Rijksinkoopsamenwerking
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Bijlage B3.4– Risico, Compliance en Informatiebeveiliging

Rijksinkoopsamenwerking

Bezoekadres
Rijkskantoor Beatrixpark
Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 20011
2500 EA Den Haag

Bijlage B3.4 - Risico, Compliance en Informatiebeveiliging

Uitvoering exportkredietverzekeringen en investeringsgaranties

Europese aanbesteding
Mededingingsprocedure met onderhandeling

voor

het ministerie van Financiën
en
het ministerie van Buitenlandse Zaken

Datum	
Kenmerk	201865004.016.017
Versie	Concept

Inhoud

1. Inleiding

1.1. Algemeen

In deze Bijlage B3.4 – Risico, Compliance en Informatiebeveiliging van de Overeenkomst worden de kaders beschreven voor het toepassen van Risico, Compliance en Informatiebeveiliging. Daarnaast bevat deze bijlage Eisen die voortvloeien uit deze kaders en waaraan Opdrachtnemer zich dient te conformeren.

1.2. Definities

De opgenomen definities, begrippen en afkortingen in de Overeenkomst, Voorwaarden en Bijlage B2 – Begrippenlijst zijn onverkort van toepassing op deze bijlage.

2. Leeswijzer

De inhoud van deze bijlage is opgesteld in het kader van de Hoofd- en Subdiensten die Opdrachtnemer zal leveren, welke zijn beschreven in Bijlage B3.1 – Dienstenbeschrijving.

hoofdstuk 3 van deze bijlage behandelt het risicomanagement met betrekking tot de levering van de Diensten. In dit hoofdstuk worden de Eisen uiteengezet die Opdrachtnemer stelt aan het beheersen van risico's.
In hoofdstuk 4 worden de compliance-eisen beschreven die nodig zijn om een rechtmatige beheersing van risico's te waarborgen. Hoofdstuk 5 bevat de Eisen en maatregelen op het gebied van informatiebeveiliging, die essentieel zijn ter ondersteuning van de levering van de Diensten. Hoofdstuk 6 behandelt de Eisen rondom belangenbescherming. Hoofdstuk 7 gaat in op de (mogelijke) toepassing van de *Algemeen Beveiligingseisen Rijksoverheidopdrachten (ABRO).*

In de onderstaande hoofdstukken zijn voor verschillende terreinen (risicomanagement, compliance, informatiebeveiliging en belangenbescherming) Eisen inzake het opstellen van plannen opgenomen. Ten behoeve van het leesgemak is hieronder een samenvatting opgenomen van deze vereiste plannen. De Eisen aan deze plannen worden in de verschillende hoofdstukken nader toegelicht.

Vereist plan	Inhoudsindicatie	Wanneer	Verwijzing
Businesscontinuïteitsplan (BCP)	Plan moet kenbaar maken op welke wijze Opdrachtnemer de continuïteit van Dienstverlening gedurende gehele Looptijd van de Overeenkomst borgt	Gedurende de Transitie voor 1 januari van elk jaar een update, tussentijdse update indien vereist	Hoofdstuk 3 (Risicomanagement)
Disaster-recoveryplan (DRP)	Plan bevat procedures voor het herstel van IT-systemen en data na calamiteiten	Gedurende de Transitie voor 1 januari van elk jaar een update, tussentijdse update indien vereist	Hoofdstuk 3 (Risicomanagement)
Auditplan	Dient inzage te geven in de procedures inzake (interne) audits en andere inspecties	Gedurende de Transitie voor 1 januari van elk jaar een update, tussentijdse update indien vereist	Hoofdstuk 4 (Compliance)
Informatiebeveiligingsplan	Dient inzage te geven in hoe Schade veroorzaakt door verstoring, uitval of misbruik voor de Diensten voorkomen wordt	Gedurende de Transitie voor 1 januari van elk jaar een update, tussentijdse update indien vereist	Hoofdstuk 5 (Informatiebeveiliging)
Belangenbeschermingsplan	Dient inzage te geven in de wijze waarop belangenverstrengeling wordt voorkomen	Bij aanvang van Contracttermijn, voor 1 januari van elk jaar een update, tussentijdse update indien vereist	Hoofdstuk 6 (Belangen-beschermingsplan)

3. Risicomanagement

Risicomanagement is een essentieel onderdeel van de activiteiten van Opdrachtgever. Opdrachtgever beheert voorzieningen die cruciaal zijn voor het functioneren van de Nederlandse overheid. Opdrachtnemer en diens eventuele Onderaannemers zijn onderdeel van het risicomanagement van Opdrachtgever en dienen hier een actieve bijdrage aan te leveren. De focus ligt op een systematische en voor Opdrachtgever acceptabele wijze van risicobeheersing, waarbij rekening wordt gehouden met specifieke dreigingen tegen de overheid of specifiek het ministerie van Financiën en Buitenlandse Zaken. Dit houdt in dat Opdrachtnemer in samenspraak met Opdrachtgever risico's moet identificeren, evalueren en prioriteren, en vervolgens maatregelen moet implementeren om deze te verminderen. Opdrachtnemer dient hiertoe op het gebied van risicomanagement een hoge mate van transparantie en een intensieve samenwerking met Opdrachtgever te waarborgen.

3.1. Eisen aan risicomanagement

Onderstaande Eisen hebben betrekking op risicomanagement.

ID	Onderwerp	Beschrijving
3.4.1	Risicomanagement	Het risicomanagement van Opdrachtnemer sluit aantoonbaar aan bij de principes van de ISO27001. (Uitvoeringsvoorwaarde)
3.4.2	Risicomanagement-beleid	• Opdrachtnemer onderhoudt een formeel beleid voor risicomanagement. Dit beleid omvat de geïdentificeerde risico's die acceptabel zijn en geïdentificeerde risico's die dat niet zijn (risicotolerantie). Dit beleid voldoet aan de standaarden en Eisen genoemd in deze bijlage en dient te worden voorgelegd aan Opdrachtgever als er van de gestelde beveiligingseisen wordt afgeweken. • De verantwoordelijkheden en processen voor risicomanagement zijn duidelijk vastgelegd in dit beleid. • Opdrachtnemer dient dit beleid actief uit te dragen en te implementeren binnen diens organisatie en diens eventuele Onderaannemers. • Het beleid wordt door Opdrachtnemer up-to-date gehouden en waar nodig aangepast indien dit benodigd is, bijvoorbeeld vanwege veranderende wet- en regelgeving. Bij materiële wijzigingen wordt het beleid opnieuw voorgelegd aan Opdrachtgever. (Uitvoeringsvoorwaarde)
3.4.3	Risicoanalyse	Opdrachtnemer voert ten minste jaarlijks, en tussentijds bij belangrijke wijzigingen in de Diensten of de inrichting ervan, een uitgebreide risicoanalyse uit. Deze analyse wordt uitgevoerd conform NEN-EN-ISO/IEC 27005:2024 of een gelijkwaardige, erkende en marktconforme methode. De meest actuele (vigerende) versie van de norm geldt hierbij als uitgangspunt. Opdrachtnemer zorgt voor de implementatie van maatregelen om de geïdentificeerde risico’s te mitigeren. (Uitvoeringsvoorwaarde)
3.4.4	Afstemming risicoanalyse	Opdrachtnemer deelt de resultaten van de risicoanalyses met Opdrachtgever, en neemt deel aan gezamenlijke risicoanalysesessies. Binnen deze sessies en in de eigen analyses integreert Opdrachtnemer informatie verstrekt door Opdrachtgever. (Uitvoeringsvoorwaarde)
3.4.5	Risicoregister	Opdrachtnemer dient een risicoregister in te richten zodanig dat dit een compleet beeld geeft van de geldende, actuele risico’s voor zowel Opdrachtnemer als Opdrachtgever. Op aanvraag vanuit Opdrachtgever kan dit register ook worden gedeeld met Opdrachtgever. Daarnaast stemt Opdrachtnemer zowel de classificering van de risico's in het risicoregister als de beheersing van deze risico's af met Opdrachtgever tijdens

		operationele, tactische en strategische overleggen. Hiertoe dient ten minste per risico de volgende informatie te worden geregistreerd en geactualiseerd: • de onzekere gebeurtenis, oorzaken en gevolgen; • de naam van de eigenaar van het risico; • de periode waarin het risico kan optreden; • de kans van optreden en de impact; • de consequenties; • de beheersmaatregelen. (Uitvoeringsvoorwaarde)
3.4.6	Delen van informatie over risico's, risicoanalyses en maatregelen	Zowel gevraagd als ongevraagd stelt Opdrachtnemer informatie beschikbaar over maatregelen, kwetsbaarheden, Incidenten en het ontwerp en de inrichting van de Diensten. Hiermee ondersteunen ze de risico-inschattingen van Opdrachtgever. (Uitvoeringsvoorwaarde)

3.2. Eisen aan Businesscontinuïteit en Disaster Recovery

Opdrachtgever vindt het van belang dat Opdrachtnemer de continuïteit van de Dienstverlening borgt. Daartoe dient Opdrachtnemer maatregelen te treffen op het gebied van Businesscontinuïteit en Disaster Recovery. Onderstaande Eisen zien daarop.

ID	Onderwerp	Beschrijving
3.4.7	Onverwijld mededelen	Opdrachtnemer dient Opdrachtgever onverwijld op de hoogte te stellen van een gebeurtenis of Incident die/dat impact kan hebben op de continuïteit van de Dienstverlening, inclusief de verwachte consequenties voor de Dienstverlening, Opdrachtnemer en Opdrachtgever en de reeds getroffen en te treffen maatregelen om de gevolgen te beperken. (Uitvoeringsvoorwaarde)
3.4.8	Businesscontinuïteit	Opdrachtnemer dient gedurende de gehele duur van de Overeenkomst te beschikken over een actueel, schriftelijk vastgelegd en getoetst Businesscontinuïteitsplan (BCP). • Het BCP dient gebaseerd te zijn op een recente Businessimpactanalyse (BIA) en risicoanalyse, waarin kritieke processen, systemen en de mogelijke impact van uitval expliciet zijn beschreven. • In het BCP is de wijze opgenomen waarop Opdrachtnemer de continuïteit van de Diensten gedurende de gehele Contracttermijn zal waarborgen, inclusief een beschrijving van ten minste de betreffende back-up/restore- en uitwijk/fallback-processen en -procedures. • In het BCP is een communicatieprotocol opgenomen voor tijdige en effectieve communicatie met alle relevante interne en externe stakeholders bij verstoringen. • Het BCP wordt minimaal eenmaal per jaar getest middels een volledige of gedeeltelijke oefening. Resultaten en eventuele verbetermaatregelen worden schriftelijk vastgelegd en aan Opdrachtgever ter beschikking gesteld. • Opdrachtnemer documenteert de rollen en verantwoordelijkheden met betrekking tot businesscontinuïteit binnen de organisatie. • Opdrachtnemer sluit schriftelijke afspraken met kritieke leveranciers en partners, waarin de beschikbaarheid en continuïteit van geleverde Diensten zijn gegarandeerd. (Uitvoeringsvoorwaarde)
3.4.9	Disaster Recovery	Opdrachtnemer dient te beschikken over een gedocumenteerd Disaster-recoveryplan (DRP) dat procedures bevat voor het herstel van IT-systemen en data na calamiteiten.

		• Het DRP specificeert meetbare Recovery Time Objectives (RTO) en Recovery Point Objectives (RPO) per systeem en proces, afgestemd op de kritikaliteit daarvan. • Opdrachtnemer zorgt voor regelmatige, beveiligde back-ups van data, die opgeslagen worden op minimaal één geografisch gescheiden locatie. • Opdrachtnemer beschikt over een alternatieve herstelomgeving die inzetbaar is om de continuïteit van de Dienstverlening te waarborgen. • Het DRP wordt minimaal jaarlijks getest. De resultaten van deze tests worden schriftelijk binnen twintig (20) kalenderdagen na het uitvoeren van de test gedeeld met Opdrachtgever, inclusief verbetermaatregelen. Incidentresponsprocedures met duidelijke escalatielijnen zijn opgenomen, inclusief verplichtingen tot directe melding aan Opdrachtgever bij Incidenten die de continuïteit kunnen beïnvloeden. (Uitvoeringsvoorwaarde)
3.4.10	Business continuity en Disaster-recovery plan actualiseren	Opdrachtnemer actualiseert het Continuïteits- en Disaster-recoveryplan ten minste: • op jaarlijkse basis; • na Wijzigingen aan de Diensten of testuitkomsten waaruit blijkt dat aanpassingen en/of aanvullende maatregelen noodzakelijk zijn. Opdrachtnemer dient het geactualiseerde Continuïteits- en Disaster-recoveryplan binnen dertig (30) Werkdagen na bovenstaande gebeurtenissen op te leveren aan Opdrachtgever ter vaststelling. Indien de actualisatie van het Continuïteits- en Disaster-recoveryplan leidt tot aanvullende maatregelen, dient Opdrachtnemer deze maatregelen te implementeren na succesvolle testactiviteiten. Opdrachtnemer dient de effectieve werking van deze maatregelen te monitoren, ze binnen de met Opdrachtgever overeengekomen doorlooptijd te realiseren, en periodiek te rapporteren over de voortgang. (Uitvoeringsvoorwaarde)
3.4.11	Tijdig informeren over wijzigingen	Opdrachtnemer verplicht zich tot het tijdig informeren van Opdrachtgever over wijzigingen in het BCP en DRP die impact kunnen hebben op de continuïteit. (Uitvoeringsvoorwaarde)
3.4.12	O-maatregel. Informatie-beveiligings-continuïteit verifiëren, beoordelen en evalueren	De Dienstverlening van de bedrijfskritische onderdelen wordt bij calamiteiten van Opdrachtnemer uiterlijk binnen een week hersteld (conform 17.1.3.3; BIO 2019). (Uitvoeringsvoorwaarde)
3.4.13	Coördinatie herstelprocessen	Opdrachtnemer dient de herstelprocessen en -procedures te coördineren en te communiceren met Opdrachtgever en Derde(n). (Uitvoeringsvoorwaarde)
3.4.14	Verbeteren herstelprocessen	Opdrachtnemer dient de herstelprocessen en -procedures te verbeteren op basis van ervaring met huidige en voorgaande cybersecurityactiviteiten. (Uitvoeringsvoorwaarde)
3.4.15	Beheer van Technische Kwetsbaarheden	Opdrachtnemer heeft zijn bedrijfsvoering zodanig ingericht dat technische kwetsbaarheden adequaat worden ontdekt, geëvalueerd en geadresseerd. Opdrachtnemer informeert Opdrachtgever onmiddellijk wanneer er een kwetsbaarheid wordt geconstateerd of verwacht, betreffende de Gegevens en/of de Diensten waar Opdrachtgever gebruik van maakt. Opdrachtnemer zal in dat geval tevens de omvang van de kwetsbaarheid aangeven, de verwachte consequenties voor Opdrachtgever alsmede de reeds getroffen en te treffen maatregelen om de gevolgen te beperken. (Uitvoeringsvoorwaarde)

4. Compliance

Opdrachtgever moet voldoen aan de geldende wet- en regelgeving op het gebied van informatiebeveiliging, privacybescherming en openbaar bestuur.

4.1. Context van Opdrachtgever

Opdrachtgever vindt naleving van wetten, voorschriften, overheidsbeleid en de specifieke Eisen voor elke Dienst of applicatie belangrijk. Naleving hiervan strekt zich ook uit tot de Diensten geleverd door Opdrachtnemer en diens Onderaannemers, wat betekent dat het essentieel is dat Opdrachtnemer hieraan bijdraagt door maximaal bewijsbaar in control te zijn en compliant te zijn. Wanneer veranderingen optreden in de genoemde wet- en regelgeving of beleidsdocumenten, dienen Opdrachtnemer en diens Onderaannemers de Diensten, in afstemming met Opdrachtgever, daarop aan te passen.

4.2. Eisen aan compliance

Onderstaande Eisen hebben betrekking op compliance.

ID	Onderwerp	Beschrijving
3.4.16	Wet- en regelgeving	Opdrachtnemer zal de Diensten leveren conform van toepassing zijnde wet- en regelgeving en diens toekomstige aanpassingen op zodanige wijze, dat Opdrachtgever te allen tijde blijvend in overeenstemming is met wet- en regelgeving, waaronder maar niet uitsluitend: • de Algemene verordening gegevensbescherming AVG (2018); • de Uitvoeringswet Algemene verordening gegevensbescherming (uAVG); • de Digital Operational Resilience Act (DORA); • de NIS2-richtlijnen (Network and Information Security Directive); • de WOO (Wet Open Overheid). (Minimumeis)
3.4.17	Beleid van Opdrachtgever	Opdrachtnemer zal de Diensten leveren conform het beleid van Opdrachtgever waaronder onderstaand overzicht (niet-limitatieve lijst): • Informatiebeveiligingsbeleid • Privacybeleid Opdrachtgever is gerechtigd om in Nader offerte-uitvragen aanvullend beleid op te leggen voor de uitvoering van de Diensten. (Uitvoeringsvoorwaarde)
3.4.18	Waarborging compliance wet- en regelgeving en beleid	Opdrachtnemer erkent dat wet- en regelgeving en beleid gewijzigd kunnen worden en dat Opdrachtnemer gebonden is aan de gewijzigde wet- en regelgeving en beleid (tenzij Opdrachtnemer schriftelijk gemotiveerd heeft aangegeven dat hij dit gewijzigde beleid niet kan opvolgen, en in dat geval zullen Partijen zich tot het uiterste inspannen om maatregelen te treffen om zich zo veel mogelijk te conformeren aan dit gewijzigde beleid). Opdrachtnemer wijzigt processen en/of procedures binnen redelijke termijn, indien dit noodzakelijk is voor de opvolging van gewijzigde wet- en regelgeving en beleid. Het is de verantwoordelijkheid van Opdrachtnemer om eventuele wijzigingen in wet- en regelgeving tijdig te signaleren en hieraan opvolging te geven. Opdrachtnemer en Opdrachtgever dienen elkaar proactief op de hoogte te houden van eventuele wijzigingen in overheidsbeleid die van invloed kunnen zijn op de uitvoering van de Overeenkomst. (Uitvoeringsvoorwaarde)
3.4.19	Identiteitsbewijs en verblijfs- en werkvergunning	Opdrachtnemer zorgt ervoor dat zijn medewerkers en eventuele Onderaannemers, die betrokken zijn bij de uitvoering van de Diensten, beschikken over ofwel: • een geldig identiteitsbewijs (paspoort, ID-kaart of rijbewijs);

		• indien van toepassing een geldige verblijfs- en werkvergunning die bij tewerkstelling bij Opdrachtgever nog een half jaar geldig is. Medewerkers die hier niet over beschikken, wordt geen toegang verleend tot locaties van Opdrachtgever. Opdrachtgever behoudt zich het recht voor om, deugdelijk gemotiveerd, werknemers van Opdrachtnemer de toegang tot de locatie te ontzeggen. Eventuele kosten die hiermee samenhangen en/of hieruit voortvloeien zijn voor rekening van Opdrachtnemer. (Uitvoeringsvoorwaarde)
3.4.20	Onderaannemer(s)	Opdrachtnemer draagt de verantwoordelijkheid voor het voldoen aan de gestelde Eisen uit dit document bij de bedrijven die hij als Onderaannemer(s) onder zijn hoede neemt gedurende de duur van de Overeenkomst. (Uitvoeringsvoorwaarde)

4.3. Eisen aan audits en certificering

Onderstaande Eisen hebben betrekking op audits en certificering, en zijn aanvullend op de Eisen die zijn opgenomen in Bijlage B – Overeenkomst, artikel 11.

ID	Onderwerp	Beschrijving
3.4.21	Certificering	Opdrachtnemer, of Onderaannemer indien deze integraal verantwoordelijk is voor het (laten) uitvoeren van de gevraagde Dienstverlening, dient: • Over een ISO 9001 of gelijkwaardige certificering te beschikken die minimaal vanaf en gedurende de Transitieperiode de gevraagde Dienstverlening afdekt. De kosten voor de (jaarlijkse) certificering en Assuranceverklaring zijn voor rekening van Opdrachtnemer, alsmede de kosten om bevindingen en afwijkingen volgend uit deze audits op te lossen. (Uitvoeringsvoorwaarde)
3.4.22	ISAE 3000 type 1 / ISAE 3402 type 1	Opdrachtnemer komt laatstelijk gedurende de Transitieperiode in het bezit van een ISAE 3000 type 1- of ISAE 3402 type 1-verklaring (of een vergelijkbare SOC1 gericht op beheersmaatregelen die over een periode worden bekeken) en het jaar daarna in het bezit van een ISAE 3000 type 2 of ISAE 3402 type 2. Daarna behaalt Opdrachtnemer jaarlijks de ISAE 3000 type 2- of ISAE 3402 type 2- verklaring gedurende de Looptijd van de Overeenkomst. Uitvoeringsvoorwaarde)
3.4.23	Auditplan	Opdrachtnemer dient gedurende de Transitieperiode de vigerende versie van het (interne-)auditplan (zoals bedoeld in paragraaf 9.2 van de NEN-EN-ISO 9001:2018) te leveren aan Opdrachtgever. Het auditplan dient ten minste weer te geven: • de beschrijving, mijlpalen en doorlooptijd van de audits, inspecties, certificeringen of beoordelingen die lopen en gepland zijn voor het komende kalenderjaar; • de processen, de onderwerpen en de functionarissen waarop de audit, inspectie, certificering of beoordeling betrekking hebben; • per audit, inspectie, certificering of beoordeling de risico's die hieraan ten grondslag liggen; • per audit, inspectie, certificering of beoordeling de organisatieonderdelen van Opdrachtnemer en/of van de Onderaannemers van Opdrachtnemer waar deze wordt uitgevoerd; • per audit, inspectie, certificering of beoordeling de functionarissen en/of de externe organisatie die deze uitvoeren/uitvoert. (Uitvoeringsvoorwaarde)
3.4.24	Auditplan actualiseren	Opdrachtnemer actualiseert het Auditplan tenminste: • op jaarlijkse basis; • na Wijzigingen aan de Diensten, testuitkomsten of ontwikkelingen waaruit blijkt dat aanpassingen en/of aanvullende maatregelen noodzakelijk zijn. Opdrachtnemer dient het geactualiseerde plan binnen twintig (20)

		Werkdagen na bovenstaande gebeurtenissen op te leveren aan Opdrachtgever ter vaststelling. Indien de actualisatie van het plan leidt tot aanvullende maatregelen, dient Opdrachtnemer deze maatregelen te implementeren na succesvolle testactiviteiten. Opdrachtnemer dient de effectieve werking van deze maatregelen te monitoren, ze binnen de met Opdrachtgever overeengekomen doorlooptijd te realiseren, en periodiek te rapporteren over de voortgang. (Uitvoeringsvoorwaarde)
3.4.25	Tijdig oplossen van audit- bevindingen	Opdrachtnemer dient na de vaststelling van bevindingen uit audits, inspecties, certificatie of beoordelingen deze op te lossen binnen de hersteltermijnen als bedoeld in artikel 11 van de Overeenkomst. Onder bevindingen wordt bedoeld mogelijke afwijkingen of tekortkomingen van Opdrachtnemer in de processen en systemen die onderdeel zijn van de Diensten. De kosten om respectievelijk deze bevindingen en aandachtspunten op te lossen zijn voor rekening van Opdrachtnemer. (Uitvoeringsvoorwaarde)

5. Informatiebeveiliging en privacybescherming

Informatieveiligheid en privacy worden gewaarborgd door het toepassen van informatiebeveiliging en privacybescherming. Informatiebeveiliging en privacybescherming omvatten het geheel aan maatregelen gericht op een kosteneffectieve beheersing van de risico's met betrekking tot de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens en data. Deze maatregelen komen voort uit wet- en regelgeving, besluiten en standaarden. Daarbij gaat het voornamelijk om de onderstaande wet- en regelgeving en toekomstige aanpassingen c.q. wijzigingen ervan:

- NIS2 (Cyberbeveiligingswet)
- AVG (GDPR)
- VIRBI
- BIO en/of ISO27001
- ABRO

5.1. Eisen aan informatiebeveiliging

Voor het ministerie van Financiën en Buitenlandse Zaken is het waarborgen van (nationale) veiligheid, de continuïteit van de overheidsdienstverlening en het vertrouwen van de burger cruciaal. De Baseline Informatiebeveiliging Overheid (BIO) of ISO27001 vormt hierbij het fundament. Onderstaande Eisen hebben betrekking op de inrichting van informatiebeveiliging en privacybescherming.

ID	Onderwerp	Beschrijving
3.4.26	BIO	De organisatie van Opdrachtnemer en zijn Dienstverlening dienen in opzet, bestaan en werking te voldoen aan de Baseline Informatiebeveiliging Overheid (BIO, versie 1.04 en opvolgende versies) en toont dat jaarlijks aan middels onafhankelijke onderzoeken. Het van toepassing zijnde Basis Beveiligingsniveau (BBN) is vastgesteld op niveau 2; de bijbehorende Eisen zijn opgenomen in dit document (conform Ketenpartnereis 1). (Uitvoeringsvoorwaarde)
3.4.27	BIO (voldoen per XX)	Opdrachtnemer voldoet gedurende de Transitieperiode aan de BIO of ISO 27001. Opdrachtnemer kan dit aantonen door een verklaring op te leveren met ISO27001 of aanvullende BIO-controles, met daarbij de maatregelen die Opdrachtnemer heeft genomen. Dit document kan worden aangeleverd door een gecertificeerde (interne-)auditafdeling of door een geaccrediteerde organisatie uitgegeven ISO 27001-certificaat, compleet met bijbehorend Statement of Applicability. Uit de interne verklaring of het certificaat blijken opzet, bestaan en werking van een geïmplementeerd informatiebeveiligingsbeleid. Opdrachtgever krijgt het recht om, zowel tijdens de aanbestedingsprocedure als tijdens de Contracttermijn, steekproefsgewijs controles/maatregelen te selecteren en hier bewijs voor te vragen. Opdrachtnemer werkt zoveel mogelijk mee aan de beantwoording van deze verzoeken. (Minimumeis)
3.4.28	Additioneel informatie-beveiligingsbeleid van Opdrachtgever	Opdrachtgever hanteert verschillende methoden om naleving van het informatiebeveiligingsbeleid te controleren. Dit wordt gedaan door middel van audits, risicobeoordelingen en nalevingsrapportages zoals beschreven in Bijlage B3.3 – Governance en stuurmechanismen. (Uitvoeringsvoorwaarde)
3.4.29	Informatie-beveiligingsplan	Opdrachtnemer dient gedurende de Transitie een Informatiebeveiligingsplan op te stellen en af te stemmen met Opdrachtgever waarin Opdrachtnemer beschrijft hoe gevaren of Schade veroorzaakt door verstoring, uitval of misbruik voor de Diensten voorkomen zal worden. En, hoe dit voldoet aan de minimaal gestelde

		beveiligingsniveaus van de Diensten. (Minimumeis)
3.4.30	Informatie-beveiligingsplan actualiseren	Opdrachtnemer actualiseert het informatiebeveiligingsplan ten minste • op jaarlijkse basis; • na Wijzigingen aan de Diensten, testuitkomsten of ontwikkelingen waaruit blijkt dat aanpassingen en/of aanvullende maatregelen noodzakelijk zijn. Opdrachtnemer dient het geactualiseerde informatiebeveiligingsplan binnen twintig (20) Werkdagen na bovenstaande gebeurtenissen op te leveren aan Opdrachtgever ter vaststelling. Indien de actualisatie van het informatiebeveiligingsplan leidt tot aanvullende maatregelen, dient Opdrachtnemer deze maatregelen te implementeren na succesvolle testactiviteiten. Opdrachtnemer dient de effectieve werking van deze maatregelen te monitoren, ze binnen de met Opdrachtgever overeengekomen doorlooptijd te realiseren, en periodiek te rapporteren over de voortgang. (Uitvoeringsvoorwaarde)
3.4.31	Informatiebeveiliging testen	• Opdrachtnemer toetst bij het uitvoeren van beveiligingstesten op basis van de meest actuele versie van de OWASP-top 10 (https://owasp.org/www-project-top-ten/). • Opdrachtnemer toetst bij het uitvoeren van beveiligingstesten op de SANS/CWE top 25 (SANS.org). (Uitvoeringsvoorwaarde)
3.4.32	Controle	Opdrachtnemer dient ten minste jaarlijks de getroffen maatregelen voor de informatiebeveiliging te laten controleren door een externe auditor. Opdrachtnemer dient aan te kunnen tonen dat diens beveiligingsmaatregelen en -organisatie continu en effectief werken. Hiertoe dient Opdrachtnemer opzet, bestaan en werking van controles en processen voor Opdrachtgever bewijsbaar aan te tonen, zo ook voor werkzaamheden die uitbesteed zijn aan Derde(n). (Uitvoeringsvoorwaarde)
3.4.33	Opslag	Gegevens gerelateerd aan een Te beschermen belang dienen veilig te worden opgeslagen in databases of bestanden, waarbij zeer gevoelige gegevens worden versleuteld. Opslag vindt alleen plaats indien noodzakelijk. (Minimumeis)
3.4.34	Toekomstbestendige cryptografie	De aangeboden Dienst of oplossing moet crypto-agile zijn. Cryptografische algoritmes (voor versleuteling, digitale handtekeningen etc.) kunnen eenvoudig en zonder ingrijpende wijzigingen worden vervangen. Daarnaast stelt Opdrachtnemer een gedetailleerde PQC-Roadmap op en deelt deze met Opdrachtgever; hierbij is het advies het 'PQC-migratie handboek' aan te houden. (Uitvoeringsvoorwaarde)
3.4.35	Cyberincidenten	Opdrachtnemer dient processen in te richten om Beveiligingsincidenten te voorkomen, te detecteren en binnen 24 uur af te handelen (Incidentmanagement en Incidentresponsplan). Indien een cyberincident volgens NIS2 als significant ingeschaald is, moet dit binnen 12 uur gemeld worden aan Opdrachtgever (CISO) (conform 16.1.2.4; BIO 2019). (Uitvoeringsvoorwaarde)
3.4.36	Datalekken	Opdrachtnemer heeft de kennis georganiseerd om de oorzaak van een datalek te kunnen vaststellen en te onderzoeken, heeft daarvoor de benodigde loggegevens om herhaling te voorkomen en heeft de stakeholders vastgesteld om ze te kunnen informeren. Opdrachtnemer dient ervoor te zorgen dat datalekken en andere verdachte gebeurtenissen binnen 24 uur worden gedetecteerd, gemeld bij Opdrachtgever en worden behandeld (conform ALG P.07; Privacy-supplement Algemeen). (Uitvoeringsvoorwaarde)
3.4.37	Beveiligings-incidenten-medewerking	Opdrachtnemer dient in voorkomende gevallen zijn medewerking te verlenen voor het verzamelen, bewaren en beschikbaar stellen van bewijsmateriaal betreffende beveiligingsgerelateerde maatregelen en

		incidenten. (Uitvoeringsvoorwaarde)
3.4.38	Beheer van informatie-beveiligings-incidenten	Op de inrichting van het beheer van informatiebeveiligingsincidenten is hoofdstuk 16 van de BIO 2019 van toepassing (conform Ketenpartnereis 5). (Uitvoeringsvoorwaarde)
3.4.39	Rapportage	Opdrachtnemer dient continue en effectief aan te kunnen tonen dat zijn beveiligingsmaatregelen en -organisatie werken. Dit behelst rapportage(s) over de werking van controles en processen, zo ook voor werkzaamheden uitbesteed aan Derde(n). Hiervoor behoeft Opdrachtgever rapportages van Opdrachtnemer ten aanzien van informatiebeveiliging. (Uitvoeringsvoorwaarde)
3.4.40	Logging Gebruikers-toegang	Opdrachtnemer dient logging en monitoring in te richten op (administratieve) Gebruikerstoegang. (Minimumeis)
3.4.41	Monitoren cybersecurity-gebeurtenissen	Opdrachtnemer dient alle informatiesystemen die hij gebruikt voor de Diensten te monitoren om cybersecuritygebeurtenissen (tijdig) te kunnen identificeren en passende maatregelen te nemen. (Uitvoeringsvoorwaarde)
3.4.42	Detectieprocessen cybersecurity-gebeurtenis-sen	Opdrachtnemer dient detectieprocessen en -procedures in te richten, te onderhouden en te testen om cybersecuritygebeurtenissen en -Incidenten inzichtelijk te kunnen maken. (Uitvoeringsvoorwaarde)
3.4.43	Cyberrespons-activiteiten	Opdrachtnemer dient cyberresponsactiviteiten op te zetten, uit te voeren (oefenen/testen), te onderhouden en te evalueren om tijdige reacties op een Beveiligingsincident te kunnen waarborgen, alsmede ten minste relevante (kennis)Documentatie betreffende deze activiteiten op te nemen in zijn Documentatie. (Uitvoeringsvoorwaarde)
3.4.44	Uitwerken Cyberrespons-activiteiten	Opdrachtnemer dient de cyberresponsactiviteiten te coördineren en te communiceren met Opdrachtgever en belanghebbende(n), alsmede ten minste relevante (kennis)Documentatie en leerpunten betreffende uitgevoerde cyberresponsactiviteiten op te nemen in zijn Documentatie. (Uitvoeringsvoorwaarde)
3.4.45	Analyse cybersecurity-gebeurtenissen	Opdrachtnemer dient analyses op de cybersecuritygebeurtenissen en -Incidenten uit te voeren en de uitkomsten hiervan te documenteren om de cyberresponsactiviteiten te ondersteunen. (Uitvoeringsvoorwaarde)
3.4.46	Samenwerking bij cybersecurity-gebeurtenissen	Opdrachtnemer dient de afhandeling van cybersecuritygebeurtenissen in samenwerking te laten plaatsvinden met Opdrachtgever en betreffende belanghebbende(n). (Uitvoeringsvoorwaarde)
3.4.47	Ondersteuning bij cybersecurity-gebeurtenissen	Opdrachtnemer dient bij cybersecuritygebeurtenissen ondersteuning te bieden aan diegene die verantwoordelijk is voor de (deel)oplossing. (Uitvoeringsvoorwaarde)
3.4.48	Evaluatie bij cybersecurity-gebeurtenissen	Opdrachtnemer dient cyberresponsactiviteiten te evalueren en te verbeteren op basis van leerpunten van opgeloste cybersecuritygebeurtenissen. (Uitvoeringsvoorwaarde)
3.4.49	PDCA-cyclus	Informatiebeveiliging en privacy zijn dynamische onderwerpen, en de maatregelen dienen vanwege toenemende risico's en bedreigingen via een PDCA-cyclus actueel te worden gehouden (conform Ketenpartnereis 2). (Uitvoeringsvoorwaarde)

6. Belangenbescherming

Opdrachtgever is gehouden te voldoen aan de geldende wet- en regelgeving omtrent belangenbescherming, integriteit en onafhankelijke besluitvorming binnen het kader van publieke Dienstverlening. Ter waarborging hiervan dient Opdrachtnemer te voldoen aan onderstaande Eisen.

6.1. Eisen aan belangenbescherming

ID	Onderwerp	Beschrijving
3.4.50	Conflicterende belangen	Opdrachtnemer heeft geen conflicterende belangen die een negatieve invloed kunnen hebben op de uitvoering van de opdracht. (Minimumeis)
3.4.51	Concernstructuur buiten de EU	Indien Opdrachtnemer deel uitmaakt van een concernstructuur waarbij het moederbedrijf is gevestigd buiten de Europese Unie, dient Opdrachtnemer de functionele en organisatorische onafhankelijkheid van de Dienstverlening aan Opdrachtgever aantoonbaar gewaarborgd te hebben. (Minimumeis)
3.4.52	Uitsluiting van buitenlandse staatsinvloed	Indien er sprake is van directe of indirecte beïnvloeding van besluitvorming of bedrijfsvoering door een buitenlandse overheid of staatsentiteit met eigendomsbelang, financiering of bestuurlijke zeggenschap in Opdrachtnemer, dient Opdrachtnemer de functionele en organisatorische onafhankelijkheid van de Dienstverlening aan Opdrachtgever aantoonbaar gewaarborgd te hebben. (Minimumeis)
3.4.53	Nevenfuncties en belangen van sleutelrollen	Leden van het bestuur, management of andere sleutelrollen binnen de organisatie van Opdrachtnemer hebben geen nevenfuncties of andere belangen die van toepassing kunnen zijn voor de uitvoering van deze opdracht. (Minimumeis)
3.4.54	Procedures voor het signaleren en beheersen van belangenconflicten	Opdrachtnemer beschikt over vastgestelde procedures en/of gedragscodes voor het tijdig signaleren en effectief beheersen van (mogelijke) belangenconflicten binnen de organisatie die een negatieve invloed kunnen hebben op de uitvoering van de Opdracht. (Uitvoeringsvoorwaarde)
3.4.55	Signalen van of onderzoeken naar belangenconflicten	Opdrachtnemer meldt onverwijld aan Opdrachtgever indien Opdrachtnemer en/of zijn Personeel betrokken raakt bij, dan wel onderwerp is van, onderzoeken inzake (mogelijke) belangenconflicten. (Uitvoeringsvoorwaarde)
3.4.56	Structurele maatregelen ter voorkoming van belangenconflicten	Opdrachtnemer past bij uitvoering van de Opdracht structurele maatregelen toe, zoals Chinese walls, functiescheiding of andere compliance-structuren, om te voorkomen dat andere belangen een (mogelijk) negatieve invloed hebben op de belangen van Opdrachtgever. (Uitvoeringsvoorwaarde)
3.4.57	Functionele en organisatorische scheiding van Personeel	Opdrachtnemer dient te borgen dat Personeel dat betrokken is bij uitvoering van de Opdracht, functioneel en organisatorisch gescheiden is van Personeel en processen die verband houden met andere Diensten die Opdrachtnemer, of een aan Opdrachtnemer gelieerde entiteit, verleent aan derden. Indien Opdrachtnemer bovenstaande niet heeft geborgd, dient Opdrachtnemer aan te tonen dat het Personeel dat betrokken is bij uitvoering van de Opdracht, geen belangen heeft bij de uitoefening van zijn werkzaamheden die een negatieve invloed kunnen hebben op de uitvoering van de Opdracht. (Uitvoeringsvoorwaarde)
3.4.58	Belangenbe-schermingsplan actualiseren	Opdrachtnemer actualiseert het Belangenbeschermingsplan voor de uitvoering van de Opdracht. Opdrachtnemer actualiseert het belangenbeschermingsplan ten minste: • op jaarlijkse basis; • na Wijzigingen aan de Diensten, testuitkomsten of ontwikkelingen waaruit blijkt dat aanpassingen en/of aanvullende maatregelen

		noodzakelijk zijn. Opdrachtnemer dient het geactualiseerde plan binnen twintig (20) Werkdagen na bovenstaande gebeurtenissen op te leveren aan Opdrachtgever ter vaststelling. Indien de actualisatie van het plan leidt tot aanvullende maatregelen, dient Opdrachtnemer deze maatregelen te implementeren na succesvolle testactiviteiten. Opdrachtnemer dient de effectieve werking van deze maatregelen te monitoren, ze binnen de met Opdrachtgever overeengekomen doorlooptijd te realiseren, en periodiek te rapporteren over de voortgang. (Uitvoeringsvoorwaarde)

7. ABRO

Opdrachtnemer dient naar verwachting per eind 2025 en mogelijk bij de uitvoering van de Opdracht te voldoen aan het vigerende normenkader zoals beschreven in het ABRO (Algemeen Beveiligingseisen Rijksoverheid)[1]. Dit normenkader bevat in ieder geval uitgangspunten en beveiligingseisen ten aanzien van risicobeheersing, compliance en informatiebeveiliging binnen overheidssamenwerkingen. Het ABRO dient als leidraad voor de borging van integriteit en beveiligingsstandaarden in publieke ketens. Deze ABRO is nog niet in werking getreden en ten tijde van deze marktconsultatie is daar dus nog niet op vooruitgelopen.

[1] *ABRO | PIANOo - Expertisecentrum Aanbesteden*[1]