Ministerie van Economische Zaken
en Klimaat

Bijlage 06
Risk, Compliance en Informatieveiligheid

IWR2026| SMS-Gateway

ICT Werkomgeving Rijk

Status:	definitief 1.0
Referentie	IUC 202510087

Inhoud

1. Inleiding 2
   1.1 Algemeen 2
   1.2 Relatie tot de aanbesteding 2
2. Riskmanagement 3
   2.1 Context van Deelnemers 3
   2.2 Eisen aan riskmanagement 3
   2.3 Eisen aan Business Continuïteit en Disaster Recovery 4
3. Compliance 5
   3.1 Context van Deelnemers 5
   3.2 Eisen aan compliance 5
4. Informatiebeveiliging en privacybescherming 7
   4.1 Eisen aan informatiebeveiliging en privacybescherming 7
5. Aanvullende maatregelen o.b.v. Quickscan nationale veiligheid 9

1. Inleiding

1.1 Algemeen

In deze Bijlage 06 Risk, compliance en informatieveiligheid van de aanbesteding SMS-Gateway worden de kaders beschreven voor het toepassen van risk, compliance en informatieveiligheid in de uitvoering van de Prestatie. Daarnaast bevat deze Bijlage eisen die voortvloeien uit deze kaders en waaraan Opdrachtnemer zich dient te conformeren.

1.2 Relatie tot de aanbesteding

Deze Bijlage is een integraal onderdeel van de aanbesteding IWR2026| SMS-Gateway. De eisen in deze Bijlage zijn van toepassing op de Prestatie (Bijlage 02 Specificatie van de Prestatie) zoals die geleverd wordt aan de Deelnemers. Elke Deelnemer dient verantwoording af te leggen over de aan te besteden Dienst. Deze verantwoording vindt plaats aan de hand van de beheersingsprocessen in deze Bijlage.

2. Riskmanagement

2.1 Context van Deelnemers

De Deelnemers beheren voorzieningen die cruciaal zijn voor het functioneren van de Nederlandse overheid en die daarom als vitale dienst door de Nederlandse overheid zijn gekwalificeerd. De beschikbaarheid van deze voorzieningen is van groot belang voor de continuïteit van de maatschappelijke dienstverlening. De Deelnemers verwerken hiervoor gegevens van burgers en organisaties waarvan verlies, uitlekken of verminking schade kan berokkenen aan de betrokkenen. De leveranciers en dienstverleners, zoals die van de SMS-Gateway, maken onderdeel uit van het riskmanagement en leveren hieraan een actieve bijdrage. Er wordt daarbij gevraagd om een hoge mate van transparantie en een intensieve samenwerking op het gebied van riskmanagement.

Als onderdeel van de Rijksoverheid, houden alle Deelnemers ook rekening met dreiging van statelijke actoren en 'advanced persistent threats' (langdurig gerichte cyberaanval). Op basis van de Quick Scan nationale veiligheid is een risicoanalyse uitgevoerd, waarbij aanvullende risico's zijn geïdentificeerd voor de dienstverlening. Het is daarom essentieel om ook bij een crisis van Nationale Veiligheid de juiste samenwerking te blijven handhaven.

2.2 Eisen aan riskmanagement

Onderstaande eisen hebben betrekking op riskmanagement. Op basis van de te leveren diensten zullen de Deelnemers het riskmanagement nader afstemmen met de Opdrachtnemer.

Eisen riskmanagement		
ID	**Onderwerp**	**Beschrijving**
2.2.1	Riskmanagement methodiek	Opdrachtnemer gebruikt een riskmanagement methodiek middels een geaccepteerde, marktconforme methode (bijv. ISO27001) met de scope van de Prestatie.
2.2.2	Aansluiting bij riskmanagement van Deelnemer	Opdrachtnemer draagt actief bij en saan op het riskmanagement van Deelnemer. Partijen werken hierbij proactief samen. Opdrachtnemer informeert de Deelnemer indien er (nieuwe of aanvullende) risico's optreden die invloed kunnen hebben op het leveren van de Prestatie.
2.2.3	Riskmanagement rapportage en overleg	Ten aanzien van riskmanagement dient Opdrachtnemer aan te kunnen tonen dat haar maatregelen en organisatie effectief werken. Hiervoor behoeven Deelnemers rapportages van Opdrachtnemer. Opdrachtnemer zal in deze verplichting voorzien, en blijven voorzien bij wijzigende omstandigheden zoals wijzigingen in de methodiek, de vigerende normenkaders en resultaten van risicoanalyses. Opdrachtnemer participeert in een periodiek (tactisch) overleg met de Deelnemers. Opdrachtnemer bespreekt risico's in het (tactisch) overleg. De frequentie en inhoud van dit overleg worden overeengekomen in de DAP.

Tabel 1: Eisen aan riskmanagement

2.3 Eisen aan Business Continuïteit en Disaster Recovery

Onderstaande eisen hebben betrekking op Business Continuïteit en Disaster Recovery. Op basis van de te leveren diensten zullen de Deelnemers de Business Continuïteit en Disaster Recovery nader afstemmen met de Opdrachtnemer.

Eisen Business Continuïteit en Disaster Recovery		
ID	**Onderwerp**	**Beschrijving**
2.3.1	Business Continuïteit methodiek	Opdrachtnemer past een geaccepteerde, marktconforme business-continuïteitsmethodiek toe (zoals ISO22301) die volledig aansluit op de scope van de Prestatie.
2.3.2	Aansluiting bij Business Continuïteit van Deelnemer	Opdrachtnemer draagt actief bij en sluit waar mogelijk aan op de business continuïteit van Deelnemer. Partijen werken hierbij proactief samen. Opdrachtnemer informeert de Deelnemer indien er (nieuwe of aanvullende) scenario's optreden bij de business continuïteit van de Prestatie.
2.3.3	Business Continuïteit- en Disaster Recoveryplan	Opdrachtnemer stelt een marktconform Business Continuïteit- en Disaster Recoveryplan op in samenspraak met de Deelnemers en houdt deze actueel. Het Business Continuïteit- en Disaster Recoveryplan verschaft inzicht hoe de impact op de Prestatie van Opdrachtnemer geminimaliseerd en de continuïteit gewaarborgd wordt. Opdrachtnemer test het Business Continuïteit- en Disaster Recoveryplan periodiek (minimaal jaarlijks) en na grotere aanpassingen zoals architectuur- of technologiewijzigingen en deelt de uitkomsten met de Deelnemers.
2.3.4	Disaster Recovery	Opdrachtnemer is verantwoordelijk voor de Disaster Recovery van de Prestatie onder normale omstandigheden en bij een crisis. In het geval van een crisis van nationale veiligheid, wanneer een of meer vitale belangen van Nederland worden bedreigd of geschaad, kan de coördinatie van de Disaster Recovery overgenomen worden door de Deelnemers.

Tabel 2: Eisen aan Business Continuïteit en Disaster Recovery

3. Compliance

3.1 Context van Deelnemers

De Deelnemers moeten voldoen aan de geldende wet- en regelgeving op het gebied van informatiebeveiliging, privacybescherming en openbaar bestuur. Op de door de Deelnemers beheerde applicaties en diensten kunnen specifieke wetten van toepassing zijn. De Deelnemers hebben tevens te maken met het beleid van haar opdrachtgevers (o.a. het Ministerie) en afnemers.

Deelnemers sturen actief op compliance aan de wet- en regelgeving, aan het geldende overheidsbeleid en aan de per applicatie of dienst geldende eisen. Hiervoor is in haar eigen beleid voor informatieveiligheid het overheidsbeleid, de wettelijke eisen en de eisen vanuit haar opdrachtgevers en afnemers verwerkt. De dienstverlening van leveranciers valt ook onder het compliance beleid, waardoor relevante input vanuit leveranciers over de invulling van beveiligingseisen en riskmanagement noodzakelijk is.

3.2 Eisen aan compliance

Onderstaande eisen hebben betrekking op compliance en zijn niet limitatief. Op basis van de te leveren diensten zal Opdrachtgever aan de uitvoering van de Dienstverleningsovereenkomst (DVO) aanvullende eisen stellen die passend zijn bij de Prestatie.

Eisen compliance		
ID	**Onderwerp**	**Beschrijving**
3.2.1	Beleid van Deelnemers	1. Deelnemers kunnen aanvullend beleid hebben voor de scope van de Prestatie. Dit informatieveiligheidsbeleid volgt het Rijksbeleid op het gebied van informatieveiligheid. 2. Deelnemers zijn gerechtigd om in de DAP aanvullend beleid op te leggen voor de uitvoering van de Prestatie. Opdrachtnemer is verplicht deze aanvullende eisen uit te voeren, dan wel zijn medewerking te verlenen aan de uitvoering van dit aanvullend beleid. 3. Het gaat hier onder andere om beleid voor privacy- en informatiebescherming in lijn met de aangegeven beleidsvisie, het VIR, het VIR-BI, Ministerieel beleid en de BIO.
3.2.2	Waarborging compliance wet- en regelgeving en beleid	Opdrachtnemer onderkent dat wet- en regelgeving en beleid gewijzigd kan worden en dat Opdrachtnemer gebonden is aan de gewijzigde wet- en regelgeving en beleid te voldoen binnen een redelijke termijn in overleg nadat de wijziging is ingetreden. (. Een voorbeeld is de recente inwerking getreden Cyberbeveiligingswet (implementatie van de NIS2-richtlijn) en de Wet weerbaarheid kritieke entiteiten (implementatie van de CER-richtlijn). Opdrachtnemer conformeert zich dat schriftelijke afstemming over non-compliance geaccepteerd moet worden door de Deelnemer, waarbij er tevens afspraken worden gemaakt over de duur van de exceptie. Afhankelijk van het risico van de non-compliance wordt de periode voor maximaal een jaar vastgelegd en geaccepteerd. Binnen deze periode dient de non-compliance verholpen te zijn of anders opnieuw geaccepteerd te worden, tenzij Opdrachtnemer schriftelijk gemotiveerd heeft aangegeven dat zij 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).
3.2.3	Waarborging wet- en regelgeving en beleid	Opdrachtnemer, Deelnemers en Opdrachtgever houden elkaar proactief op de hoogte van wijzigingen in wet- en regelgeving en beleid.

3.2.4	SOC-2/ ISAE 3000A type II verklaring	Opdrachtgever vereist een onafhankelijk bewijs van beheersing op uitgevoerde processen door Opdrachtnemer. Daartoe beschikt Opdrachtnemer over een actuele ISAE 3000A type II Assurance verklaring of (aantoonbaar) gelijkwaardig alternatief, voor de scope van de Prestatie. Het aantoonbaar gelijkwaardige alternatief voldoet tenminste aan het opleveren van bewijslast door een onafhankelijke Register IT-auditor (RE), aantoonbaarheid welke werkzaamheden daartoe worden uitgevoerd en welke bewijslast beschikbaar zal komen. Opdrachtnemer overlegt minimaal eenmaal per jaar deze ISAE 3000A type II verklaring (of aantoonbaar gelijkwaardig alternatief) aan Opdrachtgever. De verklaring bevat een mapping naar de volledige ISO 27002 normen/maatregelen-set binnen de werkzaamheden van de Prestatie, incl. eventuele aanvullende maatregelen van de Opdrachtnemer. Opdrachtgever bepaalt of er extra controls/maatregelen nodig zijn om een betere dekking voor de Prestatie van de Opdrachtnemer te realiseren. Deze extra controls worden afgestemd als bevinding op de verklaring, met als oplostermijn maximaal tot de volgende verklaring.
3.2.5	Opvolging bevindingen SOC-2/ ISAE 3000A type II verklaring	Ten aanzien van de jaarlijkse ISAE 3000A type II (of gelijkwaardige) verklaring geldt dat Opdrachtnemer de (materiële) bevindingen van de onafhankelijke Register IT-auditor (RE) deelt met de Deelnemers. Onder bevindingen wordt in zulks verstaan mogelijke tekortkomingen en/of aandachtspunten in de processen en techniek, alsmede de controls zelf. Op basis van de bevindingen zullen Partijen in gesprek gaan over de voorgestelde verbeteringen, acties, aanpak en timing en opvolging daarvan. De oplostermijn van de bevindingen is hierbij leidend.
3.2.6	Recht op audit	Opdrachtnemer conformeert zich dat het krijgen en aanleveren van een Assurance verklaring aan de Opdrachtgever geen vervanging is voor het recht om (aanvullende) audits uit te voeren bij de Opdrachtnemer.
3.2.7	Normen en standaarden	Opdrachtnemer zal jaarlijks aantoonbaar voldoen aan de vigerende normen die gelden voor de Prestatie, waarbij de volgende criteria gelden: a. Baseline Informatiebeveiliging Overheid BIO (vigerende versie), door middel van een mapping op de controls/maatregelen van de Opdrachtnemer, waarbij aangegeven wordt hoe de invulling bij de Opdrachtnemer plaatsvindt. b. NEN-NL-ISO/IEC 27001: Information securitymanagement systems Requirements (vigerende versie), door middel van een geldig certificaat met bijbehorende VvT. c. NEN-NL-ISO/IEC 27002: Code of practice for information security controls (vigerende versie), door middel van de verklaring uit eis 3.2.5. d. Opdrachtnemer conformeert zich aan de Standaarden op de "pas-toe-of-leg-uit" lijst van Forum Standaardisatie (vigerende versie), waarbij aangegeven wordt hoe de invulling bij de Opdrachtnemer plaatsvindt. Specifiek voor Browser-domeinen en e-mail dient permanent voldaan te worden aan de Internet.nl standaarden. Eventuele afwijkingen worden bij de Opdrachtgever vastgelegd en geaccepteerd of opgelost binnen een redelijke termijn in overleg.

Tabel 3: Eisen aan compliance

4. Informatiebeveiliging en privacybescherming

Informatieveiligheid en privacy worden gewaarborgd door het toepassen van informatiebeveiliging en privacybescherming. Informatiebeveiliging en privacybescherming omvat 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 de vigerende normen (op basis van wet- en regelgeving, besluiten en standaarden) die gelden voor de Prestatie.

4.1 Eisen aan informatiebeveiliging en privacybescherming

Onderstaande eisen hebben betrekking op de inrichting van informatiebeveiliging en privacybescherming en zijn niet limitatief. Op basis van de te leveren diensten zal Opdrachtgever aan de uitvoering van de overeenkomst eisen stellen die passend zijn bij de Prestatie.

ID	Item	Maatregel
4.1.1	Informatiebeveiligingsbeleid van Opdrachtgever	Opdrachtnemer dient op het moment dat hij daadwerkelijk Prestaties verleent aan Opdrachtgever te voldoen aan het informatiebeveiligingsbeleid (meest actuele versie) van Opdrachtgever.
4.1.2	BIO	Opdrachtnemer, dient op het moment dat hij daadwerkelijk Prestaties verleent aan Opdrachtgever voor wat de geleverde Prestatie te voldoen aan de Baseline Informatiebeveiliging Overheid ("BIO") https://www.bio-overheid.nl/bio2/bio-producten/baseline-informatiebeveiliging-overheid-2-bio2/ De BIO is gebaseerd op ISO 27001/2 en bevat een set extra maatregelen ten opzichte van ISO 27001 welke aangeduid zijn als overheidsmaatregel op niveau vier (4).
4.1.3	Verwerkersovereenkomst	Opdrachtnemer dient ten tijde in het kader van de verwerking van persoonsgegevens in conformiteit met de Algemene verordening gegevensbescherming (AVG) met Opdrachtgever een zogenaamde Verwerkersovereenkomst te sluiten conform Bijlage 28 (Model Verwerkersovereenkomst).
4.1.4	Informatiebeveiligings-rapportage en –overleg	Ten aanzien van informatiebeveiliging dient Opdrachtnemer aan te kunnen tonen dat haar beveiligingsmaatregelen en -organisatie effectief werkt. Dit behelst rapportage(s) over de werking van controles en processen, zo ook voor werkzaamheden uitbesteed aan Derde partijen. Hiervoor behoeft Opdrachtgever rapportages van Opdrachtnemer ten aanzien van informatiebeveiliging. Opdrachtnemer zal hierin voorzien, en blijven voorzien bij wijzigende omstandigheden zoals wijzigingen in de vigerende normenkaders, resultaten van risicoanalyses en security testen. Indien door Opdrachtgever noodzakelijk geacht, zal Opdrachtnemer participeren in een door Opdrachtgever (ad hoc) te initiëren informatiebeveiligingsoverleg met Opdrachtgever. Voor deelname aan dit overleg brengt Opdrachtnemer geen kosten in rekening.
4.1.5	Aanvullend op BIO 5.14.3	Voor HTTPS-verkeer tussen machines met een overheidspartij wordt gebruik gemaakt van PKIo-certificaten. Voor andere machine verbindingen (met ketenpartijen) wordt gebruik gemaakt van een geldig certificaat (o.b.v. X509 v3) dat uitgegeven is door een Certificaatautoriteit (CA) die onder toezicht staat van de EU. De status van de CA kent een Svc-status gelijk aan granted. CA's met een afwijkende status worden niet geaccepteerd. Het certificaat is ten minste een publiek vertrouwd Organization Validated (OV)-certificaat.

ID	Item	Maatregel
		Voor HTTPS-gebruik in een browserapplicatie wordt gebruik gemaakt van certificaten uitgegeven onder een publieke root. Het certificaat wordt ondersteund door tenminste Microsoft Edge, Mozilla FireFox, Apple Safari en Google Chrome zonder de installatie van een root certificaat. Het root certificaat kan wel vanuit het Operating System geleverd worden.
4.1.6	Aanvullend op verwerkersovereenkomst	Persoonsgegevens (zoals telefoonnummers) mogen alleen verwerkt worden voor het versturen van SMS-berichten. Opdrachtnemer zorgt dat – ook in de voortbrengingsketen, dus telecomproviders – door Opdrachtnemer verstrekte persoonsgegevens alleen voor dat doel gebruikt worden.
4.7.1	Aansluiting op incidentenproces van de deelnemer(s)	Beveiligingsincidenten worden direct gemeld bij de betreffende contactperso(o)n(en) zoals vermeld in de DVO van de Deelnemer.

Tabel 4: Eisen aan informatiebeveiliging en privacybescherming

5. Aanvullende maatregelen o.b.v. Quickscan nationale veiligheid

De overheid ondersteunt diverse vitale processen. Het inloggen met DigiD bijvoorbeeld is een vitaal proces met ca. 17 miljoen gebruikers, waarvan een groot gedeelte een ingesteld telefoonnummer heeft. Hierdoor vormt de database met gegevens van DigiD een grote set aan persoonsgegevens van burgers. Voor deze processen geeft de Quickscan nationale veiligheid aan dat er, op basis van een uitgevoerde risicoanalyse, risico's zijn voor de nationale veiligheid.

ID	Item	Maatregel
5.1.1	Gebruik	Bij het gebruik van de SMS-Gateway door een Deelnemer dient er een strikte scheiding te zijn tussen de Deelnemers, zodat het niet mogelijk is dat gebruikers van de ene Deelnemer de gegevens van andere Deelnemers kunnen inzien of de gegevensverwerking kunnen beïnvloeden.
5.1.2	Beheer (Deelnemers)	Het beheer uitgevoerd door een Deelnemer dient inzage te hebben in de volledige Monitoring & Logging van die Deelnemer van de SMS-Gateway. Bovendien dient het gebruik en de verschillende technische mogelijkheden daartoe gecontroleerd te kunnen worden. De Deelnemer zal hiervoor de cryptografische sleutels en secrets beheren.
5.1.3	Sleutels en secrets	De cryptografische sleutels en secrets die nodig zijn voor de operationalisering en het beheer van de SMS-Gateway blijven onder verantwoordelijkheid en beheer van de Deelnemer en de Deelnemer heeft te allen tijde toegang tot deze sleutels en secrets conform vastgestelde procedures. Deze procedures worden vastgelegd in een cryptografisch sleutelmanagementprotocol. Het kan nodig zijn dat bepaalde sleutels en secrets in een HSM of TPM -chip worden opgeslagen. Voor noodtoegang worden aanvullende procedures opgesteld.
5.1.4	Koppelvlak	Het koppelvlak tussen de Deelnemer en de SMS-Gateway verloopt via een besloten overheidsnetwerk zoals Diginetwerk, RON, etc. Ook voor alle beheerwerkzaamheden dient gebruik gemaakt te worden van een besloten overheidsnetwerk.
5.1.5	Beheer (SMS-Gateway)	Het beheer door de leverancier van de SMS-Gateway dient aangesloten te zijn op de Monitoring & Logging van de hele dienstverlening. Dit generieke beheer moet controleerbaar zijn voor alle Deelnemers.
5.1.6	Monitoring & Logging	De Monitoring & Logging geeft aan elke Deelnemer de volledige inzage op de werking van de SMS-Gateway (Gebruik, Beheer en Gegevensverwerking) voor de Deelnemer specifieke zaken en voor generieke beheerzaken (bijv. onderhoud op de infrastructuur). Inzage kan bijvoorbeeld gegeven worden middels het aanbieden van een portal die deze gegevens ontsluit. Deze Monitoring & Logging is aantoonbaar compleet en ongewijzigd en is gescheiden per Deelnemer. Verder is deze aangesloten op de Security Operations Centre processen van de Deelnemer. Afwijkingen in de Monitoring & Logging worden als incident behandeld conform het incidentenproces van de Deelnemer.
5.1.7	Gegevensverwerking	Bij de gegevensverwerking van de SMS-Gateway, dient er een strikte scheiding te zijn tussen de gegevens van de Deelnemers, zodat het niet mogelijk is dat gebruikers van de ene Deelnemer de gegevens van andere Deelnemers kunnen inzien of de gegevensverwerking kunnen beïnvloeden. Voor bepaalde Deelnemers is het noodzakelijk dat het telefoonnummer van de ontvanger en/of de inhoud van het bericht afgeschermd wordt van de leverancier van de SMS-Gateway. Dit vanwege de gevoeligheid van de ontvangers. De gegevensverwerking dient per Deelnemer afgesplitst te kunnen worden en voortgezet te kunnen worden op een

ID	Item	Maatregel
		aangewezen infrastructuur en/of datacenterlocatie, waarbij gebruik gemaakt kan worden van alternatieve componenten voor het leveren van de dienst. Er wordt hiervoor in overleg met de Deelnemer een uitwijkplan opgesteld en geoefend. Bij een crisis van Nationale Veiligheid kan de Deelnemer de uitvoering van het uitwijkplan vereisen. De crisis-organisatie kan bij uitwijk buiten de Deelnemer komen te liggen, en de werklocatie(s) en het in te zetten personeel kan aan extra beveiligingsmaatregelen onderworpen worden.
5.1.8	Notificatiekanaal (SMS)	Het notificatiekanaal is zodanig ingericht dat de SMS-Gateway een directe netwerkkoppeling met Nederlandse telecomproviders heeft. Voor buitenlandse telecomproviders mag een andere technische route genomen worden. Voor bepaalde Deelnemers is het noodzakelijk dat het bericht direct afgeleverd wordt enkel bij de betreffende Nederlandse telecomprovider. Voor bepaalde Deelnemers is het noodzakelijk dat het gebruikte telefoonnummer van de ontvanger direct na aflevering verwijderd wordt uit de administratie van de SMS-Gateway. Er zijn in de techniek waarborgen dat het juiste (en ongewijzigde) bericht bij de juiste telecomprovider wordt afgeleverd. De vertrouwelijkheid van de berichten is niet van dien aard dat deze end-to-end versleuteld moeten worden. Het kan zijn dat in de contractperiode technieken als Rich Communication Services (RCS) worden beproefd.
5.1.9	Ontvanger	De ontvanger van het bericht moet kunnen controleren dat het bericht daadwerkelijk afkomstig is van de Deelnemer. De ontvanger krijgt geen inzage in de (interne) gegevensverwerking van de SMS-Gateway of de aanlevering van het bericht bij de SMS-Gateway.
5.1.10	Controle van de maatregelen	Er wordt door de leverancier een (Informatie)Beveiligingsfunctionaris aangewezen voor de opdracht. Deze Beveiligingsfunctionaris binnen zijn organisatie is de primaire contactpersoon voor de aanvullende contracteisen Risk, Compliance en Informatieveiligheid. De functionaris is belast met de dagelijkse zorg voor de beveiliging, oefent toezicht uit en voert jaarlijks een Zelfinspectie uit op basis van de BIO en de ABRO. De resultaten van de Zelfinspectie en de opvolging van bevindingen zijn schriftelijk vastgelegd en maken deel uit van de Assurance van de opdracht.
5.1.11	Assurance	Bij aanvang van de levering van de Prestatie zal de transitiefase beginnen. In deze fase zal de Deelnemer de opzet en het bestaan van de maatregelen controleren en beoordelen. Dit is te zien als het "recht op audit" van de opdrachtgever en/of Deelnemer. Deze beoordeling zal leiden tot een verklaring van "Operational Readiness" vanuit de Deelnemer waaruit blijkt dat de maatregelen voldoende geïmplementeerd zijn en of er eventueel restrisico's zijn. De afronding van de transitiefase volgt hierop. Tijdens de levering van de Prestatie zal er onafhankelijke assurance plaatsvinden. Dit gebeurt aan de hand van een onafhankelijke beoordeling van beheersing op uitgevoerde processen rondom de risico's van de Prestatie. Daartoe wordt door de leverancier een geldige ISAE 3000A type II Assuranceverklaring of (aantoonbaar) gelijkwaardig alternatief overlegd, voor de scope van de Prestatie. Het aantoonbaar gelijkwaardige alternatief voldoet tenminste aan het opleveren van bewijslast door een onafhankelijke Register IT-auditor (RE), aantoonbaarheid welke werkzaamheden daartoe worden uitgevoerd en welke bewijslast beschikbaar zal komen, en zal ook op werking (cf. type II) toetsen. De verklaring wordt minimaal eenmaal per jaar overlegd aan de Deelnemer. Op basis van de Assuranceverklaring zal er vanuit centraal contractmanagement gestuurd worden op de Prestatie.

ID	Item	Maatregel
5.1.12	Uitwijkplan	Bij een crisis van Nationale veiligheid, wanneer een of meer vitale belangen van Nederland worden bedreigd of geschaad, kan de Deelnemer de uitvoering van het afgesproken uitwijkplan vereisen. De gegevensverwerking dient per Deelnemer afgesplitst te kunnen worden en voortgezet te kunnen worden op een aangewezen infrastructuur en/of datacenterlocatie, waarbij gebruik gemaakt kan worden van alternatieve componenten voor het leveren van de Dienst. Er wordt hiervoor in overleg met de Deelnemer een uitwijkplan opgesteld en geoefend. De crisis-organisatie kan bij uitwijk buiten de Deelnemer komen te liggen, en de werklocatie(s) en het in te zetten personeel kan aan extra beveiligingsmaatregelen onderworpen worden. Het uitwijkplan dient binnen 3 maanden na ondertekening Overeenkomst te worden overlegd.