Rijksvastgoedbedrijf
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Verslag marktconsultatie. Impact van de invoering van de BIO2 voor opdrachtnemers én het Rijksvastgoedbedrijf (RVB) t.a.v. de vastgoed gebonden systemen die het RVB in beheer heeft.

Versienummer 2

Datum	29 juli 2026
Status	Definitief

Colofon

Projectnaam	
Documentkenmerk	49979
Versienummer	
Projectleiders	Olaf Stins, Shaam Ramnarain
Contactpersoon	Jörgen Guntlisbergen Expert Vastgoed en Infrastructuur T 0653690531 jorgen.guntlisbergen@rijksoverheid.nl DG Vastgoed en Bedrijfsvoering Rijk | DGVBR-RVB-Transacties & Projecten | DGVBR-RVB-T&P-Inkoop&Contractmanagement Korte Voorhout 7 | 2511 CW Den Haag Postbus 16169 | 2500 BD
Bijlage(n)	2
Auteurs	Jurgen Guntlisbergen

Inhoud

Voorwoord

Voor u ligt het verslag van de marktconsultatie die het Rijksvastgoedbedrijf heeft gehouden ten behoeve van een onderzoek naar de impact van de invoering van de BIO2[1] voor opdrachtnemers én het Rijksvastgoedbedrijf (RVB) t.a.v. de vastgoed gebonden systemen (VGS) die het RVB in beheer heeft.
De marktconsultatie is gehouden in de vorm van een 'open marktconsultatie' met daarna verdiepingsgesprekken met 5 geselecteerde marktpartijen. Daarnaast is dit onderwerp ook besproken in de workshop Informatiebeveiliging, groei en standaardisatie! op de RVB marktmiddag op 13 april 2026.
Dit document betreft een verslag van de antwoorden en adviezen uit de schriftelijke rapportage, de workshop en de verdiepingsgesprekken.

[1] Baseline Informatiebeveiliging Overheid, versie 1.2.

1 Inleiding

De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen, dus ook voor het Rijksvastgoedbedrijf. Op 5 maart 2026 is de "BIO2" v1.3 van 9 januari 2026 gepubliceerd in de Staatscourant.
De BIO2 richt zich op het beveiligen van informatie binnen de overheid. Naast de eigen bedrijfssystemen beheert het Rijksvastgoedbedrijf binnen het Rijk ook vastgoed gebonden systemen die informatie genereren, ook deze dienen aan de BIO2 te voldoen.

1.1 Doel van de marktconsultatie

Het RVB had met de marktconsultatie de volgende doelen:

1. Hoe kunnen we gezamenlijk (RVB en de opdrachtnemers/leveranciers) voldoen aan de BIO2. De BIO2 geeft invulling aan de zorgplicht van de Cyberbeveiligingswet (de Nederlandse wet voor de Europese NIS2-richtlijn)
2. Toetsen of de aanpak en methodiek van het RVB werkbaar is.

1.2 Probleemschets

De BIO2 richt zich op het beveiligen van informatiesystemen binnen de overheid, waaronder gebouwinstallaties zoals klimaatbeheersing, toegangscontrole, brandmeldsystemen en energienetwerken. Deze systemen zijn steeds vaker verbonden met IT-netwerken (IoT, Building Management Systems), waardoor ze kwetsbaarder worden voor cyberrisico's. Een aanval op deze systemen kan leiden tot fysieke gevolgen, zoals storingen in kritieke processen, veiligheidsrisico's of dienstuitval.

Gebouwinstallaties vallen onder de BIO2 omdat ze deel uitmaken van het informatiesysteem. Een cyberincident kan kritieke diensten verstoren, zoals veiligheidssystemen of toegangscontrolesystemen.

Binnen de overheid geldt de BIO2 als kader voor informatiebeveiliging. De BIO2 heeft een verplichtend karakter en geeft invulling aan de zorgplicht van de Cyberbeveiligingswet. De BIO2 zal dan ook voor de leveranciers, aannemers, onderhoudspartijen etc. van het Rijksvastgoedbedrijf impact hebben.

Met deze marktconsultatie wilde het RVB samen met de markt de impact in kaart brengen en kijken hoe we gezamenlijk op praktische wijze de eisen kunnen implementeren en borgen.

1.3 Aanpak van de marktconsultatie

Het Rijksvastgoedbedrijf heeft op 10 maart 2026 de marktconsultatie op TenderNed gepubliceerd (TenderNed kenmerk: TN575607). Door het Rijksvastgoedbedrijf is een vragenlijst gepubliceerd, waarbij de markt is gevraagd om uiterlijk 3 april 2026 de vragenlijst met antwoorden via TenderNed terug te sturen. Van 11 marktpartijen zijn vragenlijsten ontvangen.
Op de jaarlijkse RVB marktmiddag op 13 april 2026 is door het BIO programma een workshop gehouden over dit onderwerp (Informatiebeveiliging, groei en standaardisatie, in gesprek!). In deze workshop zijn de eerste indrukken van de

vragenlijsten gedeeld en is met aanwezigen marktpartijen in dialoog gegaan over de markt.
Besloten is om met 5 marktpartijen een individueel verdiepingsgesprek te houden. Hiervoor zijn partijen geselecteerd uit verschillende branches om zodoende een representatief marktbeeld te verkrijgen. Dit betreffen leveranciers van systemen, installateurs en een adviesbureau. De gesprekken vonden plaats in juni en juli 2026. Voor het verdiepingsgesprek ontvingen de deelnemers vooraf een casus met vragen, aan de hand waarmee het gesprek heeft plaatsgevonden.

2 Onderzoeksvragen en reacties

De marktconsultatie had op hoofdlijnen de volgende onderzoeksvragen:

1. Bekendheid met de BIO2 binnen de markt.
2. Wat heeft de markt van het RVB nodig.
3. Is de aanpak die het RVB voor ogen heeft werkbaar en helpt dit marktpartijen.
4. Welke besturing is voor de markt het meest passend (Governance).
5. Is ondersteuning door specialistische partijen een goed idee.
6. Hoe kan de informatiebeveiliging het beste geborgd worden en blijven (ISMS)?
7. Overige adviezen

2.1 Onderzoeksvraag: bekendheid met de BIO2

Door deelnemers aan de marktconsultatie is benadrukt dat er binnen hun organisaties een brede en diepgaande kennis aanwezig is van de BIO2-maatregelen en de daarbij behorende wet- en regelgeving. Veel organisaties beschikken over ervaring met ISO 27001, ISO 27002, NIS2, ABRO, ABDO en andere relevante standaarden, wat hen in staat stelt om de BIO2-eisen effectief te interpreteren en toe te passen. Deze kennis is vaak opgebouwd door middel van certificeringen, audits, implementatietrajecten en samenwerkingen met overheden en andere partijen in de keten. Daarnaast hebben deelnemers aangegeven dat zij beschikken over gespecialiseerde expertise op het gebied van cybersecurity, risicomanagement, informatiebeveiliging en OT-systemen, wat essentieel is voor de implementatie van BIO2-maatregelen in complexe omgevingen zoals die van het RVB.

De organisaties geven aan in hoge mate in staat te zijn om de BIO2-maatregelen te implementeren als opdrachtnemer en leverancier voor het RVB. Dit wordt onderbouwd door hun bestaande certificeringen, zoals ISO 27001, en hun ervaring met het implementeren van vergelijkbare maatregelen in zowel IT- als OT-omgevingen. Deelnemers benadrukken dat zij kunnen bijdragen aan alle fasen van de implementatie, van risicoanalyse en ontwerp tot uitvoering, beheer en auditing. Daarnaast kunnen zij ondersteuning bieden bij het vertalen van BIO2-eisen naar concrete, toepasbare maatregelen, rekening houdend met de specifieke context en behoeften van het RVB. Sommige organisaties geven aan dat zij al grotendeels compliant zijn met BIO2 via hun bestaande ISO 27001-certificering, waarbij alleen specifieke overheidsmaatregelen aanvullende aandacht vereisen.

2.2 Onderzoeksvraag: wat heeft de markt van het RVB nodig?

Om de BIO2-maatregelen succesvol te kunnen implementeren en te voldoen aan de wet- en regelgeving, hebben de deelnemers aan de marktconsultatie een aantal essentiële behoeften geïdentificeerd waar het RVB aan zou moeten voldoen. Allereerst is er behoefte aan duidelijke en eenduidige kaders, zoals een definitieve classificatiematrix, gedetailleerde functionele en niet-functionele eisen voor standaard bouwblokken. Verder is er behoefte aan toegang tot relevante documentatie, betrokken stakeholders en systeeminformatie. Ten slotte geven deelnemers aan dat een gestructureerde aanpak, met heldere fasering en rapportageformaten, essentieel is voor een effectieve implementatie en naleving van de BIO2-maatregelen.

Daarnaast benadrukken de marktpartijen de noodzaak van uniformiteit en standaardisatie in de uitvraag en architectuur, om verschillen tussen RVB-regio's te voorkomen en een consistente aanpak te waarborgen. Ook wordt gewenst dat het RVB duidelijk communiceert over de impact van BIO2- en ABRO-maatregelen in aanbestedingen, zodat marktpartijen deze kunnen prijzen en voldoen aan de eisen. Een andere belangrijke behoefte is samenwerking en kennisdeling tussen het RVB en de marktpartijen, waarbij een ecosysteem wordt gecreëerd waarin dreigingen en uitdagingen gezamenlijk worden besproken. Dit stimuleert innovatie en zorgt voor een betere afstemming tussen partijen.

2.3 Onderzoeksvraag: Is de aanpak die het RVB voor ogen heeft werkbaar en helpt dit marktpartijen

Toelichting:
De aanpak die het RVB voor ogen heeft ziet er als volgt uit. Het RVB is voornemens om de BIO2 maatregelen te vertalen naar concrete uitvoerbare oplossingen en ziet de volgende route:

- *Door middel van classificatie wordt bepaald welke niveau van weerstand er geboden dient te worden*
- *Aan de weerstandsniveaus zijn BIO2 maatregelen gekoppeld welke voor het RVB concreet vertaald zijn naar de 'Wat'*
- *De RVB architectuur geeft invulling aan de 'Wat' door richting te geven aan de oplossing in de vorm van standaard bouwblokken[2] voor de benodigde netwerken en infrastructuur (o.a. servers). Architectuur dient gezien te worden net als architectuur bij het bouwen van een huis.*
- *Door het volgen van de bovenstaande aanpak is er een gestandaardiseerde oplossing die geïmplementeerd kan worden. Hiermee voldoet het RVB aan standaarden en tevens aan wet- en regelgeving voor BIO2.*

De voorgestelde aanpak van het RVB – waarbij BIO2-maatregelen worden vertaald naar concrete uitvoerbare oplossingen via classificatie, weerstandsniveaus en standaard bouwblokken – wordt door de marktpartijen over het algemeen als werkbaar beoordeeld. De gestructureerde methodiek biedt duidelijke kaders, vermindert interpretatieverschillen en versnelt de implementatie van BIO2-maatregelen.

Waar de aanpak helpt

Classificatie en weerstandsniveaus als startpunt.
Deelnemers benadrukken dat het bepalen van weerstandsniveaus via classificatie een helder kader creëert om te bepalen welke beveiligingsmaatregelen noodzakelijk zijn. Dit sluit aan bij het risico gestuurde werkwijzen en zorgt voor een efficiënte en proportionele toepassing van maatregelen.

Vertaling naar concrete "Wat"-eisen en bouwblokken
Het koppelen van weerstandsniveaus aan BIO2-maatregelen en het vertalen hiervan naar standaard bouwblokken (bijv. netwerken, infrastructuur, servers) wordt gewaardeerd als een juiste stap. Dit biedt uniformiteit, voorspelbaarheid en herbruikbaarheid, wat de implementatie versnelt.

[2] Voorbeeld van bouwblokken zijn: *Externe toegang, Back-up & Restore, Local Area Network en OT Monitoring*.

Ontbrekende stappen in de aanpak:

Uniformiteit en standaardisatie
Eenduidige kaders en architectuur: Deelnemers benadrukken de noodzaak van uniforme uitvragen en standaardisatie in de architectuur over het hele land. Momenteel zijn er verschillen tussen RVB-regio's, wat de implementatie bemoeilijkt

Samenwerking en kennisdeling
Ecosysteem en community: Deelnemers pleiten voor een ecosysteem waarin dreigingen en uitdagingen gezamenlijk worden besproken. Dit stimuleert innovatie en zorgt voor betere afstemming tussen partijen.

2.4 Onderzoeksvraag: welke besturing is het meest passend (governance)

Regierol RVB
De marktpartijen zijn van mening dat het RVB de regierol moet behouden.
De onderlinge afhankelijkheid van de VGS bouwblokken en bijbehorende hardware, firmware en softwareversies, is groot. Het door een VGS-onderhouder individueel doorvoeren van updates is niet wenselijk.

Hieronder de grote lijn van de adviezen en belangrijkste aanbevelingen:

Het RVB moet de regisseur zijn en verantwoordelijk blijven voor beleid, architectuur, contractmanagement en security policy.
Uitvoering (technische implementatie) kan worden gedelegeerd aan
Een SIAM-partij (Service Integration and Management)

Coördinerende rol: hoofdaannemer/hoofd onderhoudscontractant:
Binnen een project kan de coördinerende rol het beste ingevuld worden door de hoofdaannemer. Bij een onderhoudscontract ingeval van een integraal onderhoudscontract (GIC/IBC) de hoofdopdrachtnemer, in andere gevallen de E&K-installateur.

Zorg voor een duidelijke RASCI voor verantwoordelijkheden en rollen.

2.5 Onderzoeksvraag: is ondersteuning door specialistische partijen een goed idee?

Toelichting: RVB denkt aan het aansluiten van specialistische partijen op het gebied van netwerken en infrastructuur voor de implementatie van de BIO2 maatregelen.

De marktpartijen zijn overwegend positief over de inzet van specialistische partijen voor de implementatie van BIO2-maatregelen, met name voor opdrachtnemers die minder expertise in huis hebben. Deze ondersteuning helpt om compliance te waarborgen en de kwaliteit van de implementatie te verhogen.

Specialistische partijen bieden toegevoegde waarde op de volgende gebieden:

Technische expertise: Kennis van IT/OT-omgevingen

Kwaliteit en consistentie: Externe partijen brengen best practices in, beperken fouten in ontwerp en configuratie, en zorgen voor uniforme toepassing van maatregelen.
Aantoonbaarheid: Ondersteuning bij documentatie en toetsing is essentieel voor compliance en audits.
Risicobeheersing: Specialisten helpen bij het inschatten en mitigeren van risico's.
Onafhankelijke toetsing: Het RVB kan onafhankelijke partijen inschakelen voor audits.

2. Voor wie is ondersteuning relevant?
Opdrachtnemers met beperkte expertise: Specialistische partijen kunnen kennis gaten opvullen voor opdrachtnemers die niet over voldoende in-house kennis beschikken om BIO2-maatregelen volledig te begrijpen en toe te passen .
Kleine partijen: Voor kleinere leveranciers is het lastig om zelf aan alle BIO2 -eisen te voldoen. Specialistische ondersteuning helpt hen om compliant te blijven.
Complexe systemen: Bij systemen met veel koppelvlakken (bijv. OT/IT-integratie) is externe expertise vaak noodzakelijk om consistente en veilige implementaties te realiseren

2.6 Onderzoeksvraag: Hoe kan informatiebeveiliging binnen ISMS het beste geborgd worden en blijven

Uit de gevoerde gesprekken komen de volgende belangrijkste adviezen en inzichten naar voren over hoe informatiebeveiliging het beste geborgd kan worden en blijven binnen een ISMS voor de BIO2-implementatie bij het RVB.

1. Structuur en processen
Cyclische controles en audits: Regelmatige PDCA-cyclus (Plan-Do-Check-Act) met audits en pentesten op basis van informatiebeveiligingsprincipes is essentieel om compliance te waarborgen.
Security by Design & Default: Beveiliging moet al vanaf het ontwerp (Security by Design) en met standaardveilige instellingen (Security by Default) worden meegenomen.
Need-to-know-toegang: Toegang tot systemen en data moet beperkt worden tot alleen wat noodzakelijk is (least privilege-principe).

2. Asset- en configuratiemanagement
Centrale CMDB (Configuration Management Database): Een centrale asset- en configuratiedatabase is cruciaal voor lifecycle management, BIO2-compliance, wijzigingen en audits. Het RVB zou idealiter een centrale CMDB moeten inrichten om overzicht te houden over alle systemen, configuraties en wijzigingen.

3. Bewustwording en training
Security Awareness-trainingen: Regelmatige bewustwordingstrainingen voor medewerkers en leveranciers zijn noodzakelijk om menselijke fouten (bijv. wachtwoorden die openlijk hangen) te voorkomen

Communicatie over werkstromen: Duidelijke communicatie over incidentmeldingen (bijv. aan het NCSC) en werkprocessen is essentieel. Incidentmeldingen moeten altijd door de regievoerder worden gedaan.

4. Wijzigingsbeheer en incidentafhandeling
Door een centrale wijzigings- en incidentmanagementproces wordt een uniforme werkwijze geborgd en wordt de beschikbaarheid, integriteit en vertrouwelijkheid van

de IT-omgevingen aantoonbaar ondersteund. Daarnaast draagt het proces bij aan continue verbetering van de dienstverlening en een hogere weerbaarheid tegen verstoringen en cyberincidenten.

5. Samenwerking en ketenverantwoordelijkheid
Ketenproces voor wijzigingen: Wijzigingen moeten worden gezien als een ketenproces onder centrale regie van het RVB. Alle betrokken partijen (installateurs, systeemintegratoren, OT-platformleveranciers, cybersecuritypartners) moeten vanaf de impactanalyse worden betrokken bij beoordeling, planning, uitvoering en acceptatie.

Samenwerkingsclausules: In contracten moeten samenwerkings- en ketenverantwoordelijkheden worden opgenomen om te voorkomen dat partijen eenzijdig wijzigingen doorvoeren.

Ecosysteem van leveranciers: Het RVB kan leveranciers in een ecosysteem zetten waarin dreigingen en uitdagingen gezamenlijk worden besproken. Dit stimuleert innovatie en zorgt voor betere afstemming.

6. Classificatie en risicobeheersing
Classificatie van panden en systemen: Het RVB werkt aan een methodiek om objecten te classificeren op basis van BIO2, gevolgd door passende maatregelen. Uniformiteit in classificatie is essentieel.

Risicoanalyse (RIA): Een Risico Impact Analyse (RIA) is noodzakelijk om de impact van wijzigingen en incidenten te beoordelen.

Rubricering en ABRO: Bij opdrachten met gerubriceerde informatie (bijv. TBB of Dep.V) moet het RVB en opdrachtnemers ook voldoen aan de ABRO. Het RVB moet hier al in de aanbestedingsfase rekening mee houden.

7. Technische maatregelen
Segmentatie en beveiligde koppelingen: Duidelijke IT/OT-scheiding, netwerksegmentatie en beveiligde koppelingen zijn essentieel, met name voor systemen zoals toegangscontrole, camera-infrastructuur en gebouwbeheersystemen.

Toegangsbeheer: Strikte toegangscontrole (least privilege, logging, controleerbaarheid) voor externe partijen, met name bij toegang op afstand.

Assurance-rapportages: Het RVB kan kritieke leveranciers vragen om assurance-rapportages om risico’s te beheersen.

2.7 Overige adviezen

1. Eenduidigheid en standaardisatie
Eenduidige definities: Zorg voor duidelijke definities van begrippen zoals scope, classificatie/weerstandsniveaus, OT/IT om interpretatieverschillen te voorkomen.
Testbare eisen: Maak eisen auditeerbaar door acceptatiecriteria en bewijsvoering te specificeren, en sluit aan op bestaande standaarden (bijv. ISO 27001, NIS2) waar mogelijk.

Stabiele standaarden: Werk met een beperkte set stabiele standaarden en lever duidelijke templates voor oplevering en commissioning, om consistentie te waarborgen.
Uniforme uitvragen: Het RVB moet uniforme uitvragen en architectuur hanteren in het hele land, om verschillen tussen regio's te voorkomen

2. Beheerfase en lifecycle management
Expliciete aandacht voor beheer: Besteed expliciet aandacht aan de beheerfase, inclusief:
Monitoring (centrale logging, SIEM-koppeling).
Patching (regelmatige updates en kwetsbaarheidsbeheer).
Lifecycle management (assetbeheer, verouderde systemen).
Incidentrespons (incl. ketenpartners, meldingen aan NCSC) .
Assetbeheer: Zorg voor assetbeheer, ook voor kleine gebouwen (al is dit beperkter). Werk toe naar een standaard structuur voor alle panden

4. Kennis en bewustwording
Kennisdeling en training: Organiseer kennisdeling (bijv. Masterclasses ABRO in samenwerking met NIDV) om het kennisniveau bij opdrachtgevers en opdrachtnemers te vergroten.
Bewustwordingstrainingen: Zorg voor regelmatige Security Awareness-trainingen voor medewerkers en leveranciers, met name om menselijke fouten (bijv. wachtwoorden die openlijk hangen) te voorkomen

Eigen organisatie meenemen: Neem de eigen organisatie van het RVB mee in de ontwikkeling, met name kennis over ABRO, classificering en cyberwetgeving

5. Contractuele en inkoopgerelateerde adviezen
ISO 27001 als voorwaarde: Vereis in het inkooptraject dat partijen die toegang krijgen tot RVB-informatie, locaties en/of systemen over een ISO 27001-certificering beschikken. Dit waarborgt compatibiliteit met BIO2 .

6. Integratie van kaders en toetsing
"Test once, comply to many": Ondersteun een geïntegreerd raamwerk waarin BIO2, NIS2, ABRO, Cyberbeveiligingswet (CBW) en Cyber Resilience Act (CRA) samenkomen. Hierdoor kunnen controles en audits één keer worden uitgevoerd en voor meerdere wettelijke verplichtingen worden hergebruikt .
Expliciete toetsingsvormen: Leg per bouwblok en weerstandsniveau expliciet vast welke onafhankelijke toetsingsvorm vereist is (bijv. penetratietest, architectuurreview, BIA/RIA/PIA) en met welke frequentie .
Samenhang tussen kaders: Integreer BIO2, ABRO, CBW en CRA vroegtijdig in de bouwblok-architectuur om latere aanpassingen te voorkomen .

7. Praktische uitvoering en samenwerking
Periodieke afstemming: Organiseer periodieke afstemming met leveranciers om knelpunten vroeg te signaleren .
Centraal meldpunt voor incidenten: Richt een centraal meldpunt voor incidenten in binnen het RVB. Dit is essentieel voor de PDCA-cyclus (Plan-Do-Check-Act) en zorgt voor inzicht in de kwaliteit en volwassenheid van de opdrachtgever .
Ketenverantwoordelijkheid: Informatiebeveiliging is geen verantwoordelijkheid van alleen de opdrachtnemer, maar van de hele keten. Het RVB moet intern borgen dat medewerkers handelen in lijn met het beoogde ambitieniveau .

8. Overige specifieke adviezen

Beperkte set standaarden: Werk met een beperkte set stabiele standaarden om consistentie te waarborgen.
Commissioning lists: Gebruik commissioning lists om uniformiteit te waarborgen tussen installateurs en het RVB

Beheerlaptops: zorg voor beheerlaptops op locaties die opdrachtnemers kunnen gebruiken. Dit ter voorkoming van incidenten.

Bijlage 1 Verslag workshop RVB marktmiddag

Workshop Informatiebeveiliging, groei en standaardisatie!

Wat is er behandeld?
De workshop stond in het teken van Vastgoed Gebonden Systemen (VGS), of te wel de digitale componenten van de installaties ook wel operationele technologie genoemd.
Een aantal deelnemers van de marktmiddag hebben veel kennis van informatiebeveiliging een deel ook niet.

Het RVB is bezig met de voorbereiding voor de implementatie van de Baseline Informatiebeveiliging Overheid 2 (BIO2) voor VGS. Wat de BIO2 is en de opbouw van de BIO2 is kort gepresenteerd. Daarna is aangegeven hoe het RVB de implementatie aan het voorbereiden is en welke aanpak het RVB daarbij voor zich ziet. Hierover is vervolgens in gesprek gegaan.

De meeste deelnemers geven in het gesprek aan dat hun organisatie instaat is om de BIO2 te implementeren.

Aanpak en tips
Het groeipad en de beschrijving van de gewenste situatie kon rekenen op veel steun. Leveranciers geven aan dat het RVB één standaard voor de BIO2 eisen moet gaan voeren.
Het RVB hanteert verschillende standaarden afhankelijk van de klant of gebruiker. Standaarden verschillen ook door aanpassingen van projectteams op projectniveau. Bij instandhoudingscontracten wordt door leveranciers een vergelijkbare problematiek ervaren. In deze contracten zijn geen of verschillende informatiebeveiligingseisen opgenomen.

Een standaard voor de oplossing (digitale architectuur) wordt als positief ervaren. Wel wordt er aangegeven dat de standaard voor de oplossing voldoende gedetailleerd uitgewerkt moet worden zodat er een implementeerbare standaardoplossing ontstaat. Onderdeel van de uitwerking zijn de aansluitvoorwaarden van de verschillende VGS op de centrale infrastructuur.

Bij de inzet van een specialistische leverancier wordt aangegeven dat de regierol duidelijk belegd moet worden en dat er een duidelijke demarcatie van de werkzaamheden moet zijn.

Vervolg
Leveranciers geven aan met het RVB samen te willen werken aan de implementatie en zijn bereid hierover met het RVB in gesprek te gaan.
De komende maanden worden door RVB dialooggesprekken met leveranciers gevoerd om de implementatie en standaardisatie nader te bespreken.