlagen

- P.100** Het standaardrapport bevat een hoofdstuk waarin bijlages opgenomen worden.
- P.101** Woordenlijst - Het standaardrapport bevat, bij voorkeur in de bijlagen, een verklarende woordenlijst.
- P.102** Hulpmiddelen - Het standaardrapport bevat, bij voorkeur in de bijlagen, een opsomming van gebruikte hulpmiddelen (tooling) tijdens het onderzoek.
- P.103** Beschrijving - Per gebruikt hulpmiddel wordt een beschrijving opgenomen. De beschrijving blijft beperkt tot functionaliteit en toepassingsdoel, niet tot technische werking.
- P.104** Versienummer - Per gebruikt hulpmiddel wordt een specifiek versienummer opgenomen welke overeenkomt met de versie van het ingezette hulpmiddel.
- P.105** Publieke referentie - Per gebruikt hulpmiddel wordt een publieke referentie (URL) opgenomen waar het specifieke hulpmiddel kan worden verkregen (download/informatie website).

Ontvangen documenten

- P.110** Op verzoek van Deelnemer bevat het standaardrapport, bij voorkeur in de bijlagen, een lijst met ALLE door Opdrachtnemer ontvangen documenten, inclusief bestandsnaam.
- P.111** Op verzoek van Deelnemer wordt per ontvangen document een beschrijving opgenomen van het specifieke document.
- P.112** Op verzoek van Deelnemer wordt per ontvangen document een cryptografische hash (zoals SHA2, SHA3) berekend en opgenomen om de integriteit en authenticiteit te kunnen controleren, als en voor zover Opdrachtnemer en Deelnemer dat in het Plan van Aanpak zijn overeengekomen.

Ontvangen bestanden

- P.120** Op verzoek van Deelnemer bevat het standaardrapport, bij voorkeur in de bijlagen, een lijst met ALLE door Opdrachtnemer ontvangen bestanden, inclusief bestandsnaam.
- P.121** Op verzoek van Deelnemer wordt per ontvangen bestand een beschrijving opgenomen van het specifieke bestand.
- P.122** Op verzoek van Deelnemer wordt per ontvangen bestand een cryptografische hash (zoals SHA2, SHA3) berekend en opgenomen om de integriteit en authenticiteit te kunnen controleren, als en voor zover Opdrachtnemer en Deelnemer dat in het Plan van Aanpak zijn overeengekomen.

Gebruikte accounts

- P.130** Het standaardrapport bevat, bij voorkeur in de bijlagen, een lijst met de door Deelnemer verstrekte accounts.

- P.131** Per opgenomen account wordt het bijbehorende scope-object beschreven.
- P.132** Per opgenomen account wordt een beschrijving en rol/een korte beschrijving van permissies opgenomen.

Uitgevoerde scans

- P.140** Op verzoek van Deelnemer bevat het standaardrapport, bij voorkeur in de bijlagen, de scanresultaten (scan output) van de uitgevoerde scans. Indien scanresultaten zeer omvangrijk zijn, kan een representatieve selectie worden opgenomen mits overeengekomen.
- P.141** Op verzoek van Deelnemer wordt per scan-resultaat het scope-object gedefinieerd
- P.142** Op verzoek van Deelnemer wordt per scan-resultaat de ruwe scan-output opgenomen, inclusief versie van de gevonden componenten (software, libraries etc.).

Bewijsmateriaal

- P.150** Op verzoek van Deelnemer bevat het standaardrapport, bij voorkeur in de bijlagen, een lijst met alle door Opdrachtnemer gecreëerde/gegenereerde informatie, welke dient als bewijsmateriaal. Voorbeelden hiervan zijn state-files (Burp), Nessus scans, nmap scans, testssl.sh scans en elke andere output behorende tot het onderzoek.
- P.151** Op verzoek van Deelnemer wordt per bestand dat behoort tot het bewijsmateriaal een cryptografische hash (zoals SHA2, SHA3) berekend en opgenomen om de integriteit en authenticiteit te kunnen controleren, als en voor zover Opdrachtnemer en Deelnemer dat in het Plan van Aanpak waren overeengekomen.

Checklists

- P.160** Op verzoek van Deelnemer bevat het standaardrapport, bij voorkeur in de bijlagen, de checklists voor de standaarden die van toepassing zijn op het onderzoek.
- P.161** Binnen deze checklist dient dan elke test te worden afgevinkt, waarbij er drie verschillende statussen mogelijk zijn:
1. Getest.
 2. Niet getest.
 3. Valt niet te testen (functionaliteit afwezig).

Indien er een bevinding is, dient deze bij de individuele check te worden opgenomen als afwijking.

Indien een check niet getest is, dient dit te worden gemarkeerd (b.v. rode kleur) en dient toelichting te worden gegeven waarom een test niet uitgevoerd is.

Onbenaderbare/onbereikbare scope-objecten

- P.170** In het standaardrapport, bij voorkeur in de bijlagen, wordt beschreven of er scope-objecten ten tijde van het onderzoek technisch niet bereikbaar waren. Daarbij wordt beschreven welke scope-objecten dit betroffen en hoe is vastgesteld dat deze objecten technisch niet benaderbaar/bereikbaar waren. Indien relevant wordt vermeld welke impact dit had op de volledigheid van het onderzoek.

Artificiële Intelligentie (AI)

De eisen AI.1 tot en met AI.6 gelden voor AI-functionaliteit die wordt gebruikt bij de uitvoering van de betreffende Nadere overeenkomst of die van invloed is op het te leveren resultaat. Algemeen beschikbare kantoorfunctionaliteit en uitsluitend intern gebruikte hulpmiddelen vallen buiten de reikwijdte voor zover zij geen informatie van Deelnemer verwerken en geen materiële invloed hebben op de uitvoering of het resultaat. Opdrachtnemer verstrekt relevante, proportionele en redelijkerwijs beschikbare informatie over zijn eigen AI-gebruik. Iedere partij blijft verantwoordelijk voor de eigen verplichtingen op grond van toepasselijke wet- en regelgeving.

- AI.1** In iedere Offerte voor een Nadere overeenkomst maakt Opdrachtnemer, gevraagd of ongevraagd, transparant hoe hij omgaat met de inzet of het gebruik van AI-functionaliteit binnen de Opdracht, in lijn met de AI-verordening*:

AI.2

Opdrachtnemer geeft aan of AI-functionaliteit wordt ingezet of gebruikt en, indien van toepassing, waar deze inzet een rol speelt:

- in het eigen voortbrengingsproces, en/of
- in het aan Deelnemer te leveren resultaat (dienstverlening en/of product).

AI.3

~~Opdrachtnemer maakt inzichtelijk welke verantwoordelijkheden van Deelnemer uit hoofde van wet- en regelgeving, in het bijzonder de AI-verordening, aan de orde zijn en in de Opdracht of uitvoering moeten worden geadresseerd.~~ Opdrachtnemer verstrekt relevante, proportionele en redelijkerwijs beschikbare informatie over zijn eigen AI-gebruik die Deelnemer ondersteunt bij het vaststellen en invullen van diens verantwoordelijkheden uit hoofde van wet- en regelgeving, in het bijzonder de AI-verordening. Deelnemer blijft verantwoordelijk voor die vaststelling en invulling.

AI.4

Opdrachtnemer beschrijft hoe hij zijn eigen verantwoordelijkheden rond de inzet of het gebruik van AI beheerst en risico's mitigeert, mede afgezet tegen relevante normen zoals ISO 42001:2023.

AI.5

~~Opdrachtnemer maakt inzichtelijk hoe de inzet of het gebruik van AI-functionaliteit Deelnemer in staat stelt aan zijn wettelijke en organisatorische verantwoordelijkheden te voldoen, waaronder begrip van werking, output en beperkingen.~~ Opdrachtnemer verstrekt relevante, proportionele en redelijkerwijs beschikbare informatie over de werking, output en beperkingen van de door hem ingezette of geleverde AI-functionaliteit, ter ondersteuning van Deelnemer bij het invullen van diens wettelijke en organisatorische verantwoordelijkheden.

AI.6

Opdrachtnemer benoemt eventuele aandachtspunten voor Deelnemer met betrekking tot diens AI-verantwoordelijkheden bij het gebruik van het op te leveren resultaat (dienstverlening en/of product).

Post Quantum Cryptografie

Generiek toepassingskader PQC.1 – PQC.4

PQC.1 tot en met PQC.4 zijn van toepassing op ieder Informatiebeveiligingsonderzoek, tenzij Opdrachtgever in de Aanvraag uitdrukkelijk bepaalt dat PQC niet aan de orde is. Het ontbreken van een expliciete verwijzing naar post-quantumcryptografie, quantumveiligheid of cryptografie geldt niet als uitsluiting. Opdrachtnemer beoordeelt actief of PQC redelijkerwijs relevant is en wijst Opdrachtgever onverwijld op een mogelijke omissie of onjuiste uitsluiting. Bij twijfel zijn PQC.1 tot en met PQC.4 van toepassing.

PQC.1

Opdrachtnemer is actief gericht op mogelijke quantumtechnologie (QT) risico's in hun producten en/of diensten en het ondersteunen van Opdrachtgever in de beweging richting 'crypto agility' en quantumveilige cryptografie, conform richtlijnen van de AIVD en het NCSC en anticiperend op in ontwikkeling zijnde wet- en regelgeving (o.a. de implementatie van de NIS2 richtlijn met de Cyberbeveiligingswet).

'Actief gericht zijn' zoals hierboven gesteld betekent dat Opdrachtnemer Quantum-risico's kenbaar en aantoonbaar in zijn bedrijfsvoering, kwaliteitssysteem, productontwikkeling, dienstverlening heeft geïncorporeerd.

Onder Opdrachtnemers wordt in het kader van PQC ook begrepen: iedere betrokken derde in de gehele keten van door Opdrachtgever gecontracteerde of te contracteren diensten.

Opdrachtnemer draagt de ketenverantwoordelijkheid en staat ervoor in dat iedere voor een Nadere overeenkomst in de keten ingeschakelde derde geheel voldoet -en gedurende de looptijd van de Nadere overeenkomst blijft voldoen- aan de op Opdrachtnemer rustende verplichtingen.

~~PQC-eisen zijn alleen van toepassing indien cryptografie onderdeel is van de scope van het Informatiebeveiligingsonderzoek.~~

- PQC.2** Opdrachtnemer heeft concreet toetsbare in zijn organisatie geborgde relevante activiteiten rond quantumveiligheid, die minimaal adresseren:
1. De concrete maatregelen op korte (maximaal 6 maanden) en middellange termijn (maximaal 1 jaar) die Opdrachtnemer neemt om in Opdrachten waarin cryptografie aan de orde is, de quantumveiligheid te kunnen bedienen.
 2. Risicomanagement
 3. Maatregelen/voorzieningen met betrekking tot compliance.
 4. Anticiperen op juridische implicaties.
 5. Overige relevante ontwikkelingen ten aanzien van quantumveiligheid en cryptografie.

~~Indien cryptografie geen onderdeel is van de Opdracht, volstaat een verklaring van niet-toepasselijkheid.~~ Indien Opdrachtgever PQC in de Aanvraag uitdrukkelijk heeft uitgesloten overeenkomstig het generieke toepassingskader, volstaat een verklaring van niet-toepasselijkheid. De actieve toetsings- en signaleringsplicht uit dat kader blijft gelden.

- PQC.3** Uitwerkingen van de activiteiten als bedoeld in PQC.2 zijn gebaseerd op en in lijn met de actuele versie van:
- NIST PQC project: <https://csrc.nist.gov/projects/post-quantum-cryptography>
 - PQC migratie handboek van de AIVD: <https://www.aivd.nl/onderwerpen/informatiebeveiliging/documenten/publicaties/2024/12/3/het-pqc-migratie-handboek>
 - NCSC TLS richtlijnen: <https://www.ncsc.nl/wat-kun-je-zelf-doen/documenten/publicaties/2025/juni/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2025-05>
- Vigerende wet- en regelgeving rondom Quantumveiligheid en cryptografie (zoals de Cyberbeveiligingswet) en het Rijksbrede beleidskader cryptografie: <https://www.digitaleoverheid.nl/document/rijksbreed-beleidskader-cryptografie/>. Opdrachtnemer past deze bronnen alleen toe voor zover relevant voor de aard van het Informatiebeveiligingsonderzoek.

- PQC.4** Opdrachtnemer levert halfjaarlijks een geactualiseerd overzicht van de activiteiten rond relevante quantumveiligheid op aan Opdrachtgever. ~~Indien PQC niet relevant is voor het Informatiebeveiligingsonderzoek, volstaat een jaarlijkse verklaring van ongewijzigde status.~~ Indien Opdrachtgever PQC in de Aanvraag uitdrukkelijk heeft uitgesloten overeenkomstig het generieke toepassingskader, vervalt de halfjaarlijkse rapportageplicht en volstaat een jaarlijkse verklaring van ongewijzigde status.

Hoofdstuk 3 - Eisen aan het aanvraagproces

- AP.01** Deelnemer classificeert de betreffende (verzameling van) informatiebeveiligingsonderzoek(en) volgens de classificatiematrix in Bijlage 1 van dit Programma van Eisen. De door Deelnemer bepaalde classificatie geldt als begrenzing van de scope of omvang van de betreffende Aanvraag voor een (verzameling van) informatiebeveiligingsonderzoek(en).
- AP.02** In het geval sprake is van een Aanvraag voor een verzameling van informatiebeveiligingsonderzoeken, dan is het proces van classificatie eender en wordt de scope en de totale omvang bepaald en altijd uitgedrukt met de (verzameling van) classificatie(s), met dit verschil dat de totale omvang van deze Opdracht een maximum is en niet wordt overschreden. Afwijkingen van de aard in de afroep en uitvoering van een informatiebeveiligingsonderzoek binnen een dergelijke Opdracht zijn afhankelijk van de proportionaliteit en omstandigheden van het geval.
- AP.1.1** Deelnemer kan Opdrachtnemer in RVICTO-PT-veld gedurende de looptijd van deze Raamovereenkomst steeds opnieuw oproepen via minicompentie tot het uitbrengen van een Offerte op basis van een Aanvraag:
- Voor **afzonderlijke** Opdrachten met een classificatie "Groot" en/of "**Speciaal**";
 - Voor een verzameling van Opdrachten ongeacht de classificatie met een gezamenlijke opdrachtwaarde van > €25.000 excl. btw.
- AP.1.2** Deelnemer kan Opdrachtnemer in RVICTO-PT-veld en Opdrachtnemer in RVICTO-PT-bank gedurende de looptijd van deze Raamovereenkomst steeds opnieuw oproepen tot het uitbrengen van een Offerte op basis van een Aanvraag volgens het toerbeurtschema:
- Voor **afzonderlijke** Opdrachten met een classificatie "Klein" en /of "Normaal";
 - Voor een verzameling van Opdrachten ongeacht de classificatie met een gezamenlijke opdrachtwaarde van ≤ €25.000 excl. btw.

Hierbij geldt het volgende:

1. De inkoopafdeling die namens een Deelnemer of meerdere Deelnemers Aanvragen uitzet, stelt het toerbeurtschema op en bepaalt voor welke Deelnemer(s) dit schema van toepassing is en houdt dit actueel bij;
2. In dit schema worden alle Opdrachtnemers RVICTO-PT-veld en RVICTO-PT-bank opgenomen en wordt per Aanvraag geregistreerd welke Opdrachtnemer aan de beurt is om de Aanvraag te ontvangen. De volgorde van Opdrachtnemers in het toerbeurtschema wordt vastgesteld op basis van de definitieve rangorde bij de gunning van de Raamovereenkomst, waarbij de hoogst gerangschikte Opdrachtnemer als eerste aan de beurt is. Voor iedere opvolgende Aanvraag die volgens het toerbeurtschema moet worden uitgezet, wordt de eerstvolgende Opdrachtnemer in de vastgestelde volgorde uitgenodigd. Nadat alle Opdrachtnemers aan de beurt zijn geweest, begint de toerbeurtcyclus opnieuw bij de eerst gerangschikte Opdrachtnemer. Afwijking van deze volgorde is uitsluitend toegestaan in de gevallen zoals bepaald in dit Programma van Eisen bij AP1.2 punt 5 en AP.4 en AP.11.
3. In dit schema staan ten minste de volgende gegevens geregistreerd: volgorde van Opdrachtnemers, datum en kenmerk Aanvraag, de Opdrachtnemer die Aanvraag heeft ontvangen, informatie de gunning, bijzonderheden;
4. Indien Opdrachtnemer geen Offerte wenst uit te brengen, niet tijdig reageert of een ongeldige Offerte indient, wordt de betreffende Aanvraag aangeboden aan de eerstvolgende Opdrachtnemer in het toerbeurtschema;
5. Indien Deelnemer een Aanvraag aanvankelijk aan Opdrachtnemer toekent, maar voor gunning intrekt en daarom geen Nadere overeenkomst wordt gegund, behoudt de Opdrachtnemer die op basis van het toerbeurtschema was uitgenodigd zijn positie als eerstvolgende in de volgorde. **Ook indien de Nadere overeenkomst na de intake wegens een onjuiste classificatie wordt ontbonden overeenkomstig AP.18, wordt de toerbeurtpositie van de aanvankelijk geselecteerde Opdrachtnemer niet verbruikt of gewijzigd. Dit geeft geen automatisch recht op de opnieuw uitgezette Opdracht.**

Het toerbeurtschema is transparant en wordt door de inkoopafdeling van Deelnemer op verzoek van Opdrachtnemer ter inzage verstrekt binnen vijf (5) werkdagen na ontvangst van dit verzoek.

Deelnemer is verantwoordelijk voor het correct toepassen en bijhouden van het toerbeurtschema.

AP.2 Opdrachtnemer stelt één (1) e-mailadres of contactpunt (in geval van gebruik van digitaal systeem) beschikbaar waarnaar alle Aanvragen gezonden kunnen worden door Deelnemer. De goede werking daarvan is de verantwoordelijkheid van Opdrachtnemer.

AP.3 Een Aanvraag voor een Nadere overeenkomst op basis van een resultaatverplichting bevat ten minste:

1. Aanvraag kenmerk
2. Ministerie
3. Deelnemer
4. Organisatieonderdeel
5. Contactgegevens aanvrager
6. Classificatie van de Opdracht conform de classificatiematrix en de opdrachtoomschrijving **waarbij in ieder geval duidelijk wordt benoemd:**
 - a) Aantal en type scope-objecten
 - b) Indicatieve aantallen (URL's, endpoints, rollen, systemen),
 - c) Aanvalsperspectief (black, grey of whitebox),
 - d) De te testen omgeving (ontwikkel, test, acceptatie of productie)
 - e) De toe te passen normenkaders
 - f) de beschikbaarheid van testaccounts en whitelisting
 - g) Welke optionele onderdelen van het standaardrapport (eisen P.110 tot en met P.170) Deelnemer verlangt
7. Aanvullende eisen t.a.v. de Offerte en/of uitvoering van de Nadere overeenkomst
8. Beoogde testperiode
9. Prijs
10. Beoordelingsmethodiek inclusief gunningscriterium en subgunningscriteria
11. Termijn voor het indienen van een Offerte

In een Aanvraag voor een Nadere overeenkomst op basis van een resultaatverplichting kan optioneel nog het volgende worden opgenomen:

12. Datum informatiesessie/intakegesprek/pré-bid meeting
13. Of voor het in te zetten Personeel van Opdrachtnemer een geheimhoudings- /integriteitsverklaring, VOG en eventueel nog een Verklaring van Geen Bezwaar (VGB) overgelegd moet worden
14. De locatie van uitvoering voor de Opdracht (intern bij Deelnemer of extern bij Opdrachtnemer)
15. Mogelijkheid van een herhalingsopdracht/hertest
16. Of de Algemene Beveiligingseisen voor Rijksoverheidsopdrachten (ABRO) van toepassing is op de Opdracht en zo ja, welke hoofdstukken, welk (rubricerings- of TBB-niveau en eventueel op welk gedeelte van de Opdracht dit ziet.
17. Eisen ten aanzien van inzet onderaannemers/derden
18. AI-aspecten en/of PQC aspecten
19. Of cyberbeveiligingsafspraken van toepassing zijn op de Opdracht (zie NOK)
20. Of de maximumtarieven voor deze Opdracht buiten werking worden gesteld, e.e.a. conform eis T.3

AP.4 Indien zich een situatie voordoet waarbij Deelnemer in het kader van de Aanvraag passende maatregelen moet treffen in het kader van de nationale veiligheid, heeft Deelnemer het recht om van de eisen AP1.1 en AP1.2 af te wijken en een Aanvraag op alternatieve en passende wijze uit te zetten onder één of meerdere Opdrachtnemers waarmee deze Raamovereenkomst

is gesloten. Voorts kan de nationale veiligheid er tevens toe leiden dat een Opdracht buiten scope van deze Raamovereenkomst wordt gekwalificeerd door Deelnemer.

- AP.5.1** Voorafgaand aan een Aanvraag kan Deelnemer een informatiesessie of een pre-bid meeting organiseren met alle Opdrachtnemers en een toelichting geven op de voorgenomen Aanvraag en de procedure.
Deelnemer geeft daarbij een toelichting op de context/achtergrond van de Opdracht. Vragen stelt Opdrachtnemer tijdens de vragenronde(n).
- AP.5.2** Opdrachtnemer valideert de classificatie bij ontvangst van de Aanvraag. Indien Opdrachtnemer meent dat de classificatie niet overeenkomt met de aard en omvang van de Opdracht meldt hij dit bij Deelnemer:
- Uiterlijk 2 werkdagen na datum Aanvraag voor een Opdracht met classificatie "Klein" en/of "Normaal"
 - Uiterlijk 5 werkdagen na datum Aanvraag voor een Opdracht met classificatie "Groot" en/of "Speciaal".
 - Indien Opdrachtnemer niet tijdig reageert, wordt de classificatie geacht te zijn geaccepteerd.
- AP.5.3** Deelnemer herijkt hierop de classificatie en past ofwel de scope aan, dan wel de classificatie, dan wel motiveert waarom de gegeven classificatie in ogen van de Deelnemer juist is. In alle gevallen zendt Deelnemer dit bericht aan alle Opdrachtnemers in de minicompetitie of aan de Opdrachtnemer die op basis van het toerbeurtschema de Aanvraag heeft ontvangen. Deelnemer past indien nodig ook de termijn voor het indienen van Offertes aan.
- AP.5.4** Bij aanpassing van de scope of classificatie trekt Deelnemer de Aanvraag in en zet de Deelnemer de Aanvraag opnieuw in minicompetitie uit of herstart de Aanvraag via het toerbeurtschema. Het bericht zoals genoemd in AP.5.3 kan tegelijkertijd worden gezonden met de herstart van de minicompetitie of de Aanvraag via het toerbeurtschema.
- AP.6** Deelnemer is gerechtigd een Aanvraag gemotiveerd in te trekken zonder tot gunning over te gaan. Deelnemer hoeft Opdrachtnemer hiervoor niet schadeloos te stellen of te compenseren, in welke vorm dan ook.
- AP.7** Gunning van een Nadere overeenkomst vindt altijd plaats op basis van de beste prijs/kwaliteitsverhouding. De gunningscriteria prijs en kwaliteit worden op basis van onderstaande subgunningscriteria (al dan niet aangevuld met de optionele sub-gunningscriteria) door Deelnemer gehanteerd:

Prijs:
<u>FINANCIEEL</u> Vaste totaalprijs excl. btw. (onderbouwing van de prijs kan onderdeel zijn van de beoordeling van de kwaliteit van de prijs. E.e.a. per Aanvraag te bepalen)
Kwaliteit:
<u>ORGANISATIE</u> Plan van Aanpak o.a. conform P.24.
<u>PERSONEEL</u> Deskundigheid, samenstelling/skills van in te zetten personen inclusief onderbouwing waarom deze personen worden ingezet. NB: bij een Aanvraag voor meerdere informatiebeveiligingsonderzoeken kan worden volstaan met anonieme profielen voor zover concrete personen niet kunnen worden opgegeven e.e.a. naar de omstandigheden van het geval en de Aanvraag.

Deelnemer zal de onderlinge weging per Aanvraag aangeven. De totale weging is 100%.

AP.8 ~~Opdrachtnemer brengt binnen het in de Aanvraag gestelde aantal dagen een Offerte uit aan Deelnemer conform de in de Aanvraag afgesproken procedure.~~ Indien Opdrachtnemer besluit een Offerte uit te brengen, dient hij deze binnen de in de Aanvraag gestelde termijn en conform de daarin afgesproken procedure bij Deelnemer in. De in de Aanvraag gestelde termijn is een Fatale termijn.

De richtlijn voor de termijnen die Deelnemer hanteert voor het indienen van Offertes (elektronisch aangeleverd) zijn:

- 10 werkdagen voor Opdrachten met de classificatie "Klein" en/of "Normaal".
- 15 werkdagen voor Opdrachten met de classificatie "Groot".
- NTB in de Aanvraag voor Opdrachten met de classificatie "Speciaal".

AP.9 Opdrachtnemer is verplicht om formeel schriftelijk op de Aanvraag te reageren:

- door het indienen van een Offerte of
- door een mededeling dat Opdrachtnemer geen Offerte uitbrengt voorzien van een deugdelijke motivering

AP.10 Indien de formeel schriftelijke reactie zoals bedoeld in AP.9 niet binnen de in eis AP.8 gestelde termijn door Deelnemer is ontvangen of deze niet voldoet aan de daaraan gestelde eisen dan wordt Opdrachtnemer geacht geen Offerte te hebben gedaan.

AP.11 Opdrachtnemer voorkomt te allen tijde dat er sprake is van (kans op) belangenverstrengeling bij een Aanvraag of de uitvoering van een Nadere overeenkomst.

In geval van (mogelijke/vermoedelijke) belangenverstrengeling:

- vraagt de Opdrachtnemer de Deelnemer direct na ontvangst van de Aanvraag om een gemotiveerd verzoek tot vrijstelling van deelname aan de minicompetitie of Aanvraag op basis van het toerbeurtschema. De Deelnemer kan dit verzoek goedkeuren of het verzoek afwijzen.
- kan een Deelnemer besluiten om een Opdrachtnemer niet voor een minicompetitie of Aanvraag op basis van het toerbeurtschema uit te nodigen, waarvan hij de betreffende Opdrachtnemer(s) daarvan vooraf verzending van de Aanvraag gemotiveerd bericht zal geven
- meldt Opdrachtnemer tijdens uitvoering van de Opdracht mogelijke belangenverstrengeling zodra deze bekend wordt.

AP.12 De Offerte omvat ten minste:

- De vaste totaalprijs van de Opdracht;
- Het Plan van Aanpak e.e.a. conform de informatie in de Aanvraag;
- Opbouw onderzoeksteam en in te zetten personen;
- De bij de Opdracht in te zetten onderaannemers/derden (toeleveranciers) en hun beoogde bijdrage aan de uitvoering van de Opdracht (indien geen onderaannemers worden ingezet, vermeldt Opdrachtnemer dit expliciet in de offerte).

AP.13 Deelnemer beoordeelt de Offerte op basis van de in de Aanvraag vastgestelde criteria en informeert Opdrachtnemer over de uitkomst daarvan. Offertes die niet aan de gestelde eisen voldoen, worden niet beoordeeld en uitgesloten. Deelnemer kan, in geval van twijfel of onduidelijkheid over de gestelde eisen, besluiten een Offerte (gemotiveerd) toch te beoordelen en de Offerte niet uit te sluiten. Een afwijzing van de Offerte wordt gedaan onder vermelding van de relevante redenen.

AP.14 Offertes met optionele prijzen of prijzen die niet in overeenstemming zijn met de Aanvraag of de Raamovereenkomst worden aangemerkt als 'voorwaardelijke Offertes' en leiden tot uitsluiting en het niet verder beoordelen van die Offertes. Dit geldt ook voor Offertes waarin essentiële onderdelen ontbreken.

AP.15 Opdrachtnemer is verplicht de Offerte met betrekking tot de voorwaarden, prijzen en beschikbaarheid van capaciteit gestand te doen, tenzij na een periode van vier (4) weken, gerekend vanaf het uiterste moment van sluiting van de inschrijftermijn, geen gunningsbeslissing is genomen.

Deelnemer kan bij een Aanvraag een afwijkende gestanddoeningstermijn verlangen.

Bij (Bijzondere) Opdrachten waarop de ABRO van toepassing is, kan Deelnemer een gestanddoeningstermijn verlangen waarmee rekening wordt gehouden met de termijn van het onderzoek dat NBIV nodig heeft voor het al dan niet afgeven van een ABRO-Verklaring. Deelnemer houdt hierbij rekening met het proportionaliteitsbeginsel en zal de dan verlangde (afwijkende) gestanddoeningstermijn in de Aanvraag specificeren.

- AP.16** Bij mededeling van de uitkomst van de beoordeling kan Deelnemer een redelijke termijn aanhouden alvorens de Nadere overeenkomst te sluiten. In voorkomend geval wordt dit vermeld in de mededeling van de uitkomst van de beoordeling.
- AP.17** Indien de in de Aanvraag genoemde Opdracht door Deelnemer aan Opdrachtnemer wordt gegund, is Opdrachtnemer verplicht die Opdracht uit te voeren overeenkomstig de voorwaarden van deze Raamovereenkomst. Daartoe is Opdrachtnemer alsdan verplicht met Deelnemer een Nadere overeenkomst te sluiten.
- AP.18** Na gunning van de Nadere overeenkomst blijft de scope binnen de gegunde classificatie. Indien Deelnemer en/of Opdrachtnemer tijdens de intake vaststelt dat de classificatie niet passend is voor de scope, dan ontbindt de Deelnemer de Nadere overeenkomst en wordt de betreffende Opdracht voor een informatiebeveiligingsonderzoek met de nieuwe inzichten opnieuw uitgezet conform de eisen AP.1.1 en AP.1.2. **Uitsluitend in deze situatie heeft de Opdrachtnemer recht op een vergoeding van de Deelnemer en factureert de duur van de intakebijeenkomst vermenigvuldigd met het aangeboden tarief/tarieven in de Offerte van de personen die namens Opdrachtnemer aanwezig zijn geweest bij de intake.**
- AP.19** Indien geen van de door Deelnemer tot mededinging opgeroepen Opdrachtnemers in RVICTO-PT-veld op een daartoe strekkend verzoek van Deelnemer een conform de gestelde eisen Offerte uitbrengt dan zet Deelnemer de Aanvraag uit bij de Opdrachtnemers in RVICTO-PT-bank conform de eisen van dit hoofdstuk.
- AP.20** Indien geen van de door Deelnemer tot mededinging opgeroepen Opdrachtnemers in RVICTO-PT-bank op een daartoe strekkend verzoek van Deelnemer een conform de gestelde eisen Offerte uitbrengt dan mag Deelnemer de Aanvraag buiten de Raamovereenkomst uitzetten.

Hoofdstuk 4 - Eisen aan prijs en facturering

- T.1** De prijscomponent is uitgedrukt in euro's excl. btw en bestaat uit een vaste totaalprijs die is opgebouwd uit de uurtarieven uit Bijlage 6 van de Raamovereenkomst – Prijzenblad vermenigvuldigd met het aantal uren.
- T.2** In de maximale uurtarieven, de Offertes en in de Nadere overeenkomsten vastgelegde tarieven en vaste prijzen zijn alle kosten inbegrepen voor de gecontracteerde dienstverlening zoals, maar niet beperkt tot kosten intakegesprek voor beveiligingsonderzoeken, kosten voor voorbereiding en uitvoering van beveiligingsonderzoeken conform een Plan van Aanpak inclusief eventuele aanpassingen en het opstellen van het standaardrapport, salariskosten, kosten voor ABRO-toetsen, kosten voor aanvullende en maatwerkrapportages en rapportages met afwijkende rapportageperiode, toeslagen en toelages voor het personeel (a.g.v. bijvoorbeeld overwerk/onregelmatig werk/consignatiedienst etc.), overheadkosten, kosten voor ondersteunend werk, kosten voor het gebruik van apparatuur, software en licenties, telefoonkosten, databundels, BYOD-kosten, kosten voor VOG, reis- en verblijfkosten, parkeerkosten, opleidingskosten, wervings- en selectiekosten, vervangingen, leegloop(risico) van personeel, verzekeringspremies, winst, sociale lasten, ziekte/re-integratie en arbeidsongeschiktheid van personeel, pensioen, scholing, secundaire arbeidsvoorwaarden, kort verzuim, ziekteverzuim, feestdagen, vakantiedagen, (maatwerk)rapportages voor Opdrachtgever en Deelnemer, management, kosten voor bewijslasten, alsmede de (bureau)marge of opslag voor de uitvoering van de Raamovereenkomst.
- T.3** De maximale uurtarieven die Opdrachtnemer mag offrenen ter onderbouwing van zijn vaste totaalprijs zijn vastgelegd in Bijlage 6 van de Raamovereenkomst – Prijzenblad. Overschrijding van deze maximum uurtarieven leidt tot uitsluiting van de Offerte, ~~tenzij de Deelnemer in de Aanvraag overschrijding toelaat én de overschrijding binnen de voorwaarden is aangeboden zoals Deelnemer deze in de Aanvraag heeft gesteld~~ ~~tenzij de Deelnemer in de Aanvraag heeft aangegeven dat de maximum uurtarieven voor de betreffende Nadere overeenkomst vervallen in die uitzonderlijke gevallen waar de gevraagde expertise niet beschikbaar is tegen de maximum uurtarieven en onder de voorwaarde dat de totale opdrachtwaarde zonder toepassing van de maximum uurtarieven niet meer dan 10% hoger is dan de totale opdrachtwaarde met toepassing van de maximum uurtarieven~~ én het de classificatie niet aantast.
- T.4** Opdrachtnemer factureert vanuit één rechtspersoon, en daarbinnen één centraal punt. Het is niet toegestaan dat door Opdrachtnemer ingezette onderaannemers rechtstreeks aan Deelnemer een factuur te sturen. Een combinant mag, na voorafgaande toestemming door Deelnemer, wel rechtstreeks een factuur sturen aan Deelnemer. Afspraken hierover worden vastgelegd per Nadere overeenkomst of in de vastgelegde werkafspraken met Deelnemer.
- T.5** Opdrachtnemer stuurt uitsluitend elektronische facturen (e-facturen) naar de Deelnemer. Een e-factuur is een gestructureerd elektronisch bestand (geen pdf) waarbij de vereiste gegevens altijd op een vaste plek met specifieke codering in het bestand staan. Opdrachtnemer kan op twee manieren e-facturen verzenden:
- E-factureren vanuit een (boekhoud)softwarepakket via o.a. Peppol;
 - E-factureren met behulp van een serviceprovider via o.a. Peppol.
- Voor meer informatie over e-factureren, zie: <https://www.helpdesk-efactureren.nl/> en [Bijsluiter e-factureren aan de Rijksoverheid: Informatie voor leveranciers | Helpdesk e-factureren](#).
- T.6** Opdrachtnemer en Deelnemer leggen de specificaties die van belang zijn voor goede e-facturering vast in de onderlinge werkafspraken (bijvoorbeeld in een DAP). De factuur dient minimaal onderstaande gegevens te bevatten:
- De wettelijk verplichte factuurgegevens;
 - Factuurnummer en datum;
 - Naam/kostenplaats van de Deelnemer/directie/afdeling;
 - Inkoopordernummer(s) en bijbehorende omschrijving;
 - Het Overheidsidentificatienummer (OIN) van de Deelnemer;

- Het subtotaal exclusief btw;
- Het btw-percentages en -bedrag;
- Het totaalbedrag inclusief btw.

T.7

Indien een Deelnemer voor zijn inkoopproces gebruik maakt of gaat maken van een digitaal systeem, dan sluit Opdrachtnemer hierop aan, voor zover dit redelijkerwijs van Opdrachtnemer verwacht mag worden. Deelnemer biedt Opdrachtnemer hiervoor een redelijke implementatietermijn van ten minste drie (3) maanden.

Eventuele kosten van Opdrachtnemer voor het realiseren, wijzigen, beheren en onderhouden, het opleiden/instrueren van zijn Personeel en alle andere kosten betreffende het gebruik van dit digitale systeem worden niet door Deelnemer vergoed, tenzij sprake is van een maatwerksysteem of onevenredig hoge kosten. In dat geval treden Opdrachtnemer en Deelnemer in overleg over een alternatieve werkwijze.

Indien en zolang Opdrachtnemer niet is aangesloten of geen gebruik maakt van dit digitale systeem van Deelnemer, accepteert Opdrachtnemer het risico dat Opdrachtnemer hierdoor uitgesloten wordt van deelname aan de minicompetities of Aanvragen op basis van het toerbeurtschema die door deze Deelnemer uitgeschreven worden binnen deze Raamovereenkomst en als gevolg hiervan geen Nadere overeenkomsten van deze Deelnemer gegund kan krijgen. Deelnemer communiceert tijdig wanneer een digitaal systeem verplicht wordt gesteld.

Hoofdstuk 5 - Eisen aan organisatie en beheer

Centraal en decentraal contractmanagement

- 0.1** Na gunning van de Raamovereenkomst leggen Opdrachtnemer en Deelnemer afzonderlijk werkafspraken vast, dit kan overkoepelend voor alle nog te sluiten Nadere overeenkomsten worden gedaan of per Nadere overeenkomst.
- 0.2** De werkafspraken dienen te voldoen aan het gestelde in dit programma van eisen en mogen niet afwijken van de Raamovereenkomst.
- 0.3** Opdrachtnemer stelt één gemandateerde vaste accountmanager beschikbaar voor Opdrachtgever en één gemandateerde vaste accountmanager per Deelnemer die het centrale aanspreekpunt is, die de dienstverlening voor Opdrachtgever en/of Deelnemer coördineert, die zorg draagt voor (toezicht op) naleving van de Raamovereenkomst door Opdrachtnemer en toezicht houdt op de kwaliteit van de totale dienstverlening van Opdrachtnemer. Deze persoon dient telefonisch en per e-mail goed bereikbaar te zijn. Opdrachtnemer zorgt voor gemandateerde en minstens gelijkwaardige vervanging bij afwezigheid van de vaste accountmanager, hetgeen tijdig kenbaar wordt gemaakt.
- 0.4** Tenminste éénmaal per kwartaal en kort na de termijn waarbinnen de rapportage conform hoofdstuk 6 moet worden opgeleverd vindt er een overleg plaats tussen Opdrachtgever en Opdrachtnemer. De gesprekspunten worden vastgelegd in een verslag door Opdrachtnemer. In onderlinge afstemming kan een overleg worden overgeslagen indien er onvoldoende besprekspunten zijn.
- 0.5** Opdrachtnemer en Deelnemer stellen gezamenlijk de gewenste overlegfrequentie vast en de inhoud van het overleg.

Klantoverleg

- 0.6** Opdrachtnemer en Deelnemer hebben op verzoek of na instemming van Deelnemer strategisch en/of tactisch overleg, met als doelstelling de relatie en samenwerking tussen hen te optimaliseren en Prestaties van Opdrachtnemer te monitoren en eventueel te verbeteren. De frequentie van deze overlegvormen en betrokken personen kan in onderling overleg worden bepaald en wordt vastgelegd in de werkafspraken.

Hoofdstuk 6 - Eisen aan rapportages (ROK niveau)

R.1 Opdrachtnemer levert standaard rapportages aan Opdrachtgever om een eenduidige verwerking van de gevraagde gegevens mogelijk te kunnen maken en hanteert daarvoor het format dat tijdens implementatie wordt vastgesteld en is gebaseerd op:

- het rapportageformat conform Bijlage 12.1 – Model Rapportage ROK RVICTO-PT
- het rapportageformat conform Bijlage 12.2 – Model Rapportage SROI

R.2 Opdrachtnemer verstrekt de Rapportage ROK RVICTO-PT aan Opdrachtgever per drie (3) maanden.

De aanlevertermijn start op de eerste dag na einde kwartaal en sluit uiterlijk vijftien (15) dagen na einde kwartaal. Het betreft de periodes:

Kwartaal: 1-1-202x tot en met 31-3-202x

Kwartaal: 1-4-202x tot en met 30-6-202x

Kwartaal: 1-7-202x tot en met 30-9-202x

Kwartaal: 1-10-202x tot en met 31-12-202x

- De eerste rapportageperiode betreft de eerste drie (3) maanden die volledig binnen een van de genoemde kwartalen valt, aangevuld met de periode vanaf de startdatum van de Raamovereenkomst.
- De laatste rapportageperiode wordt aangevuld tot en met de einddatum van de Raamovereenkomst.

Opdrachtnemer verstrekt de Rapportage SROI één keer per contractjaar aan Opdrachtgever en conform de uitleg in eis M.6. De jaarlijkse opleverdatum wordt door Opdrachtgever bij implementatie van de Raamovereenkomst afgestemd met Opdrachtnemer.

R.3 Teneinde de uniformiteit en betrouwbaarheid van de aanvraagdata in de rapportages te waarborgen, geldt het volgende:

1 - Opdrachtgever wijst per rapportageperiode (kwartaal) één Opdrachtnemer RVICTO-PT-veld en één Opdrachtnemer RVICTO-PT-bank aan als coördinerend Opdrachtnemer voor het opstellen van de aanvraagdata op basis van de minicompenties. De aanwijzing geschiedt volgens een roulatiesysteem waarbij iedere Opdrachtnemer minimaal één keer als coördinerend Opdrachtnemer fungeert.

2 - De coördinerend Opdrachtnemer is verantwoordelijk voor:

- Het opstellen van het concepttabblad met aanvraagdata minicompenties voor de betreffende rapportageperiode;
- Het verzamelen van alle relevante aanvraagdata op basis van de door Deelnemers verstrekte Aanvragen;
- Het waarborgen van de volledigheid en juistheid van de aanvraagdata;
- Uiterlijk vijf (5) kalenderdagen na de einddatum van de betreffende meetperiode distribueren van het concepttabblad aan de overige Opdrachtnemers ter verificatie.

3 - Iedere Opdrachtnemer is verplicht:

- Het concepttabblad te controleren op volledigheid en juistheid binnen drie (3) kalenderdagen na ontvangst;
- Eventuele afwijkingen, onvolkomenheden of ontbrekende gegevens schriftelijk (per e-mail) te melden aan de coördinerend Opdrachtnemer;
- Bij akkoord een schriftelijke goedkeuring te verstrekken aan de coördinerend Opdrachtnemer.

4 - De coördinerend Opdrachtnemer verwerkt binnen drie (3) kalenderdagen na ontvangst van alle verificaties de eventuele correcties en stelt het definitieve tabblad met aanvraagdata vast.

Dit definitieve tabblad wordt gelijktijdig door de coördinerend Opdrachtnemer verstrekt aan alle Opdrachtnemers.

5 - Iedere Opdrachtnemer is zelf verplicht het door de coördinerend Opdrachtnemer opgestelde en door alle Opdrachtnemers geverifieerde tabblad met aanvraagdata ongewijzigd te gebruiken in zijn individuele rapportage. Afwijkingen of aanpassingen aan dit tabblad zijn niet toegestaan.

6 - Iedere Opdrachtnemer vult vervolgens het tabblad aan met aanbodata en vult de tabbladen aanvragen toerbeurtschema en Nadere overeenkomsten in en dient de volledige rapportage in conform gestelde termijn in R.2.

7- Als Opdrachtnemers binnen de verificatietermijn geen consensus bereiken over de aanvraagdata, of indien de coördinerend Opdrachtnemer de termijnen niet naleeft, dienen Opdrachtnemers dit uiterlijk op kalenderdag elf (11) na einddatum meetperiode te escaleren naar Opdrachtgever.

8- Opdrachtgever beslist bindend bij escalatie.

- R.4** Opdrachtgever en Opdrachtnemer kunnen een voorstel doen om het format van de genoemd in eis R.1 aan te passen en stemmen een voorgestelde wijziging onderling af. Uitsluitend Opdrachtgever besluit of een aanpassing wordt doorgevoerd. De doorgevoerde wijziging geldt voor alle Opdrachtnemers.
- R.5** Opdrachtnemer levert op verzoek van Opdrachtgever aanvullende (maatwerk)rapportages of een rapportage met een afwijkende rapportageperiode. Opdrachtgever gaat hier terughoudend mee om.
- R.6** Opdrachtnemer zal op verzoek van Deelnemer aanvullende of (maatwerk)rapportages opleveren indien deze bijdragen aan het bereiken van het Resultaat tijdens de uitvoering van een Nadere overeenkomst.
- R.7** Opdrachtnemer is zelf verantwoordelijk voor het bijhouden van de informatie die in rapportages moeten worden opgenomen.
- R.8** Bij constatering door Opdrachtgever van foutieve informatie in de rapportages of het vermoeden daarvan, levert Opdrachtnemer op eerste verzoek per direct aanvullend bewijs dan wel corrigeert de foutieve informatie en levert een herziene rapportage aan.
- R.9** De rapportageverplichtingen blijven van kracht na beëindiging van de Raamovereenkomst, totdat alle Nadere overeenkomsten zijn beëindigd.

Hoofdstuk 7 - Eisen met betrekking tot prestatie management (ROK niveau)

K.1 Opdrachtgever meet de prestaties van de Opdrachtnemer op basis van twee (2) Kritieke Prestatie Indicatoren (KPI-1 en KPI-2), één (1) prestatie-indicator (PI-1) en één (1) meetgegeven (M-1).

- KPI-1 Kwaliteit van de dienstverlening
- KPI-2 Rapportages
- PI-1 Percentage gegunde Opdrachten
- M-1 Percentage uitgebrachte Offertes

De score per Opdrachtnemer aangaande KPI's, PI-1 en M-1 wordt geaggregeerd op het niveau van de Raamovereenkomst (Deelnemeroverstijgend) vastgesteld.

Deelnemer kan per Nadere overeenkomst extra KPI's, PI's of andere meetgegevens overeenkomen met Opdrachtnemer.

K.2 De meetperiode voor KPI-1, PI-1 en M-1 betreft vier (4) kwartalen conform eis R.2.

De peildata zijn gelijk aan de laatste dag van de meetperiode:

Meetperiode 1: ingangsdatum ROK tot en met 4^e kwartaal

Meetperiode 2: 5^e kwartaal tot en met 8^e kwartaal

Meetperiode 3: 9^e kwartaal tot en met 12^e kwartaal

Meetperiode 4: 13^e kwartaal tot en met einddatum ROK

KPI-2 wordt per kwartaal vastgesteld. De meetperiode is altijd één kalenderkwartaal, zie eis R.2. De peildatum is de laatste dag van dat kwartaal.

K.3 Opdrachtnemer conformeert zich aan de 2 sturingsmechanismen die van toepassing zijn op de uitvoering van Raamovereenkomst zoals beschreven in dit hoofdstuk:

Sturingsmechanisme 1 sanctiemogelijkheden KPI-1 en KPI-2

Sturingsmechanisme 2 rouleren RVICTO-PT-veld en RVICTO-PT-bank

KPI-1 Kwaliteit van de dienstverlening NOK

K.4 KPI-1 wordt per meetperiode door Opdrachtgever vastgesteld door het rekenkundig gemiddelde te bepalen van de beoordeling door Deelnemer, op basis van Bijlage 13.1 – Model Kwaliteit dienstverlening NOK en eventueel de beoordeling door Opdrachtgever, van Nadere overeenkomsten die in de meetperiode zijn afgerond/beëindigd.

Berekening:

Opdrachtgever stelt de behaalde score op KPI-1 vast door de som van de toegekende (rapport)cijfers te delen door het aantal Nadere overeenkomsten dat in de meetperiode is afgerond/beëindigd.

$$KPI-1 = \Sigma (\text{rapportcijfers per NOK}) / n \text{ (aantal afgeronde/beëindigde Nadere overeenkomsten in de meetperiode)}$$

Norm:

De norm voor KPI-1 $\geq 7,0$ op 1 cijfer achter de komma nauwkeurig.

K.5 Opdrachtnemer verzoekt Deelnemer om Bijlage 13.1 – Model Kwaliteit dienstverlening NOK in te vullen waarbij de beoordeling per afgeronde/beëindigde Nadere overeenkomst wordt uitgevoerd over de totale looptijd van de Nadere overeenkomst.

De Deelnemer beoordeelt elke afgeronde/beëindigde Nadere overeenkomst op basis van de instructie die is opgenomen in Bijlage 13.1

- K.6** Opdrachtnemer levert de ingevulde Bijlage 13.1 – Model Kwaliteit dienstverlening NOK per afgeronde Nadere overeenkomst aan bij Opdrachtgever tegelijkertijd met het indienen van de rapportage voor het 4^e kwartaal, het 8^e kwartaal, 12^e kwartaal en 16^e kwartaal.

Iedere Bijlage 13.1 – Model Kwaliteit dienstverlening NOK die op dag 15 na einddatum meetperiode niet in het bezit is van Opdrachtgever, wordt geregistreerd als niet ontvangen en daaraan kent Opdrachtgever het cijfer 5,0 toe als behaalde score voor de betreffende afgeronde/beëindigde Nadere overeenkomst, tenzij Opdrachtnemer kan aantonen dat Deelnemer na herhaaldelijke verzoeken van Opdrachtnemer geen beoordeling wil/gaat geven. De betreffende Nadere overeenkomst telt in dat geval niet mee voor het bepalen van de score op KPI-1.

Opdrachtgever behoudt zich het recht voor een ingevulde Bijlage 13.1 te verifiëren bij Deelnemer.

KPI-2 Rapportages

- K.7** KPI-2 wordt per meetperiode door Opdrachtgever als volgt vastgesteld:

A - de rapportage is op tijd aangeleverd

B - de rapportage is juist en volledig

Berekening tijdigheid

Opdrachtgever registreert nauwkeurig de exacte datum en het precieze tijdstip waarop de rapportage van de Opdrachtnemer is ontvangen. Vervolgens berekent Opdrachtgever het aantal kalenderdagen tussen de ontvangstdatum van de rapportage en de einddatum van het kwartaal.

Tijdigheid KPI-2 = Aantal kalenderdagen tussen de ontvangstdatum van de rapportage - de einddatum van het kwartaal.

Norm tijdigheid

De norm voor KPI-2 tijdigheid ≤ 15 kalenderdagen

Berekening juistheid en volledigheid

Opdrachtgever stelt vast dat Opdrachtnemer binnen de periode voor netto hersteltijd op juiste wijze heeft gerapporteerd en dat de rapportage geen gebreken bevat.

Juistheid en volledigheid KPI-2 = Aantal kalenderdagen tussen datum ontvangst volledige en juiste rapportage en datum eerste verzoek door Opdrachtgever tot herstel.

Norm juistheid en volledigheid

De norm voor KPI-2 juistheid en volledigheid $\leq$ zeven (7) Werkdagen (of $7 \times 24 = 168$ uur) na eerste verzoek door Opdrachtgever tot herstel.

- K.8** Van op onjuiste wijze rapporteren of rapporteren met gebreken is sprake wanneer Opdrachtnemer, niet, onvolledig, onjuist (inclusief niet conform de overige rapportagevereisten, zoals syntax en structuur) rapporteert over een rapportageperiode en Opdrachtnemer deze gebreken niet naar het oordeel van Opdrachtgever op voldoende wijze herstelt binnen de maximale "netto hersteltijd" van zeven (7) werkdagen (of $7 \times 24 = 168$ uur), na een schriftelijk verzoek daartoe door Opdrachtgever:

- Deze netto hersteltijd van gebreken betreft de cumulatieve tijd die Opdrachtnemer nodig heeft tussen een schriftelijk verzoek van Opdrachtgever om alsnog een juiste en volledige rapportage aan te leveren en het door Opdrachtnemer schriftelijk indienen van een nieuwe/herstelde rapportage.
- De tijd die Opdrachtgever zelf nodig heeft tussen het ontvangen van een rapportage van Opdrachtnemer, het toetsen van deze rapportage en het versturen van een reactie naar

Opdrachtnemer over het accepteren of laten herstellen van een rapportage wordt niet in deze netto hersteltijd meegeteld.

- Opdrachtnemer kan binnen deze maximale netto hersteltijd meerdere (herstelde) versies van een rapportage bij Opdrachtgever indienen, maar streeft ernaar het aantal herstelde versies te minimaliseren (doel: 'first time right').

K.9 Opdrachtgever kan de volledigheid en juistheid van de rapportages op zowel automatische wijze (door bijvoorbeeld RPA) als handmatige wijze toetsen.

Opdrachtgever is gerechtigd om een gering aantal evidente kleine omissies/fouten in de rapportage van Opdrachtnemer na overleg met Opdrachtnemer zelf te herstellen, als Opdrachtgever verwacht dat dit sneller is dan een herstel door Opdrachtnemer. Opdrachtnemer krijgt dan wel de beschikking over de door Opdrachtgever herstellende rapportage, als hij hierna zelf ook nog gebreken in de rapportage moet herstellen.

Gebreken die het gevolg zijn van onvolledige, onduidelijke of foutieve informatieverstrekking door een Deelnemer en die Opdrachtnemer als behoorlijk geïnformeerde en normaal oplettende Opdrachtnemer had moeten/kunnen constateren, zijn geen reden voor het kwijtschelden van gebreken in de rapportage. Opdrachtgever kan verlangen dat Opdrachtnemer deze gebreken, al dan niet na raadpleging van de Deelnemer, herstelt.

PI-1 Percentage gegunde Opdrachten

K.10 PI-1 wordt per meetperiode door Opdrachtgever vastgesteld door het percentage te bepalen van het aantal Nadere overeenkomsten dat na minicompetitie aan Opdrachtnemer is gegund ten opzichte van het aantal geldige Aanvragen dat is uitgezet in RVICTO-PT-veld via een minicompetitie. Een Aanvraag is geldig indien deze via een minicompetitie in RVICTO-PT-veld is uitgezet en niet is ingetrokken, geannuleerd of ongeldig verklaard. Het aantal geldige Aanvragen kan verlaagd worden met het aantal Aanvragen waarbij Opdrachtnemer op grond van eis AP.11 van Deelnemer een vrijstelling heeft ontvangen voor deelname aan de minicompetitie **of op grond van eis AP.4 niet heeft ontvangen**. Opdrachtgever zal dit toepassen indien deze verlaging gevolgen heeft voor de roulatiebeslissing van Opdrachtnemer.

Berekening:

Opdrachtgever stelt de behaalde score op PI-1 vast door het aantal via minicompetitie aan Opdrachtnemer gegunde Nadere overeenkomsten op basis van Bijlage 12.1 – Model rapportage ROK RVICTO-PT te delen door het aantal geldige Aanvragen in RVICTO-PT-veld via minicompetitie.

$$PI-1 = (\text{Aantal via minicompetitie gesloten Nadere overeenkomsten met Opdrachtnemer} / \text{Totaal aantal geldige Aanvragen uitgezet in RVICTO-PT-veld via minicompetitie}) \times 100$$

Norm:

De norm voor PI-1 $\geq 10,00\%$ op 2 cijfers achter de komma nauwkeurig.

M-1 Aanbiedingspercentage Offertes

K.11 M-1 wordt per meetperiode door Opdrachtgever vastgesteld door het percentage te bepalen van het aantal via minicompetitie door Opdrachtnemer uitgebrachte geldige Offertes ten opzichte van het aantal geldige Aanvragen dat is uitgezet in RVICTO-PT-veld via een minicompetitie. Het aantal geldige Aanvragen kan verlaagd worden met het aantal Aanvragen waarbij Opdrachtnemer op grond van eis AP.11 van Deelnemer een vrijstelling heeft ontvangen voor deelname aan de minicompetitie **of op grond van eis AP.4 niet heeft ontvangen**. Opdrachtgever zal dit toepassen indien deze verlaging gevolgen heeft voor de roulatiebeslissing van Opdrachtnemer.

Berekening:

$M-1 = (\text{Aantal geldige Offertes uitgebracht door Opdrachtnemer} / \text{Totaal aantal geldige Aanvragen uitgezet in RVICTO-PT-veld via minicompetitie}) \times 100.$

Norm:

Geen.

Sturingsmechanisme 1 sanctiemogelijkheden KPI-1 en KPI-2

K.12 Bij het niet behalen van KPI-1 wordt een gele kaart/sanctie toegewezen door Opdrachtgever aan Opdrachtnemer zoals aangegeven in de onderstaande eisen.

K.13 De toewijzing van een gele kaart/sanctie voor KPI-1 heeft geaggregeerd betrekking op alle Deelnemers en binnen de Raamovereenkomst.

K.14 Als de prestaties van Opdrachtnemer in een meetperiode niet voldoen aan de voor KPI-1 geldende normwaarde, krijgt de Opdrachtnemer voor de tekortkoming een gele kaart als sanctie. Deze gele kaart houdt in dat Opdrachtnemer een formele schriftelijke aanwijzing ontvangt om de geconstateerde tekortkoming(en) te herstellen tot de overeengekomen normwaarden. Wordt aan het einde van de opvolgende meetperiode wederom niet voldaan aan de voor KPI-1 geldende normwaarde, dan ontvangt Opdrachtnemer een tweede gele kaart als sanctie en is Opdrachtnemer in verzuim. Opdrachtgever is vervolgens gerechtigd om de Raamovereenkomst door middel van een aangetekend schrijven buiten rechte geheel of gedeeltelijk te ontbinden.

De sanctie conform deze eis is van kracht zodra aan de volgende voorwaarden is voldaan: aantal beoordeelde Nadere overeenkomsten > 2

én:

aantal verschillende beoordelaars > 2

én:

behaalde score door Opdrachtnemer < 7,0

Los van de hierboven omschreven sanctie draagt Opdrachtnemer zorg voor het opstellen van een herstelplan conform Bijlage 13.2 - Model Herstelplan RVICTO bij toewijzing van een gele kaart.

K.15 Als de prestaties van Opdrachtnemer in een meetperiode niet voldoen aan de voor KPI-2 geldende normwaarden kan Opdrachtgever besluiten Opdrachtnemer voor een bepaalde periode uit te sluiten van deelname aan minicompetities of Aanvragen via het toerbeurtschema van Deelnemer waardoor Opdrachtnemer geen Offertes mag aanbieden.

De toewijzing van de sanctie op KPI-2 heeft geaggregeerd betrekking op alle Deelnemers en binnen de Raamovereenkomst.

De opschorting van deelname van Opdrachtnemer aan minicompetities of het toerbeurtschema duurt voort tot aan het moment dat Opdrachtnemer, naar het oordeel van Opdrachtgever, een juiste en volledige rapportage heeft ingediend over de betreffende meetperiode en Opdrachtgever deze schriftelijk heeft geaccepteerd. Opdrachtnemer dient dan binnen een door Opdrachtgever te bepalen redelijke termijn van ten minste 2 weken alsnog een juiste en volledige rapportage op te leveren. Indien binnen deze ingebrekestellingsperiode wederom niet, onjuist en/of onvolledig wordt gerapporteerd, dan is Opdrachtnemer in verzuim en is Opdrachtgever gerechtigd om de Raamovereenkomst buiten rechte geheel dan wel gedeeltelijk te ontbinden.

K.16 Er zijn 3 ijkmomenten waarop roulatie tussen RVICTO-PT-veld en RVICTO-PT-bank kan plaatsvinden:

Ijkmoment	Timing
Ijkmoment 1	Na afronding meetperiode 1 op basis van data voor meetperiode 1
Ijkmoment 2	Na afronding meetperiode 2 op basis van data voor meetperiode 2
Ijkmoment 3	Na afronding meetperiode 3 op basis van data voor meetperiode 3

K.17 Per ijkmoment rouleert maximaal 1 Opdrachtnemer van RVICTO-PT-veld naar RVICTO-PT-bank.

K.18 Per ijkmoment rouleert maximaal 1 Opdrachtnemer van RVICTO-PT-bank naar RVICTO-PT-veld, maar uitsluitend indien er een opdrachtnemer van RVICTO-PT-veld naar RVICTO-PT-bank is gerouleerd.

K.19 Roulatie wordt vastgesteld en schriftelijk gecommuniceerd door Opdrachtgever uiterlijk dertig (30) kalenderdagen na het einde van de meetperiode die het ijkmoment markeert en is bindend voor partijen. De communicatie bevat minimaal:

- Welke Opdrachtnemer van RVICTO-PT-veld naar RVICTO-PT-bank rouleert
- Welke Opdrachtnemer van RVICTO-PT-bank naar RVICTO-PT-veld rouleert
- De scores op KPI-1, PI-1 en M-1 per Opdrachtnemer
- De motivering van het roulatiebesluit
- De beslisregels die zijn toegepast

K.20 De roulatie treedt in werking op de eerste dag van de tweede maand binnen de eerstvolgende meetperiode na het ijkmoment.

K.21 Het bepalen van de Opdrachtnemer die rouleert van RVICTO-PT-veld naar RVICTO-PT-bank gaat als volgt:

- 1 primair – rouleren op basis van de score KPI-1
- 2 secundair – rouleren op basis van de score PI-1, M-1 of loting

Van RVICTO-PT-veld naar RVICTO-PT-bank, primair rouleren op basis van KPI-1

K.22 Opdrachtnemer in RVICTO-PT-veld die op KPI-1 een score onder de norm heeft behaald én waarbij deze score voldoet aan de voorwaarden van K.14, rouleert van RVICTO-PT-veld naar RVICTO-PT-bank.

K.23 Indien meer dan 1 Opdrachtnemer een score op KPI-1 onder de norm heeft behaald dan geldt het volgende:
De hoogte van de score op KPI-1 bepaalt welke Opdrachtnemer van RVICTO-PT-veld naar RVICTO-PT-bank gaat:

- De Opdrachtnemer met de laagste score op KPI-1 rouleert naar RVICTO-PT-bank;
- De andere Opdrachtnemer(s) rouleren niet.

K.24 Indien 2 of meer Opdrachtnemers een gelijke laagste score onder de norm op KPI-1 hebben dan geldt selectie tussen de Opdrachtnemers met de gelijke laagste score op KPI-1, op basis van PI-1.

Van RVICTO-PT-veld naar RVICTO-PT-bank, secundair rouleren op basis van PI-1

K.25 Opdrachtnemers in RVICTO-PT-veld rouleren op basis van PI-1 indien:

- Op basis **van** primair rouleren geen Opdrachtnemer in aanmerking komt voor rouleren van RVICTO-PT-veld naar RVICTO-PT-bank
OF
- Op basis van primair rouleren bij gelijke KPI-1 scores niet kan worden bepaald welke Opdrachtnemer rouleert naar RVICTO-PT-bank

K.26 Opdrachtnemer met een PI-1 score onder de norm komt in aanmerking voor rouleren van RVICTO-PT-veld naar RVICTO-PT-bank.

K.27 Indien op basis van primair rouleren geen Opdrachtnemer is gerouleerd naar RVICTO-PT-bank, dan rouleert de Opdrachtnemer met een score op PI-1 onder de norm van RVICTO-PT-veld naar RVICTO-PT-bank.

Indien meer dan 1 Opdrachtnemer een score onder de norm heeft, dan geldt het volgende:

- De Opdrachtnemer met de laagste score onder de norm op PI-1 rouleert naar RVICTO-PT-bank;
- De andere Opdrachtnemers rouleren niet.

Zijn de scores gelijk en kan niet worden bepaald welke Opdrachtnemer rouleert dan vindt selectie plaats op basis van de laagste score op M-1 tussen de Opdrachtnemers met gelijke score onder de norm op PI-1.

Zijn de scores op M-1 gelijk dan volgt loting door IUC-EZK/LVVN.

K.28 Indien op basis van primair rouleren bij een gelijke score op KPI-1 onder de norm niet kan worden bepaald welke Opdrachtnemer rouleert van RVICTO-PT-veld naar RVICTO-PT-bank dan geldt het volgende:

- De Opdrachtnemer met de laagste score op PI-1 rouleert van RVICTO-PT-veld naar RVICTO-PT-bank.

Indien op basis van PI-1 niet bepaald kan worden welke Opdrachtnemer rouleert omdat scores gelijk zijn, dan rouleert de Opdrachtnemer met de laagste score op M-1.

Zijn de scores op M-1 gelijk dan volgt loting door IUC-EZK/LVVN.

Van RVICTO-PT-veld naar RVICTO-PT-bank, rouleren door loting IUC-EZK/LVVN

K.29 De loting is transparant, objectief en wordt gedocumenteerd.
Alle betrokken Opdrachtnemers worden vooraf geïnformeerd over de lotingsprocedure door Opdrachtgever.

Rouleren van RVICTO-PT-bank naar RVICTO-PT-veld

K.30 Indien op basis van K.16 tot en met K.29 geen positie open is in RVICTO-PT-veld dan rouleert er geen Opdrachtnemer van RVICTO-PT-bank naar RVICTO-PT-veld.

K.31 Indien op basis van K.16 tot en met K.29 een positie open is in RVICTO-PT-veld dan rouleert Opdrachtnemer die de hoogste score op KPI-1 boven de norm heeft behaald én waarbij ~~de score wel voldoet aan de voorwaarden uit K.14.~~ **aan de voorwaarden is voldaan dat er meer dan 2 Nadere overeenkomsten zijn beoordeeld én dat deze beoordelingen door meer dan 2 verschillende beoordelaars zijn gedaan:**

- Indien meer dan 1 Opdrachtnemer dezelfde hoogste score op KPI-1 heeft behaald dan rouleert de Opdrachtnemer met de hoogste score op PI-1.
- Indien er geen score op basis van KPI-1 kan worden vastgesteld dan rouleert de Opdrachtnemer met de hoogste score op PI-1.

- Indien meer dan 1 Opdrachtnemer dezelfde hoogste score op PI-1 heeft dan rouleert van de Opdrachtnemer met dezelfde hoogste score op PI-1 de Opdrachtnemer met de hoogste score op M-1.
- Indien meer dan 1 Opdrachtnemer met dezelfde hoogste score op PI-1 ook dezelfde hoogste score op M-1 heeft dan volgt loting door IUC-EZK/LVVN conform K.29 om te bepalen welke Opdrachtnemer rouleert.

K.32 Voor de Opdrachtnemer die rouleert geldt dat de KPI-1, PI-1 en M-1 worden berekend vanaf ingangsdatum roulatie.

*Achterwege blijven sanctie/gele kaart sturingsmechanisme 1 en/of rouleren van **RVICTO-PT-veld** naar **RVICTO-PT-bank** sturingsmechanisme 2*

K.33 Toewijzing van een sanctie/gele kaart aan Opdrachtnemer op basis van sturingsmechanisme 1 en/of roulatie voor sturingsmechanisme 2 van RVICTO-PT-veld naar RVICTO-PT -bank blijft achterwege indien:

- Naar het oordeel van de Opdrachtgever toewijzing of roulatie als disproportioneel moet worden beschouwd;
en/of
- De oorzaak van het verkrijgen van een sanctie/gele kaart of roulatie van RVICTO-PT-veld naar RVICTO-PT-bank buiten de invloedssfeer van Opdrachtnemer ligt, dan wel anderszins niet voor rekening en risico van Opdrachtnemer dient te komen.

K.34 Het als gevolg van op basis van eis K.33 kwijtschelden van een gele kaart/sanctie aan Opdrachtnemer of roulatie van RVICTO-PT-veld naar RVICTO-PT-bank beperkt zich uitsluitend tot de betreffende situatie voor Opdrachtnemer en is afhankelijk van de omstandigheden van het geval.

K.35 Opdrachtnemer kan geen recht ontlenen aan de beslissing van Opdrachtgever tot het doen kwijtschelden van een sanctie/gele kaart of roulatiebeslissing voor een andere Opdrachtnemer van deze Raamovereenkomst en dit heeft daarmee dan ook niet automatisch het gevolg dat een toe te wijzen gele kaart/sanctie en/of een roulatiebeslissing van RVICTO-PT-veld naar RVICTO-PT-bank voor Opdrachtnemer wordt kwijtgescholden.

Hoofdstuk 8 - Eisen aan Maatschappelijk Verantwoord Ondernemen

Specifieke voorschriften met betrekking tot social return (SR)

M.1 Opdrachtnemer is verplicht om ten minste **2%** van de (Opdracht)waarde van de aan Opdrachtnemer op grond van deze Raamovereenkomst te gunnen Nadere overeenkomsten, in te zetten voor social return (SR). Dit percentage wordt aan de hand van de gerealiseerde (Opdracht)waarde of omzet excl. btw van een Opdrachtnemer vertaald in een bedrag (percentage SR maal waarde), hierna te noemen de "social return-verplichting" (ook: SR-verplichting). De SR-verplichting wordt dus per Nadere overeenkomst bepaald. Meerdere afzonderlijke SR-verplichtingen op grond van meerdere Nadere overeenkomsten met een Opdrachtnemer worden bij elkaar opgeteld tot een (cumulatieve) SR-verplichting.

Het doel van de SR-verplichtingen is het realiseren van sociale impact door mensen met afstand tot de arbeidsmarkt (hierna ook: doelgroepkandidaten) aan werk en inkomen te helpen of het perspectief van deze mensen op werk en inkomen te verbeteren.

Opdrachtnemer kan op verschillende manieren de SR-verplichtingen invullen:

(1) **Arbeidsparticipatie:**

inzet van mensen met afstand tot de arbeidsmarkt op een uit te voeren Opdracht ten behoeve van een Deelnemer of inzet buiten een Opdracht van Deelnemer.

(2) **Compensatieorders:**

door het plaatsen van orders/Opdrachten bij c.q. het inzetten van

a - sociale/maatschappelijke ondernemingen of

b - sociale werkbedrijven.

Ad a - Sociale of maatschappelijke ondernemingen zijn ondernemingen die:

- (a1) een product of dienst leveren;
- (a2) in plaats van met een winstdoelstelling dit primair en expliciet doen om bij te dragen aan een maatschappelijk doel welke is vastgelegd in haar statuten;
- (a3) een deel van de omzet herinvesteren in het bereiken van het maatschappelijke doel en/of beperkt zijn in de verdeling van winst en vermogen, e.e.a. om te garanderen dat het maatschappelijk doel voor gaat;
- (a4) hun relevante stakeholders identificeren en daarmee minimaal jaarlijks in dialoog gaan;
- (a5) transparant zijn op hun website (of op andere wijze die publiekelijk toegankelijk is zoals in hun jaarverslag) over de meest materiële gecreëerde maatschappelijke waarde;
- (a6) onafhankelijk van de overheid en/of andere entiteiten een eigen strategie kunnen nastreven.

Ad b - Een sociaal werkbedrijf (SW-bedrijf) is een bedrijf dat duurzaam en beschut werk biedt aan mensen die geen werk vinden in een regulier bedrijf, zoals langdurig werklozen en mensen met een verstandelijke, lichamelijke, psychische of andere beperking.

(3) **Overig:**

het perspectief op werk en inkomen voor mensen met afstand tot de arbeidsmarkt kan op diverse manieren verbeterd worden. Denk aan opleiding, training, advies/coaching, voorlichting aan kandidaten, hulp bieden aan een sociaal initiatief of vrijwilligerswerk. Dit kan ook gericht zijn op de toekomstige arbeidsmarkt met als doel uitval te voorkomen. Ook kan Opdrachtnemer (IT of intermediair) diensten

leveren die primair ten gunste zijn van doelgroepkandidaten en/of de arbeidsmarkt. Bij voorkeur sluit Opdrachtnemer ook aan bij beleidsdoelen¹ van een Deelnemer.

De mate van invulling wordt bepaald door toepassing van het bouwblokkenmodel. Opdrachtnemers kunnen aan de hand van dit model 'blokken' met een transparante, vooraf vastgestelde waarde stapelen, zie de tabel hieronder. De optelsom van de waardes van de toegepaste blokken bepaalt of en in welke mate een Opdrachtnemer heeft voldaan aan zijn SR-verplichting, niet de daadwerkelijk betaalde looncomponent. Een combinatie van blokken is toegestaan. Ingeval meerdere blokken op een doelgroepkandidaat van toepassing zijn, geldt de hoogste SR-waarde. Een vaste SR-waarde in het geval van arbeidsparticipatie telt volledig mee als de doelgroepkandidaat is ingezet, ongeacht duur en omvang (voltijd/deeltijd) van het dienstverband of de inzet. Een SR-waarde telt eenmalig mee, ook als de doelgroepkandidaat meerdere jaren wordt ingezet.

Bij een SR-waarde mag een 'bonuswaarde' worden opgeteld als voldaan wordt aan een extra criterium, zoals vermeld in de tabel onder de bouwblokken. Ingeval twee of meer bonuswaardes op een doelgroepkandidaat van toepassing zijn, gelden de twee hoogste SR-waardes.

Opdrachtgever heeft het recht om vanaf 2 jaar na start van de Raamovereenkomst – eenmalig – een of meerdere bouwblokken toe te voegen en/of de SR-waarde per blok te herzien, om daarmee in te kunnen spelen op veranderende arbeidsmarktomstandigheden. Een eventuele herziening van SR-waarden heeft geen gevolgen voor reeds toegekende SR-waarden. Wijzigingen worden minimaal 3 maanden vooraf aangekondigd.

De Opdrachtnemer is hoofdverantwoordelijk voor het werven, selecteren, inzetten en begeleiden van doelgroepkandidaten, maar kan hierbij derden inzetten. Een doelgroepkandidaat kan uitsluitend ter vervulling van de SR-verplichting worden opgevoerd als deze behoort tot een doelgroep of bouwblok zoals vermeld in onderstaande bouwblokkentabel.

Bouwblok	Bijzonderheid	SR-waarde
(1) Arbeidsparticipatie		
Doelgroep van de banenafpraak, geregistreerd in het doelgroepregister van het UWV	<p>Dit betreft nu mensen met indicatie:</p> <ul style="list-style-type: none"> • Participatiewet (en niet in staat zelfstandig het minimumloon te verdienen); • (Voormalige) leerlingen uit het voortgezet speciaal onderwijs (vso) en praktijkonderwijs (pro) die zich schriftelijk hebben aangemeld bij het UWV; • Wsw (Wet sociale werkvoorziening); • Wajong met arbeidsvermogen; • WIW-baan / ID-baan (voormalige Wet inschakeling werkzoekenden) of (voormalig Besluit in- en doorstroombanen); • Mensen die een medische beperking kregen vóór hun 18e verjaardag of tijdens hun studie (en niet in staat 	€ 40.000

	zelfstandig het minimumloon te verdienen).	
WW (werkloosheidswet)	Geen onderscheid in duur WW-uitkering	€ 15.000
WIA/WAO	WIA (Wet werk en inkomen naar arbeidsvermogen) WAO (Wet op de arbeidsongeschiktheidsverzekering)	€ 30.000
Wajong (oude regeling)	Wet arbeidsongeschiktheidsvoorziening jonggehandicapten, voor 01-01-2015	€ 40.000
IOAW/IOAZ	IOAW (Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers) IOAZ (Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen)	€ 15.000
WSW-inzet (detachering/dienst), niet zijnde in loondienst nemen van WSW'er	Bij in eigen loondienst nemen WSW'er is er sprake van doelgroep banenafpraak	Betaalde factuurwaarde aan WSW-bedrijf
Niet-uitkeringsgerechtigde werkzoekende (Nugger)	1 jaar of langer werkzoekend	€ 15.000
Leer-/werktraject BBL of stage BOL van minimaal 2 maanden	Mbo-niveau 1 t/m 4	€ 15.000
Stage leerling voorgezet speciaal onderwijs (vso) of praktijkonderwijs (pro)		€ 15.000
Voortijdige schoolverlaters (zonder startkwalificatie) tot 27 jaar	Startkwalificatie: een diploma op minimaal havo-, vwo- of mbo-niveau 2 of hoger.	€ 15.000
(2) Compensatieorders		
Compensatieorder	Inzet SW-bedrijf of sociale/maatschappelijke onderneming (conform de (beoogde) rechtsvorm BVm/maatschappelijke bv, ingeschreven in het register PSO gecertificeerde organisaties trede 3 & 30+ Gecertificeerde organisaties , lid Social Enterprise NL of een vergelijkbare vorm)	Factuurwaarde (excl. btw)
(3) Overig		
Overige activiteiten om sociale impact te maken gericht op	Nader te bepalen, zoals opleiding, training, workshop, advies, coaching,	€ 100 per besteed uur of

genoemde doelgroepen	voorlichting, hulp bij toeleiding naar werk etc.	factuurwaarde (excl. btw)

Bonuswaarde:	Bijzonderheid	Bovenop SR- waarde
Vast dienstverband	In aanvulling op standaard SR-waarde	€ 10.000 extra
Tijdelijk dienstverband voortijdige schoolverlaters zonder startkwalificatie tot 27 jaar	In aanvulling op standaard SR-waarde	€ 10.000 extra
Tijdelijk dienstverband na diploma MBO	In aanvulling op standaard SR-waarde	€ 10.000 extra
Tijdelijk dienstverband na diploma vso of pro	In aanvulling op standaard SR-waarde	€ 10.000 extra
Leeftijd 50+	In aanvulling op standaard SR-waarde	€ 5.000 extra
(Ex-)gedetineerde	In aanvulling op standaard SR-waarde	€ 10.000 extra
Inzet bij Deelnemer	In aanvulling op standaard SR-waarde	€ 5.000 extra
Aanstelling als militair, burgerpersoneel of reservist bij Defensie	In aanvulling op standaard SR-waarde	€ 10.000 extra

Een kandidaat mag (maximaal) 1 jaar na de laatst verkregen uitkering of indicatie nog als zodanig worden opgevoerd.

Indien de Opdrachtnemer de Opdracht samen met onderaannemer(s) uitvoert, dan mag de feitelijke uitvoering van de SR-verplichting (deels) uitgevoerd worden door deze onderaannemer(s). De verantwoordelijkheid voor de invulling van de SR-verplichting en het aanleveren van de gevraagde gegevens ligt bij de Opdrachtnemer, ook als die verplichting door onderaannemer(s) ingevuld wordt. Ingeval van inzet van een combinatie, zijn de combinanten elk hoofdelijk aansprakelijk voor het gedeelte waarop hun eigen SR-verplichting ziet.

M.2

Aan het begin of voorafgaand aan een contractjaar maakt Opdrachtnemer een inschatting van zijn voorlopige SR-verplichting van het komende contractjaar. Dit kan gezien worden als een zelf te bepalen voorschot. Na een contractjaar (jaar T) stelt Opdrachtgever – na afstemming met Opdrachtnemer – de definitieve SR-verplichting per Opdrachtnemer vast op grond van de door Opdrachtnemer gerealiseerde omzet op Opdrachten in dat jaar: de SR-verplichting jaar T. Indien Opdrachtnemer dit bedrag van de definitieve SR-verplichting niet geheel in jaar T ingevuld heeft, dan wordt het restant (de onderschrijding) opgeteld bij de SR-verplichting van het daaropvolgende jaar (T+1), naast de eventuele SR-verplichting van dit nieuwe contractjaar. Hetzelfde geldt voor de opvolgende contractjaren. Na het laatste contractjaar van de Raamovereenkomst wordt de balans opgemaakt en over de dan nog resterende (cumulatieve) SR-verplichting is Opdrachtnemer een boete verschuldigd die gelijk staat aan tweemaal het bedrag van de niet-gerealiseerde SR-verplichting. Opdrachtgever stemt met Deelnemer(s) een passende bestemming van deze boete af. Een eventuele (beoogde) invulling van de (resterende) SR-verplichting van Opdrachtnemer na het einde van de looptijd van de Raamovereenkomst wordt buiten beschouwing gelaten en heeft geen gevolgen voor de vaststelling van de hoogte van de boete, indien van toepassing.

Een overschrijding van de SR-verplichting van Opdrachtnemer in een contractjaar T (oftewel, als Opdrachtnemer meer ingevuld/gerealiseerd heeft dan zijn SR-verplichting), mag deze

overschrijding in het opvolgende contractjaar T+1 afgetrokken worden van de SR-verplichting van dat opvolgende contractjaar (en eventueel daarna). Met andere woorden, Opdrachtnemer kan zelf bepalen in welke contractjaren hij in welke mate zijn SR-verplichtingen invult.

Voorbeeld boetebepaling:

Contractjaar	SR-verplichting	SR-restant (negatief: niet ingevulde SR-verplichting na dit contractjaar; positief: overschrijding van SR- verplichting)	Boete
1	€ 40.000	-/- € 10.000 (niet ingevuld in jaar 1, op te tellen bij SR- verplichting jaar 2)	-
2	€ 10.000 (restant jaar 1) + € 60.000 (jaar 2) = € 70.000	€ 0 (jaar 1, volledig gerealiseerd) -/- € 10.000 (niet ingevuld jaar 2, op te tellen bij SR- verplichting jaar 3)	-
3	€ 10.000 (restant jaar 2) + € 50.000 (jaar 3) = € 60.000	€ 0 (jaar 2) + € 10.000 (meer ingevuld in jaar 3, af te trekken van SR-verplichting jaar 4)	-
4	-/- € 10.000 (overschrijding jaar 3) + € 90.000 (jaar 4) = € 80.000	€ 0 (jaar 3) -/- € 30.000 (niet ingevuld in jaar 4)	-
Einde looptijd Raam- overeenkomst	€ 30.000 (restant jaar 4)		2 x € 30.000 = € 60.000

Voorbeelden invulling SR-verplichting:

- In contractjaar 1 hebben Deelnemers aan Opdrachtnemer drie Opdrachten verstrekt, op basis waarvan Opdrachtnemer € 2.000.000,- heeft gefactureerd. De hiermee opgebouwde SR-verplichting van contractjaar 1 is 2% hiervan, dus € 40.000. Opdrachtnemer had in dit contractjaar besloten om een persoon met WW-uitkering in tijdelijke dienst te nemen. Dit bouwblok heeft een waarde van € 15.000. Verder heeft Opdrachtnemer op een van de Opdrachten een sociale onderneming ingezet, die als onderaannemer €15.000 aan u gefactureerd had (=compensatieorder). Opdrachtnemer heeft hiermee dit jaar totaal 30.000 aan SR-verplichting ingevuld, waarmee het SR-restant € 10.000 is. Dit neemt Opdrachtnemer mee naar contractjaar 2.
- In contractjaar 2 lopen nog twee Opdrachten uit het eerste jaar door en Opdrachtnemer krijgt vijf nieuwe Opdrachten erbij. Opdrachtnemer factureert dit jaar € 3.000.000 aan Deelnemers. De SR-verplichting hiervan komt uit op € 60.000. Omdat Opdrachtnemer nog € 10.000 SR-restant uit contractjaar 1 heeft, is de cumulatieve SR-verplichting € 70.000. Gedurende contractjaar 2 heeft Opdrachtnemer een kandidaat uit het doelgroepregister ingezet op een Opdracht bij een Deelnemer. Deze persoon is 60 jaar. De waarde van het bouwblok 'doelgroepregister' is € 40.000. Opdrachtnemer krijgt twee bonuswaardes erbij: € 5.000 voor 'leeftijd 50+' en € 5.000 voor 'inzet bij deelnemer'. De WW'er die Opdrachtnemer in contractjaar 1 had ingezet, heeft in contractjaar 2 een vast dienstverband bij Opdrachtnemer gekregen. Opdrachtnemer krijgt hierom een bonuswaarde van € 10.000. De SR-waarde gerelateerd aan de inzet van de WW'er heeft Opdrachtnemer al in contractjaar 1 ontvangen en telt niet nogmaals mee. Opdrachtnemer heeft hiermee in contractjaar 2 totaal voor € 60.000 aan SR-

verplichting ingevuld, waarmee het SR-restant € 10.000 is. Dit neemt Opdrachtnemer mee naar contractjaar 3.

M.3 Opdrachtnemer dient binnen 2 maanden na start van de Raamovereenkomst bij Opdrachtgever een (concept) Plan van Aanpak in voor (beoogde) invulling van zijn SR-verplichting. Hierna stemt Opdrachtnemer het Plan van Aanpak met Opdrachtgever af. Het definitieve Plan van Aanpak dient Opdrachtnemer binnen 3 maanden na start van de Raamovereenkomst bij Opdrachtgever in. Het doel van dit Plan van Aanpak en de tijdige afstemming hierover is om met betrokken partijen gezamenlijk vast te stellen of de beoogde wijze van invulling van de SR-verplichting concreet, voldoende ambitieus, haalbaar, acceptabel en realistisch is.

Op het Plan van Aanpak is geen expliciete goedkeuring van Opdrachtgever vereist, aangezien Opdrachtnemer zelf verantwoordelijk is voor invulling van zijn SR-verplichting.

Opdrachtgever kan wel een (beoogde) invulling van een SR-verplichting gemotiveerd weigeren of besluiten om deze geheel of gedeeltelijk niet mee te laten tellen voor invulling van de SR-verplichting van Opdrachtnemer, bij gebrek aan sociale impact. Opdrachtnemer heeft er daarom zelf belang bij zijn Plan van Aanpak af te stemmen. Opdrachtnemer mag zijn Plan van Aanpak gedurende de looptijd van de Raamovereenkomst aanvullen en/of wijzigen. Deze aanvullingen/wijzigingen stemt Opdrachtnemer steeds met Opdrachtgever af.

M.4 Er mag bij de invulling van SR-verplichting géén sprake zijn van verdringing of oneerlijke concurrentie op de arbeidsmarkt, waarbij de gerealiseerde sociale impact ten koste gaat van banen van ander personeel.

Invulling van SR-verplichtingen ten behoeve van andere opdrachtgevers, wordt niet meegerekend als invulling van SR-verplichting ten behoeve van Opdrachtgever en/of Deelnemer(s), behalve voor het eventuele gedeelte dat duidelijk en aanvullend ten behoeve van Opdrachtgever en/of Deelnemer(s) wordt gerealiseerd. Een geplaatste of geholpen kandidaat mag dus niet meerdere keren als social return worden opgevoerd.

M.5 De wijze van invulling van de SR-verplichting van de Opdrachtnemer sluit in algemene zin aan bij het kabinets-/rijksbeleid en bij voorkeur ook bij de beleidsdoelstellingen, bedrijfsvoering en behoeftes van de Deelnemer(s). Voor deze Raamovereenkomst wijzen Deelnemers op het belang van het bieden van stageplekken aan MBO-ers (BOL of BBL) die een ICT-opleiding volgen. Een wijze van invulling mag geen conflicterende situaties opleveren. Opdrachtnemer dient hierover tijdig af te stemmen met Opdrachtgever en/of Deelnemer(s). Opdrachtgever en/of Deelnemer(s) hebben het recht om een door Opdrachtnemer beoogde wijze van invulling van zijn SR-verplichting, om zwaarwegende redenen, gemotiveerd te weigeren. Opdrachtnemer kan Opdrachtgever en/of Deelnemers niet verplichten in meer of mindere mate bij te dragen aan de invulling van zijn SR-verplichting.

M.6 Opdrachtnemer legt jaarlijks verantwoording af aan Opdrachtgever over de voortgang van de invulling van zijn SR-verplichting, middels oplevering van Bijlage 12.2 – Model rapportage SROI inclusief bewijsstukken conform R.2.

Aanvullend hierop geldt dat binnen zes maanden tot drie maanden voor het einde van de Raamovereenkomst de Opdrachtnemer een (aanvullende) rapportage oplevert om (extra) inzicht te geven in de mate waarin zijn (cumulatieve) SR-verplichting is ingevuld en er nog interventies wenselijk zijn. De laatste rapportage en bewijsmiddelen levert Opdrachtnemer binnen één tot zes maanden na het einde van de Raamovereenkomst in, op basis waarvan vastgesteld moet kunnen worden of en in welke mate aan de SR-verplichting voldaan is en of Opdrachtnemer nog een boete over het restant verschuldigd is.

In deze rapportages dient Opdrachtnemer de werkelijk gerealiseerde omzet op Opdrachten in het desbetreffende contractjaar te vermelden, alsmede de geldende en gerealiseerde SR-verplichting op grond van de toepasselijke bouwblokken en hiervoor geldende waardes.

Opdrachtnemer geeft met bewijs(stukken) inzicht in de indicaties van de ingezette of geholpen doelgroepkandidaten, de duur van hun inzet, de gerealiseerde overige vormen van

sociale impact (indien van toepassing), de in het betreffende contractjaar gefactureerde Opdrachtwaarde op grond van afgeronde en nog lopende Nadere overeenkomsten onder de Raamovereenkomst, alsmede de factuurwaarde van vergoedingen aan eventuele ingezette derden (zoals sociale onderneming, SW-bedrijf) en hun eventuele status als sociale onderneming, SW-bedrijf et cetera, voor zover Opdrachtnemer daar een beroep op doet. Uit dit bewijs moet blijken dat en in welke mate er sprake is van een vorm van sociale impact zoals genoemd in de bouwblokkentabel. Wet-/regelgeving met betrekking tot de bescherming van persoonsgegevens dient hierbij uiteraard gerespecteerd te worden. Verklaringen van derden (zoals accountant) of betrokken instanties (zoals gemeente, UWV, school, certificerende instelling) of tijdelijke inzage door betrokken personen namens Opdrachtgever in bewijsstukken, kunnen ook fungeren als bewijs. Bij het ontbreken van voldoende bewijs en/of gerede twijfel hieraan, heeft Opdrachtgever het recht om de hieraan gerelateerde SR-waarde(s) geheel of gedeeltelijk niet mee te laten tellen. Ook kan Opdrachtgever verlangen om op kosten van Opdrachtnemer een (onafhankelijke) externe audit te laten uitvoeren, waarmee kan worden vastgesteld of en in welke mate Opdrachtnemer heeft voldaan aan zijn SR-verplichting.

- M.7** Deelnemer heeft het recht om een persoon/medewerker die is ingezet ten behoeve van het voldoen aan de SR-verplichting van Opdrachtnemer, in dienst te nemen.

Opdrachtnemer garandeert zonder enig voorbehoud dat hij geen relatie- of concurrentiebedingen of bepalingen anderszins met vergelijkbare strekking met social return kandidaten overeenkomt of overeengekomen is, dan wel dat hij daarvan in voorkomend geval volledige afstand doet zowel jegens Opdrachtgever/Deelnemer, als jegens de betreffende medewerker, als dat beding of die bepaling op enigerlei wijze een overeenkomst belemmert voor de inzet van de betreffende medewerker bij Opdrachtgever/Deelnemer, ongeacht op welke wijze of via welke contractuele partijen de medewerker aan Opdrachtgever/Deelnemer ter beschikking gesteld wil worden. Dit geldt eveneens in situaties waarin de medewerker zelf besluit om in dienst te treden bij Deelnemer.

De overgang van de social return medewerker naar indiensttreding bij Deelnemer geschiedt zonder dat Opdrachtnemer aanspraak kan maken op een geldelijke vergoeding.

Specifieke voorschriften met betrekking tot diversiteit en inclusie

- M.8** Alle ministeries en andere rijksorganisaties hebben het "Charter Diversiteit" van SER Diversiteit in Bedrijf ondertekend en zich eraan gecommitteerd. SER Diversiteit in Bedrijf is een project van de Sociaal Economische Raad (SER). Het bevordert diversiteit en inclusie op de werkvloer en ondersteunt o.a. via het Charter Diversiteit organisaties bij het opzetten, uitvoeren en monitoren van hun diversiteitsplannen. Zie: <https://www.ser.nl/nl/thema/diversiteitinbedrijf/charter-diversiteit>

Opdrachtgever verwacht dat Opdrachtnemer (inclusief onderaannemers) zich inspannt om de in het kader van deze Raamovereenkomst te leveren diensten op een inclusieve wijze uit te voeren. Opdrachtnemer draagt op die wijze bij aan een inclusieve samenleving, zijn eigen productiviteit en via uit te voeren Opdrachten ook aan een inclusievere Rijksoverheid.

Opdrachtnemer tekent binnen één (1) jaar na ingangsdatum van de Raamovereenkomst het "Charter Diversiteit" van SER Diversiteit in Bedrijf, committeert zich aan dit Charter en/of zet een vergelijkbaar instrument in waarmee Opdrachtnemer zich committeert aan zelf opgestelde doelen om diversiteit en inclusie op de werkvloer te bevorderen.

Als Opdrachtnemer het Charter Diversiteit ondertekent, dient hij binnen zes maanden na ondertekening bij SER Diversiteit in Bedrijf een Plan van Aanpak in te dienen en jaarlijks te rapporteren over de voortgang hiervan. Bij toepassing van een vergelijkbaar instrument, past Opdrachtnemer ook een vergelijkbare mate van verantwoording toe. Opdrachtnemer stuurt Opdrachtgever kopieën van het ondertekende Charter (of vergelijkbaar instrument), het Plan van Aanpak en de voortgangsrapportages.

Vanwege het grote aantal aanvragers dient Opdrachtnemer zich na gunning aan te melden als toekomstig ondertekenaar bij Diversiteit in Bedrijf, zodat SER Diversiteit in Bedrijf zicht krijgt op het aantal aanvragen dat zij kunnen verwachten.

Als SER Diversiteit in Bedrijf na gunning van deze Raamovereenkomst geen nieuwe aanmeldingen voor het Charter Diversiteit accepteert en het aanmeldingsformulier daarom niet beschikbaar is, dient Opdrachtnemer binnen één (1) jaar na de start van de Overeenkomst om een vergelijkbaar instrument in te zetten waarmee Opdrachtnemer zich committeert aan zelf opgestelde doelen om diversiteit en inclusie op de werkvloer te bevorderen.

Een vergelijkbaar instrument is dat Opdrachtnemer een eigen rechtsgeldige verklaring overlegt die - met of zonder betrokkenheid van SER Diversiteit in Bedrijf – onder meer aangeeft dat Opdrachtnemer:

- (a) de toepassing van de principes van gelijke kansen wil bevorderen en diversiteit en inclusie ziet als meerwaarde voor het bereiken van de organisatiedoelstellingen;
- (b) op welke onderdelen Opdrachtnemer de diversiteit en inclusie in de organisatie concreet wil bevorderen;
- (c) Opdrachtnemer binnen 6 maanden na deze verklaring een Plan van Aanpak zal uitwerken waarin zijn onderneming concreet aangeeft hoe Opdrachtnemer dat gaat realiseren;
- (d) Opdrachtnemer met de ondernemingsraad/personneelsvertegenwoordiging / vertegenwoordigers van medewerkers een dialoog start/vervolgt over het uitwerken en toepassen van het diversiteitsbeleid;
- (e) Opdrachtnemer de medewerkers informeert over de betrokkenheid en resultaten op het gebied van diversiteit en inclusie;
- (f) Opdrachtnemer ten minste jaarlijks verslag doet over de voortgang in het behalen van die doelen ten aanzien van het bevorderen van diversiteit en inclusie. Dat verslag publiceert Opdrachtnemer openbaar of is Opdrachtnemer bereid zonder voorwaarden te versturen naar ieder die daar om vraagt.

Bijlage 1 - Classificatiematrix

	A Klein	B Normaal	C Groot	D Speciaal
Prijsrange (exc. Btw)	€0-10k	> €10-25k	> €25-40k	> € 40k
Generiek	A	B	C	D
1. Applicatie	1A	1B	1C	1D
2. Infrastructuur	2A	2B	2C	2D
3. Cloud	3A	3B	3C	3D
4. IoT / OT	4A	4B	4C	4D
5. Overig	5A	5B	5C	5D

Bedragen exclusief btw; bovengrenzen inbegrepen. Met "k" wordt duizend euro bedoeld.

Uitsluitend de maximale totaalprijs van de toepasselijke classificatie is bindend. Een Offerte onder de genoemde ondergrens is om die reden niet ongeldig, mits deze overigens aan de gestelde eisen voldoet. Voor klasse D bevat de classificatiematrix geen maximale totaalprijs.

Onderstaand de onderscheidende kenmerken die richtinggevend zijn voor de te kiezen classificatie. Onderstaande nadere invulling is echter niet limitatief noch randvoorwaardelijk. Het zal altijd afhankelijk zijn van de betreffende voorgenomen opdracht welke (combinatie van) specifieke elementen de classificatie bepalen. Dat kunnen dus ook aanvullende elementen zijn die onderstaand niet expliciet zijn genoemd:

Generiek

Deze generieke kenmerken zijn altijd van toepassing en staan los van de classificatie van het doelwit/object (1 t/m 5).

~~Audit-proof betekent dat een accountant kan vaststellen dat het opgeleverde eindresultaat navolgbaar, betrouwbaar en in overeenstemming (compliant) is met relevante standaarden/afspraken en wet-/regelgeving, zodat hiermee zekerheid verkregen kan worden over de kwaliteit van uitvoering en resultaten.~~

Onder audit-proof wordt verstaan dat de rapportage zodanig is onderbouwd dat bevindingen controleerbaar en herleidbaar zijn. Dit kan onder meer blijken uit een duidelijke relatie tussen het onderzochte object of onderdeel, de geconstateerde bevinding, de wijze waarop deze is vastgesteld, het bijbehorende risico en de onderbouwing of bewijslast waarop de bevinding is gebaseerd. De rapportage bevat voldoende informatie om de bevinding door een deskundige derde te kunnen begrijpen en, voor zover redelijkerwijs mogelijk, te reproduceren. De vorm en omvang van de bewijslast zijn proportioneel aan de aard van de test en de betreffende bevinding. Met audit-proof wordt geen afzonderlijke accountantsverklaring, assuranceverklaring of certificering bedoeld. Het aanleveren van alle ruwe scanresultaten, tooling-output of technische artefacten is niet standaard vereist, tenzij dit in het Plan van Aanpak is overeengekomen of voor verificatie noodzakelijk is.

TBB = Te Beschermen Belangen: Een organisatie heeft haar eigen organisatie doelstellingen en heeft er belang bij dat deze doelstellingen worden behaald. Om deze doelstellingen te behalen wordt er informatie verwerkt en zijn er processen ingericht, die worden ondersteund door netwerk – en informatiesystemen. Iedere organisatie heeft haar eigen unieke te beschermen belangen. LET OP: geheimhouding c.q. Bijzondere Informatie is altijd een TBB, maar een TBB is niet altijd gerubriceerd.

~~Deze kenmerken zijn alternatief gesteld, niet cumulatief als ook niet limitatief.~~

Er bestaat geen één-op-één relatie tussen de classificatiecategorieën Klein, Normaal, Groot en Speciaal en de toepasselijke TBB-niveaus. De classificatie van een Opdracht en het toepasselijke TBB-niveau worden op basis van verschillende criteria bepaald. Het TBB-niveau is afhankelijk van het te beschermen belang van de betreffende Opdracht. Een Opdracht met TBB-2/STG-G of TBB-3/STG-C kan een relevante aanwijzing vormen voor classificatie 'Speciaal'. Deze indicator is echter uitsluitend richtinggevend en wordt in onderlinge samenhang met de andere kenmerken beoordeeld.

De vermelding van TBB-niveaus in de classificatiematrix vormt geen limitatieve of randvoorwaardelijke koppeling tussen een TBB-niveau en een classificatiecategorie. Een TBB-niveau bepaalt niet automatisch de classificatie en een eenmaal gekozen classificatie sluit een ander toepasselijk TBB-niveau niet uit. TBB-

2 kan eveneens van toepassing zijn indien het te beschermen belang van de betreffende Opdracht daartoe aanleiding geeft. Het toepasselijke TBB-niveau wordt per Nadere Opdracht vastgesteld en voorafgaand aan de uitvoering kenbaar gemaakt.

De kenmerken in de classificatiematrix zijn richtinggevend, niet limitatief en niet cumulatief vereist. Zij worden in onderlinge samenhang beoordeeld. Er geldt geen vooraf vastgestelde rangorde van afzonderlijke kenmerken. Het voldoen aan één afzonderlijk kenmerk leidt niet automatisch tot indeling in de betreffende klasse. Eventuele aanvullende kenmerken moeten objectief verband houden met de aard, omvang, complexiteit, duur of het belang van de Opdracht.

A	B	C	D
<p>Geen combinatie 1-5</p> <p>Uitvoering (zonder intake): tot 4 dagen</p> <p>Tot 1 specifiek normenkader</p> <p>Richtinggevende indicator: DepV TBB 4</p>	<p>Audit-proof op Klein</p> <p>Mogelijke combinatie 1-5: 2 stuks</p> <p>5-10 dagen</p> <p>Richtinggevende indicator: DepV TBB 4</p> <p>Toe te passen security policies DigiD, CIS hardening (of equiv.) De test raakt bijzondere persoonsgegevens</p>	<p>Audit-proof</p> <p>Mogelijke combinatie 1-5: 3 stuks</p> <p>10 dagen – 3 weken</p> <p>Richtinggevende indicator: DepV TBB 4</p> <p>Toe te passen security policies + review CIS hardening (of equiv.) incl detail-review De test raakt bijzondere persoonsgegevens</p>	<p>Audit-proof</p> <p>Mogelijke combinatie 1-5: 4 en meer stuks</p> <p>> 3 weken</p> <p>Richtinggevende indicator: TBB-2/STG-G of TBB-3/STG-C; ook TBB-4 kan bij deze klasse passen.</p> <p>Toe te passen security policies + review</p> <p>De test raakt bijzondere persoonsgegevens</p>

1. Applicatie

Web, mobile, desktop etcetera.

1A	1B	1C	1D
<ul style="list-style-type: none"> - Enkele niet-complexe applicatie of evt. enkele simpele applicaties - Beperkte hoeveelheid koppelingen/afhankelijkheden - Kan onder "standaardpakket". 	<ul style="list-style-type: none"> - Enkelvoudige complexe applicatie zonder randzaken/afhankelijkheid - Simpele applicatie met ketentest en/of noemenswaardige interne (binnen dezelfde IT-omgeving) afhankelijkheden. 	<ul style="list-style-type: none"> - Complexe applicatie met veel ketentesten en interne afhankelijkheden. - Applicatietest incl integratietesten (zoals IAM i.r.t. AD/AAD). 	<ul style="list-style-type: none"> - Combinatie van gerelateerde (complexe) applicaties incl. ketentest e.a.

2. Infrastructuur

2A	2B	2C	2D
<ul style="list-style-type: none"> - Simpele / kleine / gestandaardiseerde omgeving – bijv. Windows omgeving (AD) met klein aantal (<50) servers - Bij zwaar gestandaardiseerde omgevingen 50 t/m 100 systemen. 	<ul style="list-style-type: none"> - Gemiddeld complexe omgeving, dan wel kleiner dan 150 systemen. - Kan verschillende OS-soorten bevatten. - identiteitsgegevens-verzamelingen/IAM (bijv. Entra/AAD componenten) - Kleine, doch complexe (server)omgeving 	<ul style="list-style-type: none"> - (Middel)grote complexe omgeving met verschillende OS-soorten, complexe netwerkinrichting, incl. controles op toepassen standaarden zoals CIS en compliance aan normen zoals DORA/ETSI. 	<ul style="list-style-type: none"> - Diepgaande testen op complexe omgevingen met veel relaties/afhankelijkheden, >500 systemen in verschillende omgevingen met netwerkscheiding, auditrapporten en uitgebreide controles op meerdere standaarden.

	(kleiner dan 50 te testen systemen) - Middelgrote, niet zeer complexe omgeving.		
--	--	--	--

3. Cloud

Storage is onderdeel van de cloud-omgeving

3A - Enkele cloud-omgeving met een beperkt aantal "applicaties" of systemen. - 'Simpele' omgeving met gestandaardiseerd endpoint management (bijv. Azure ARC).	3B - Enkele cloud-omgeving met aanvullende compliance eisen of grotere aantallen systemen/complexiteit, beperkte hoeveelheid tenants.	3C - Simpele multi-cloud of complexe single cloud incl. containers, infra, applicaties en compliance checks.	3D - Complexe multi-cloud omgeving of grote, zeer complexe single cloudomgevingen incl aanvullende eisen.
---	---	--	---

4. IoT/OT

Internet of Things / Operationele Technologie

4A - Simpele omgeving (beperkte hoeveelheid modellen/soorten (I)OT apparaten).	4B - Veel segmentatie, gestandaardiseerde apparaten - Weinig segmentatie, veel verschil binnen de omgeving, omvang beperkt.	4C - Veel segmentatie, veel verschillende (soorten) apparaten - Complexe toegangscontroles en eisen aan ontsluiting.	4D - Naast segmentatie ook bijv. access-gates en network-boundaries aangevuld met specifieke eisen en groot scala verschillende systemen.
--	--	---	---

5. Overig

~~Deze categorie betreft pentesten die niet binnen de domeinen 1 tot en met 4 vallen. De verdere invulling ontbreekt logischerwijs, omdat het een vooraf onbepaalde restcategorie betreft. De classificatie A t/m D blijft van toepassing; de omvang, complexiteit en het belang van de voorgenomen pentest bepalen de indeling. Deelnemers classificeren de opdracht in de Aanvraag, waarna Opdrachtnemers deze classificatie kunnen bevestigen of weerspreken tijdens de minicompetitie of toerbeurtschema.~~

~~Voorbeeld restcategorie: Vertrouwd Toegangspad test (VTP). Dit type onderzoek richt zich op een specifiek toegangspad of keten en valt daardoor niet binnen de vaste domeinen Applicatie, Infrastructuur, Cloud of IoT/OT. De kenmerken van een VTP test verschillen per organisatie en per object, waardoor vooraf geen vaste indeling kan worden bepaald.~~

5A - ...	5B - ...	5C - ...	5D - ...
--------------------	--------------------	--------------------	--------------------

Categorie 5 "Overig" betreft penetratietesten die binnen de scope van de Raamovereenkomst vallen, maar niet onder de categorieën 1 tot en met 4 kunnen worden gebracht. Deze categorie verruimt de scope van de Raamovereenkomst niet.

De indeling in klasse A, B, C of D vindt plaats aan de hand van dezelfde generieke kenmerken als bij de overige categorieën. Het bijbehorende verdeelmechanisme is van toepassing. Het TBB-niveau wordt afzonderlijk bepaald op basis van het te beschermen belang van de Opdracht.

Deelnemer vermeldt de classificatie in de Aanvraag. Opdrachtnemers kunnen deze bevestigen of gemotiveerd weerspreken. Een mogelijk voorbeeld is een Vertrouwd Toegangspad-test (VTP-test), voor zover deze niet onder de categorieën 1 tot en met 4 valt.

Bijlage 2 – Model standaardrapport

1. Documentbeheer

- └ Opdrachtgever
- └ Projectnummer/-naam
- └ Start- en einddatum onderzoek
- └ Versienummer:
- └ Versiedatum
- └ Versienaam en -omschrijving, inclusief documentclassificatie (*rubriceringsniveau, wel/niet bewerkt voor bredere distributie-doeleinde*)
- └ Verantwoordelijke rapporteur/auteur
- *Optioneel (bij publieksversie): Bij de uitvoering ingezette professionals*
- └ Distributielijst, verspreidingsmethode en reviewers
- └ Review en accordering:
 - Tekst waarin wordt bevestigd dat de rapportage accuraat en naar waarheid is opgesteld
 - Bevestiging dat een review is uitgevoerd (door overige professionals betrokken bij het onderzoek dan wel door andere/externe reviewers)
 - Handtekening rapporteur (fysiek of digitaal)
- └ Voorwaarden gebruik rapportage en vertrouwelijkheid

2. Managementsamenvatting

- └ Start- en einddatum onderzoek
- └ Overzicht gebruikte standaarden
- *Optioneel: Aangeleverde CIA-scores per scope-object*
- *Optioneel: Root-cause analyse*
- └ Overzicht van aangetroffen kwetsbaarheden / bevindingen per CVSS-risicocategorie
- └ Fysieke locaties (land) van onderzochte objecten en naleving wet- en regelgeving
- └ Samenvatting van aanbevelingen voor verbetering

3. Inleiding

- └ Doel en reikwijdte van de test
- └ Achtergrondinformatie over de organisatie
- └ Assumpties en beperkingen
- └ Relevante standaarden en methodologieën

4. Scope

- └ Scope-objecten en afbakening
- └ Overzicht van afwijkingen ten opzichte van het Plan van Aanpak
- └ Fysieke locaties (land) van onderzochte objecten en naleving wet- en regelgeving

5. Methodiek

- ↵ **Uitvoering volgens fasering Pentest Execution Standard of andere standaard**
- ↵ **Toegepaste testmethodieken**
 - Aanvalsperspectief, beschikbare voorkennis en assume breach principe
 - Gebruikte standaarden, richtlijnen, referentiebronnen
- ↵ **Toegepaste classificatiemethodiek van bevindingen: CVSS**
- ↵ **Tijddlijn met uitgevoerde acties**

6. Bevindingen

- ↵ **Indeling per scope-object**
- ↵ **Beschrijving kwetsbaarheden**
(incl. referenties naar CVE-nummers of evt. nieuwe CVE-aanvraag)
- ↵ **CVSS-score, classificatie en vectorstring**
- ↵ **Impactanalyse**
(incl. impact op omliggende systemen)
- ↵ **Reproductiestappen en gebruikte exploits**
- ↵ **Aanbevelingen met verwijzing naar CWE-database**

7. Conclusie en aanbevelingen

- ↵ **Samenvatting van de belangrijkste bevindingen**
- ↵ **Aanbevelingen voor verbeteringen, inclusief een advies over de prioritering van de aanbevelingen**

Bijlagen

- ↵ **Begrippenlijst / Verklarende woordenlijst**
- ↵ **Onderzoeksteam en individuele certificeringen**
 - Naam rapporteur en zijn/haar certificeringen
 - Namen overige betrokken professionals en hun certificeringen
 - *Optioneel (op verzoek Deelnemer):* Informatie over validatie van certificeringen en eventueel CCV-keurmerk van de organisatie
- ↵ **Hulpmiddelen**
 - Beschrijving hulpmiddelen
 - Versienummer per hulpmiddel
 - URL naar download/informatiepagina hulpmiddel
 - *Optioneel (op verzoek Deelnemer):* **Overzicht van ontvangen documenten en bestanden**
 - *Optioneel:* Documenten, beschrijvingen en cryptografische hashes
 - *Optioneel:* Bestanden, beschrijvingen en cryptografische hashes
- ↵ **Overzicht verstrekte accounts (inclusief rollen en permissies)**
 - Accounts, bijbehorende scope-objecten, rollen en permissies
- **Optioneel (op verzoek Deelnemer): Uitgevoerde scans**
 - *Optioneel:* Scanresultaten en scope-objecten
 - *Optioneel:* Ruwe scanoutput
 - Volledige CVSS-berekeningen en vectorstrings
- **Optioneel (op verzoek Deelnemer): Bewijsmateriaal**
 - *Optioneel:* Cryptografische hashes voor bewijsmateriaal
 - *Optioneel:* Bewijs van gedetecteerde en geïdentificeerde toegangswegen
 - *Optioneel:* Bewijsvoering dat tests op scope-objecten zijn uitgevoerd en niet op beschermende maatregelen
- **Optioneel (op verzoek Deelnemer): Checklists**
 - *Optioneel:* Overzicht van gebruikte standaarden en frameworks

- *Optioneel*: Checklist per standaard
- Status (Getest/Niet getest/Valt niet te testen)
- Toelichting bij niet-geteste onderdelen
- Afwijkingen en bevindingen gekoppeld aan specifieke tests
- ↵ **Beheer van testresultaten**
 - Afspraken over veilige verwerking van resultaten
 - *Optioneel*: Afspraken over versleuteling/hashing ter beveiliging en verificatie van integriteit
 - Afspraken over bewaartermijnen
- ↵ **Lijst van onbenaderbare/onbereikbare scope-objecten**
 - Scope-objecten die niet bereikbaar waren
 - Hoe bereikbaarheid is vastgesteld
 - Impact op de testresultaten