Ministerie van Onderwijs, Cultuur en Wetenschap

NIS2 programma OCW brede Retainer Overeenkomst

Bijlage 1 - Programma van eisen

IUC-Noord

17-12-2025

Colofon

Titel	NIS2 programma OCW brede Retainer overeenkomst
Document	Bijlage 1 - Programma van eisen
Afzendgegevens	Inkoop Uitvoeringscentrum Noord (IUC-Noord) Dienst Uitvoering Onderwijs Ministerie Onderwijs, Cultuur en Wetenschap Cascadeplein 3, verdieping 3 9726 AH Groningen Postbus 30155 9700 LG Groningen
Datum	17-12-2025

INHOUD

1 Algemeen 4

2 Incident Response en Forensics 5

3 SLA ..... Fout! Bladwijzer niet gedefinieerd.

4 Beveiliging en Privacy 9

5 Prijs en facturatie 10

6 Exitplan 10

Bijlage 1 - Programma van eisen

In dit Programma van eisen is een onderverdeling in kopjes aangebracht ter bevordering van de leesbaarheid. De eisen die specifiek van toepassing zijn op de (uitvoering van de) opdracht staan hier omschreven. De in dit hoofdstuk opgenomen eisen zijn de minimale vanuit de overeenkomst geldende kaders. Door in te schrijven op de aanbesteding verklaart Opdrachtnemer dat hij voor de uitvoering van de opdracht minimaal aan deze eisen voldoet.

1 ALGEMEEN

	Algemeen
1.1	Alle informatie, ongeacht de vorm, die in het kader van deze aanbesteding is beschikbaar gesteld, behoort tot het bedrijfskapitaal van Opdrachtgever. Deze informatie mag alleen door Opdrachtnemer worden gebruikt voor de offerte die Opdrachtnemer aan Opdrachtgever doet.
1.2	De Opdrachtnemer zal zorgdragen dat derde partijen die betrokken zijn bij de uitvoering van (een deel van) de opdracht gebonden zijn aan verplichtingen die ten minste gelijkwaardig zijn aan de contractuele verplichtingen van de Opdrachtnemer zelf uit hoofde van de dienstverleningsovereenkomst, waaronder- maar niet beperkt tot- verplichtingen inzake geheimhouding, informatiebeveiliging en vertrouwelijkheid.
1.3	De Opdrachtnemer zal voor Opdrachtgever bepaalde werken en materialen ontwikkelen en/of vervaardigen in het kader van de dienstverleningsovereenkomst. De ontwikkelde en/of vervaardigde documenten, materialen, programmatuur en overige werken van intellectuele aard behoren tot eigendom van de Opdrachtgever.
1.4	IB-Incidenten die bij Opdrachtnemer worden gemeld zonder tussenkomst van de Opdrachtgever vallen niet onder de werking en verplichtingen van deze overeenkomst.
1.5	De Opdrachtnemer stelt één (1) centraal aanspreekpunt (één functionaris inclusief plaatsvervanger of één team) aan voor alle communicatie met betrekking tot de uitvoering van deze dienstverleningsovereenkomst.
1.6	Het personeel dat Opdrachtnemer inzet voor de uitvoering van de opdracht gedurende de looptijd van de dienstverleningsovereenkomst zijn zowel medior als op senior niveau op het gebied van informatiebeveiliging. Opdrachtgever stelt als eis dat een medior minimaal 3 tot 5 jaar aantoonbaar werkervaring heeft op het gebied van informatiebeveiliging (en over relevante kennis beschikt binnen het kader van deze opdracht). Opdrachtgever stelt als eis dat een senior minimaal 5 jaar aantoonbaar werkervaring heeft op het gebied van informatiebeveiliging (en over relevante kennis beschikt binnen het kader van deze opdracht).

2 IB-INCIDENT RESPONSE EN FORENSICS

	IB-Incident Response en Forensics
2.1	Alle schriftelijke en mondelinge communicatie tussen partijen geschiedt in de Nederlandse taal. Geautomatiseerde systeeminformatie, zoals logging, behoeft niet in het Nederlands te worden vertaald. In het geval van enige vertaling van documenten of communicatie geldt dat de Nederlandse tekst te allen tijde leidend is en bindend is. Bij tegenstrijdigheid tussen de Nederlandse tekst en een vertaling prevaleert de Nederlandse tekst, tenzij uitdrukkelijk schriftelijk anders is overeengekomen.
2.2	De Opdrachtnemer levert ondersteuning bij IB-incident response en digitaal forensisch onderzoek met een beschikbaarheid van vierentwintig uur per dag, zeven dagen per week, driehonderdvijfenzestig dagen per jaar (24/7/365). Binnen maximaal zestig (60) minuten na ontvangst van een melding stelt de Opdrachtnemer een team van informatiebeveiligingsexperts operationeel.
2.3	De Opdrachtnemer verplicht zich binnen uiterlijk twee (2) uur na ontvangst van de melding van een (vermoeden van een) IB-incident met een onderzoek te starten, waarin een eerste inschatting wordt gemaakt van de reikwijdte en de impact van het IB-incident. Dit onderzoek kan in onderling overleg op afstand (remote) plaatsvinden. De Opdrachtnemer zal deze verplichting expliciet vastleggen in de SLA.
2.4	De Opdrachtnemer verplicht zich er toe dat binnen een termijn van drie (3) uur na eerste melding van een geconstateerd IB-incident deskundigen fysiek aanwezig zijn op de door Opdrachtgever opgegeven locatie(s). De aanwezigheid heeft tot doel het IB-incident doeltreffend te verhelpen en de daarmee gepaard gaande schade zoveel mogelijk te beperken. Op basis van de incidentclassificatie en een afweging van de risico's kan in onderling overleg met de Opdrachtgever worden besloten de incidentafhandeling geheel of gedeeltelijk op afstand te laten plaatsvinden. De definitieve beslissing omtrent de locatie(s) waar de werkzaamheden worden verricht, berust bij de Opdrachtgever en is bindend voor de Opdrachtnemer. Nadere uitwerking van deze verplichting dient te worden vastgelegd in de SLA.
2.5	De Opdrachtnemer draagt zorg voor een adequaat ingericht incident response-proces, waarin de verantwoordelijkheden, bevoegdheden en taken een getraind incidentresponse team expliciet en aantoonbaar zijn vastgelegd.
2.6	Elke medewerker van de Opdrachtnemer die wordt ingezet tijdens een IB-incident in de rol van Forensisch Expert dient in het bezit te zijn van minimaal één (1) erkende forensische certificering, zoals bijvoorbeeld een GIAC-certificering (GCFA) of een daarmee gelijkwaardig certificaat. Dit moet op verzoek door Opdrachtnemer worden aangetoond. Indien een medewerker van de Opdrachtnemer wordt ingezet als Forensisch of Recovery Expert zonder genoemde certificering, dient deze medewerker te werken onder directe supervisie en één-op-één begeleiding van een medewerker die voldoet aan de gestelde certificeringseisen. De Opdrachtnemer dient deze kwalificaties schriftelijk te kunnen aantonen op verzoek van de opdrachtgever.
2.7	De Opdrachtnemer levert, afhankelijk van het soort melding, passende informatiebeveiligingsexpertise en minimaal de volgende diensten: a. Initiële en acute respons b. Root-cause analyse (RCA)* c. Recovery services** d. Digitaal forensisch onderzoek e. Compromise assessment/analyses met betrekking tot malware, phishing en ransomware incl. mitigatie-herstelmaatregelen (bijv. het verwijderen van malware en ondersteuning bij ransomware-aanval), f. Incident -en klantcommunicatie (waaronder met de threat actor),

	IB-Incident Response en Forensics
	g. Advisering bij bestuurlijke besluitvorming h. Juridische ondersteuning i. Second opinion j. Adviseringen (in het kader van mitigatie-en herstelmaatregelen denk hierbij aan containment, eradiction en recovery) k. Incident evaluatie incl. rapportages Geleverde ondersteuning en advies heeft betrekking op IB-incidenten. Hieronder kunnen vallen: • Ransomware & afpersing • Datalekken & ongeautoriseerde exfiltratie • Identiteits- & toegangscompromittering • Business Email Compromise & social engineering • Cloud- & SaaS-inbraken • Supply-chain- & derde-partij-aanvallen • Exploitatie van kwetsbaarheden • Malware & persistent threaths • Netwerk- & perimeter-inbraken • Insider-dreigingen Eventuele onbenutte overschotten worden benut in het daarop volgende jaar, voor geplande inzet van aanvullende diensten, zoals trainingen, workshops, oefeningen, lessons learned sessions, table top exercities, Threat hunting, (pen)testen, kwetsbaarheden assesments, onderhoud, audits en kwaliteitsmetingen. * Root cause analyse Bij de ondersteuning van een root cause onderzoek kan het rapporteren hierover onderdeel uitmaken van de gevraagde support. Onder een root cause onderzoek verstaan wij naast het verzamelen, analyseren en interpreteren van digitale bewijsstukken met o.a. als doel om een objectief en gedetailleerd begrip te krijgen over de omvang, tijdsbestek en impact van het (vermoedelijke) incident. Rapportage van dit onderzoek dienen tenminste de volgende onderwerpen te worden behandeld: • het initiële toegangspunt • de capabilities van de malware • de duur van de compromittatie • de gebruikte tactieken, technieken en procedures • het verkregen toegangsniveau per systeem • welke bedrijfsgegevens (potentieel) zijn geëxfiltreerd • bewijsmateriaal ter identificatie van de aanvaller - Advies mitigerende maatregelen dan wel wegnemen van de root cause ** Recovery services De Opdrachtnemer adviseert OCW in geval van een dergelijk incident ten aanzien van recovery services om de impact van een digitaal incident voor OCW te minimaliseren zodat de dienstverlening spoedig kan worden hervat. Recovery services kunnen worden omschreven als activiteiten en processen die uitgevoerd moeten worden om de normale werking van systemen, applicaties en IT-middelen te herstellen.
2.8	De Opdrachtnemer garandeert dat uitsluitend personeel dat een geverifieerde en geldige screening heeft ondergaan, belast wordt met de uitvoering van werkzaamheden binnen het kader van deze opdracht. De screening dient te voldoen aan geldende wettelijke eisen op het gebied van integriteit, betrouwbaarheid en veiligheid, waarbij het screeningsprofiel passend dient te zijn bij de aard van de uit te voeren werkzaamheden. De Opdrachtnemer waarborgt dat alle medewerkers die worden ingezet bij een IB-incident, voorafgaand aan aanvang van de werkzaamheden minimaal een passende en geldige Verklaring Omtrent Gedrag (VOG) hebben ingediend bij de Opdrachtnemer.

	IB-Incident Response en Forensics
	De Opdrachtgever behoudt zich het recht voor om, met inachtneming van de geldende privacywetgeving, inzage te nemen in de ingediende VOG en screeningsprofielen voor zover dit noodzakelijk wordt geacht ter beoordeling van het personeel welke belast wordt met de uitvoering van werkzaamheden binnen het kader van deze opdracht.
2.9	De Opdrachtnemer is verplicht alle tijdens de uitvoering van de opdracht verkregen, verwerkte of onderzochte data, alsmede alle fysieke en digitale datadragers die (mede)gegevens van de Opdrachtgever bevatten, te allen tijde op zorgvuldige, vertrouwelijke en beveiligde wijze te bewaren, over te dragen en na beëindiging van de opdracht volledig, aantoonbaar en op beveiligde wijze te vernietigen, tenzij schriftelijk anders is overeengekomen met Opdrachtgever.
2.10	De Opdrachtnemer beschikt over schriftelijk vastgelegde en aantoonbare procedures voor het veilig uitwisselen van informatie en apparatuur tussen Opdrachtnemer en Opdrachtgever. De procedures dienen o.a. te voldoen aan vigerende wet- en regelgeving waaronder in ieder geval, maar niet uitsluitend de AVG en geldende normenkaders zoals de Baseline Informatiebeveiliging Overheid (BIO).
2.11	De Opdrachtnemer is gehouden binnen één (1) maand na de melding van een IB-incident, volledig en schriftelijk te rapporteren aan de Opdrachtgever. Deze rapportage dient minimaal te bevatten: a. Logboek van gebeurtenissen (timeline) b. Inzet uren functionarissen c. Een gedetailleerde analyse van de oorzaken van het IB-incident, inclusief technische en organisatorische factoren die tot het IB-incident hebben geleid (o.a. Indicators of Compromise (IOC's) d. Een volledige beschrijving van de impact van het IB-incident op de dienstverlening, systemen en data van de Opdrachtgever e. De genomen maatregelen en herstelacties die zijn of worden geïmplementeerd om herhaling van soortgelijke IB-incidenten te voorkomen, inclusief concrete verbetermaatregelen en geplande actiepunten. f. Een evaluatie van de effectiviteit van de getroffen maatregelen De rapportage en de daarin opgenomen maatregelen worden ter beoordeling voorgelegd aan de Opdrachtgever en dienen te voldoen aan de relevante wet-en regelgeving, waaronder de AVG en de Nederlandse implementatie van de Network and Information Security directive (NIS2-richtlijn) en veiligheidsnormen zoals ISO/IEC27001 en actuele BIO. Nadere uitwerking van deze verplichting dient te worden vastgelegd in de SLA.
2.12	De Opdrachtnemer hanteert een gedocumenteerd communicatieplan voor interne en externe meldingen, opvolging en afhandeling van IB-incidenten. De Opdrachtnemer garandeert dat IB-incidenten tijdig worden gedetecteerd, geanalyseerd, gerapporteerd en verholpen, teneinde de nadelige gevolgen en risico's voor de Opdrachtgever tot een minimum te beperken.

3 SERVICE DOCUMENTATIE

	Service Documentatie
3.1	Nadere uitvoeringsafspraken betreffende de diensten en prestaties worden vastgelegd in Dossier Afspraken en Procedures (DAP) en Service Level Agreement (SLA). Beide documenten maken een integraal en onlosmakelijk onderdeel uit van de dienstverleningsovereenkomst. De Opdrachtnemer en Opdrachtgever zorgen dat de DAP en SLA uiterlijk binnen drie (3) maanden na ingang van de dienstverleningsovereenkomst worden ondertekend en als bindende documenten worden toegevoegd aan de dienstverleningsovereenkomst.
3.2	Alle kosten die voortvloeien uit het opstellen, afstemmen, onderhouden en uitvoeren van de DAP en SLA, waaronder begrepen de kosten voor beheers-,overleg- en rapportageactiviteiten, dienen volledig te zijn verdisconteerd in de door de Opdrachtnemer uitgebrachte aanbieding.
3.3	De Opdrachtnemer is verantwoordelijk voor het tijdig opstellen en ter goedkeuring voorleggen van de DAP en SLA.
3.4	In de DAP en SLA wordt vastgelegd dat minimaal éénmaal per jaar een evaluatiegesprek plaatsvindt tussen de Opdrachtnemer en Opdrachtgever. Het doel van dit overleg is het beoordelen en bespreken van de mate waarin de uitvoering van de werkzaamheden en dienstverlening overeenkomstig de overeengekomen kwaliteitsniveaus plaatsvindt. De periodieke door de Opdrachtnemer te verstrekken digitale rapportages vormen de primaire grondslag voor dit evaluatiegesprek. Indien uit het evaluatiegesprek blijkt dat de dienstverlening niet in overeenstemming is met de overeengekomen kwaliteitsniveaus, prestatienormen of overige afspraken uit de DAP en SLA, stelt de Opdrachtnemer in overleg met de Opdrachtgever een verbeterplan op. Dit verbeterplan bevat ten minste de te nemen corrigerende maatregelen, de uitvoeringstermijnen daarvan en de verantwoordelijke functionarissen. Het verbeterplan dient binnen de door de Opdrachtgever vastgestelde termijn ter goedkeuring aan de Opdrachtgever te worden voorgelegd. Na goedkeuring maakt het verbeterplan deel uit van de DAP en SLA en is de Opdrachtnemer gehouden tot de uitvoering daarvan. De definitieve frequentie en planning van deze gesprekscyclus worden na de gunning in overleg tussen Opdrachtnemer en Opdrachtgever vastgesteld in de DAP en SLA.
3.5	De DAP en SLA wordt beheerd door de Opdrachtnemer. De Opdrachtgever is eigenaar van de DAP en SLA. Beide partijen zijn gezamenlijk verantwoordelijk voor de actualiteit, inhoud, kwaliteit en borging van de afspraken die in de DAP en SLA zijn vastgelegd. De Opdrachtnemer draagt zorgt voor een periodieke herziening van de DAP en SLA, ten minste éénmaal per jaar. De resultaten van deze herziening worden ter goedkeuring aan de Opdrachtgever voorgelegd. Wijzigingen in de DAP en SLA kunnen uitsluitend plaatsvinden na voorafgaande en schriftelijke instemming van beide partijen. Indien tussen partijen verschil van inzicht ontstaat over de interpretatie of uitvoering van de DAP en SLA, treden Opdrachtnemer en Opdrachtgever onverwijld in overleg om tot een voor beide partijen aanvaardbare oplossing te komen. Tot op het moment van overeenstemming blijft de laatste rechtsgeldig vastgelegde en ondertekende versie van de DAP en SLA onverkort van kracht.
3.6	In de DAP wordt door de Opdrachtnemer een noodnummer vastgelegd met bijbehorende autorisatie- en identificatiemechanismen ter verificatie van de beller vanuit OCW.

4 BEVEILIGING EN PRIVACY

	Beveiliging & Privacy
4.1	Alle gegevens die betrekking hebben op of afkomstig zijn van de Opdrachtgever zullen te allen tijde uitsluitend worden opgeslagen, verwerkt en beheerd binnen de Europese Economische Ruimte (EER). Deze verplichting geldt tevens voor alle derde partijen die betrokken zijn bij de uitvoering van de overeenkomst. De Opdrachtgever en Opdrachtnemer binden zich eraan te voldoen aan de toepasselijke wet- en regelgeving inzake gegevensbescherming waaronder de Algemene Verordening Gegevensbescherming (AVG) en de uitvoeringswet UAVG. Doorhaling of doorgifte van deze gegevens buiten de EER is slechts toegestaan indien daartoe voorafgaande schriftelijke toestemming is verleend door de Opdrachtgever en indien passende waarborgen conform de AVG zijn getroffen. De Opdrachtnemer waarborgt dat de verwerking en opslag van persoonsgegevens te allen tijde rechtmatig, behoorlijk en transparant plaatsvindt, overeenkomstig de verplichtingen die uit deze regelgeving voortvloeien.
4.2	De Opdrachtnemer neemt passende technische en organisatorische maatregelen om de beveiliging van informatiesystemen te waarborgen conform de toepasselijke wet- en regelgeving, waaronder AVG, Archiefwet en de Nederlandse implementatie van de NIS2; Nederlandse cyberbeveiligingswet (Cbw) en Cyberbeveiligingsbesluit (Cbb)wanneer deze formeel in werking zijn getreden.
4.3	De Opdrachtgever is verwerkingsverantwoordelijke in de zin van de AVG voor alle verwerkingen die plaatsvinden in het kader van de uitvoering van de opdracht. De Opdrachtnemer treeft hierbij op als verwerker en verklaart zich te conformeren aan de verplichtingen die hieruit voortvloeien. De afspraken met betrekking tot de verwerkingen worden vastgelegd in een verwerkingsovereenkomst, die als Bijlage 4 aan de dienstverleningsovereenkomst is toegevoegd. De definitieve verwerkersovereenkomst wordt na gunning en uiterlijk binnen één (1) maand na de ondertekening van de dienstverleningsovereenkomst vastgesteld en door beide partijen rechtsgeldig ondertekend.
4.4	De Opdrachtnemer draagt zorgt voor de juistheid, volledigheid en integriteit van alle gegevensbestanden die zich onder zijn beheer bevinden in het kader van de uitvoering van de overeengekomen werkzaamheden.
4.5	De Opdrachtnemer dient aantoonbare procedures en technische maatregelen te hebben geïmplementeerd ter waarborging van de vertrouwelijkheid en integriteit van gegevens, zowel bij opslag (waaronder file servers, databases en gebruikersworkstations) als tijdens transport (waaronder systeeminterfaces, communicatie via publieke netwerken en elektronisch berichtenverkeer). Alle datatransmissies inclusies XML-feeds, dienen te geschieden via beveiligde en versleutelde verbindingen.
4.6	De Opdrachtnemer hanteert een vastgesteld privacybeleid inclusief bijbehorende procedures waarin verantwoordelijkheden, werkwijzen, en naleving van wettelijke vereisten met betrekking tot de verwerking van (persoons)gegevens zijn vastgelegd. Dit beleid voorziet in een cyclisch proces van toetsing, evaluatie en verbetering, gericht op het waarborgen van transparante naleving van wet- en regelgeving en het structureel corrigeren van eventuele geconstateerde afwijkingen.

5 PRIJS EN FACTURATIE

	Prijs en Facturatie
5.1	De Opdrachtnemer moet de opdracht uitvoeren op basis van de aangeboden uurtarieven in het prijzenblad, die bij inschrijving zijn verstrekt.
5.2	De Opdrachtnemer dient de Opdrachtgever vooraf een geschatte urenverantwoording te verstrekken voor geplande inzet van werkzaamheden.
5.3	De Opdrachtnemer dient de Opdrachtgever wekelijks een urenverantwoording te verstrekken bij geplande en directe inzet van werkzaamheden.
5.4	Niet gebruikt voorschot mag uitsluitend in afstemming met Opdrachtgever worden ingezet voor de overige dienstverlening binnen de Incident Response Retainer Services.
5.5	De Opdrachtnemer verbindt zich ertoe zich te conformeren aan de voorschriften zoals opgenomen in bijlage 6 Financiële bijsluiter OCW, inzake het elektronisch factureren aan de Rijksoverheid.
5.6	De Vergoeding kan na 23 april 2030 éénmaal per jaar per 1 januari worden bijgesteld met een percentage tot maximaal het 'CBS-prijsindexcijfer CAO lonen per uur inclusief bijzondere beloningen, categorie zakelijke dienstverlening'. Hierbij wordt telkens het maandcijfer van de voorafgaande maand november gehanteerd, waarbij het indexcijfer van november 2025 wordt gesteld op 100%. Basislink: http://statline.cbs.nl/statweb/publication/?vw=t&dm=slnl&pa=82838ned&la=nl. De Opdrachtnemer dienst uiterlijk drie (3) maanden voorafgaand aan de ingangsdatum van de indexering een schriftelijk verzoek tot prijsaanpassing in bij de Opdrachtgever. Dit verzoek bevat een gedegen onderbouwde en transparante calculatie, waaruit de opbouw en onderbouwing van de voorgestelde prijsaanpassing blijkt. Een prijsaanpassing kan uitsluitend worden doorgevoerd nadat overeenkomstig overleg heeft plaatsgevonden en na ontvangst van een schriftelijke bevestiging van de Opdrachtgever, welke bevestiging binden is voor partijen.

6 EXITREGELING

	Exitplan
6.1	In het geval de overeenkomst, om welke reden dan ook, geheel of gedeeltelijk eindigt, is de Opdrachtnemer gehouden volledige medewerking te verlenen aan de retransitie (Exit). Deze medewerking omvat alle redelijke handelingen en voorzieningen die noodzakelijk zijn om de continuïteit van de betreffende diensten te waarborgen en een ordelijke, tijdige en volledige overdracht aan Opdrachtgever of een door de Opdrachtgever aangewezen derde te bewerkstelligen.
6.2	Voor het einde van het eerste contractjaar stelt de Opdrachtnemer een exit plan op en levert dit ter goedkeuring aan de Opdrachtgever aan. In het exit plan wordt op gestructureerde wijze vastgelegd welke maatregelen, activiteiten en verantwoordelijkheden gelden in het geval de overeenkomst eindigt, ongeacht de reden van beëindiging. De Opdrachtnemer is verplicht het exit plan jaarlijks, in overleg met de Opdrachtgever, te actualiseren en de geactualiseerde versie ter goedkeuring aan de Opdrachtgever voor te leggen.

6.3	Het exit plan heeft tot doel de continuïteit van de dienstverlening te waarborgen en schade of verstoringen voor de Opdrachtgever te voorkomen ten tijde van de retransitie (Exit). Het exit plan bevat ten minste het volgende: a. Medewerking en continuïteit: de wijze waarop de Opdrachtnemer de voortgang van de dienstverlening tijdens de exit fase waarborgt en medewerking verleent aan overdracht of beëindiging. b. Data en intellectueel eigendom: de procedures en verantwoordelijkheden ten aanzien van eigendom, overdracht, verwijdering en beveiliging van gegevens, documentatie en intellectuele eigendomsrechten c. Planning en fasering: een planning van de exit fase, termijnen d. Kennis en personeel: de maatregelen met betrekking tot overdracht van kennis, documentatie en eventuele continuïteit van personeel dat betrokken is bij de dienstverlening e. Juridische en financiële aspecten: de bepalingen inzake verplichtingen, verrekeningen, lopende overeenkomsten met derden, aansprakelijkheden en overige juridische verplichtingen die voortvloeien uit de beëindiging. f. Onderhoud: waarborgen voor de continuïteit van onderhoud, support en beheer tijdens en na de exit fase, totdat overdracht volledig is gerealiseerd. g. Rollen en verantwoordelijkheden: een duidelijke toelichting van verantwoordelijkheden en bevoegdheden tijdens de uitvoering van het exit plan, inclusief escalatie- en communicatie procedures. h. Beschrijving van de dienstverlening, contacten en stakeholders: een overzicht van de te beëindigen of over te dragen diensten, betrokken stakeholders, contactpersonen en relevante communicatielijnen. i. Compliance en audit: de wijze waarop gedurende de exit fase wordt voldaan aan toepasselijke wet- en regelgeving, beveiligingsnormen en eventuele toezichtvereisten van de Opdrachtgever of bevoegde instanties