BIR2017 FAQ's

Baseline Informatiebeveiliging Rijksdienst

Inhoudsopgave

Algemeen

Nr	Vraag	Antwoord
1.	**Waarom is er eigenlijk een nieuwe BIR nodig?**	De onderliggende ISO27001 standaard is in de periode 2014/2015 vernieuwd, waardoor ook een herziening van de BIR in de rede lag. De Algemene Rekenkamer adviseerde in mei 2015 een vernieuwing van de BIR en door het CIO-beraad werd de wens geuit om tot een handzamer BIR te komen met minder administratieve last.
2.	**Wat is er veranderd in de nieuwe BIR?**	Globaal zijn in de BIR2017 de volgende zaken veranderd: • Om risicomanagement hanteerbaar en efficiënt te houden kiest de BIR voor een diepgang van de uitwerking van het risicomanagement die proportioneel is aan de te beschermen belangen in combinatie met relevante dreigingen. Daartoe wordt onderscheid gemaakt in drie basisbeveiligingsniveaus (BBN 1 t/m 3). • Per control zijn rollen toebedeeld. • De BIR is geactualiseerd aan de hand van de nieuwe ISO27002 norm en de rijksmaatregelen zijn opgeschoond. • De ISO controls worden in de BIR2017 ongewijzigd gehanteerd. • De rijksmaatregelen zijn gesaneerd.
3.	**Op welke gebieden verbetert de BIR de beheerslast?**	De BIR vermindert de beheerslast door o.a. expliciet rekening te houden met BBN1 systemen, proportioneel risicomanagement toe te passen en proportionele verantwoording te vragen.
4.	**Wat is de relatie tussen de BIR en het VIR?**	De BIR vult enkele bepalingen uit het VIR op generieke wijze in. Het gaat hier met name om de in artikel 4, lid a en b, genoemde bepalingen ten aanzien van het uitvoeren van een risicoafweging om de betrouwbaarheidseisen vast te stellen en om, op basis van deze eisen, de juiste maatregelen uit te kiezen.
5.	**Welke wetgeving is opgenomen in de BIR?**	Waar van toepassing bevat de BIR verwijzingen naar de beveiligingsaspecten van de wet- en regelgeving die is vermeld in bijlage 1 van de BIR2017.
6.	**Zijn alle maatregelen vanuit privacy regelgeving ook opgenomen in de BIR?**	Nee, wel wordt in de BIR2017 waar nodig verwezen naar de AVG.
7.	**Wordt het nu veiliger met een nieuwe BIR?**	Door het toepassen van de BIR2017 wordt het eenvoudiger om de focus op feitelijke veiligheid te leggen. De BIR zelf is een instrument dat wel toegepast moet worden om de Rijksdienst veiliger te maken.
8.	**Biedt de BIR bescherming tegen statelijke actoren?**	Ja. Vanaf BBN2 vindt bescherming tegen statelijke actoren plaats in de vorm van detectie. BBN3 biedt tevens weerstand tegen APT's zoals de dreiging van statelijke actoren.
9.	**Bij wie kan ik terecht met vragen over de BIR?**	Bij de CIO of CISO van uw organisatie.
10.	**Wat moet ik doen als de BIR voor mijn situatie niet werkt?**	Het zal niet zo zijn dat de hele BIR niet werkt. In een explain kan aangegeven waarom bepaalde onderdelen van de BIR niet geïmplementeerd kunnen worden (bijvoorbeeld bij SCADA-systemen) en wat de alternatieve maatregelen zijn om de risico's af te dekken. In de jaarlijkse ICV kan dit vervolgens nog nader worden toegelicht.
11.	**Waarom ontbreekt een begrippenlijst?**	Sommige begrippen, zoals informatiesysteem, zijn al gedefinieerd in andere regelgeving zoals het VIR. Als in de praktijk blijkt dat bepaalde begrippen in de BIR nadere toelichting nodig hebben, dan zal dit in de toekomst mogelijk toegevoegd worden als onderdeel van het onderhoudsproces.
12.	**Komt er ook een BIR specifiek voor cloudtoepassingen?**	Nee, dat is niet nodig, want de BIR2017 is ook van toepassing op cloudtoepassingen. Daarnaast zijn er enkele handreikingen opgenomen over de cloud.

ISO 27001/27002

Nr	Vraag	Antwoord
13.	**Waarom gebruiken we niet gewoon de ISO27001?**	De ISO27001 is een strategisch kader. Het strategisch kader voor de informatie-beveiliging bij de Rijksdienst wordt gevormd door de voorschriften BVR, VIR en VIR-BI.
14.	**Waarom gebruiken we niet gewoon de ISO27002 als baseline?**	Dat is al het geval, de ISO 27002 vormt namelijk de basis van de BIR2017. Om de organisaties binnen de Rijksdienst inzicht te geven in wat men minimaal van elkaar kan verwachten, is in de BIR2017 een set concrete aanvullende maatregelen opgenomen, de rijksmaatregelen. De rijksmaatregelen die in de BIR2017 zijn opgenomen zijn noodzakelijk om te voldoen aan de beveiligingseisen uit belangrijke wet- en regelgeving en om betrouwbaar in ketens te kunnen samenwerken. Dit aangevuld met een aantal 'no brainers' die voor professioneel werken randvoorwaardelijk zijn.
15.	**Als mijn leverancier een (ISO-)-certificering heeft, is dat dan ook goed?**	Nee, het is mogelijk dat een (externe) dienstenleverancier beschikt over een ISO27001-certificering, ISAE3402-certificering of een ander kwaliteitskeurmerk. Een dergelijk keurmerk geeft een waarborg over het proces dat bij de diensten-leverancier is ingericht, maar geeft niet aan op welk niveau de beveiliging is gerealiseerd. Hoewel dit dus wel meerwaarde heeft, overlap kent met de BIR-controls en gebruikt kan worden als onderdeel van de Statement of Compliancy, omvat en vervangt het niet volledig de verantwoording over de rijksmaatregelen uit de BIR.
16.	**Zijn de implementatierichtlijnen uit de ISO verplicht?**	Nee, de implementatierichtlijnen zijn niet verplicht.
17.	**Op welke versie van de ISO is de BIR gebaseerd?**	Bij het opstellen van de BIR2017 is de meest recente Nederlandstalige versie van ISO 27002 gehanteerd (2015).
18.	**Wat gebeurt er als er een nieuwe versie van de ISO uitkomt?**	Dan wordt de BIR aangepast middels het evaluatie- en bijstellingsproces zoals beschreven in de BIR.
19.	**Waarom zijn in de BIR2017-spreadsheet alleen de controls en de rijksmaatregelen en niet alle implementatierichtlijnen uit de ISO-27002 opgenomen?**	Omdat de implementatierichtlijnen geen verplichtend karakter hebben en de controls en rijksmaatregelen wel.
20.	**Waar zijn de niveau 4 maatregelen uit de BIR 2012 gebleven?**	De niveau 4 maatregelen zijn in de BIR 2017 weergegeven als rijksmaatregelen. Ten aanzien van de niveau 4 implementatierichtlijnen uit de BIR 2012 is ervoor gekozen om in de BIR 2017 te verwijzen naar de ISO 27002 waarin deze per control zijn vermeld.
21.	**Waarom is in de BIR2017 een tweetal controls weggelaten uit de ISO27002?**	De controls 6.1.4 en 14.2.4 uit de ISO 27002 zijn in de BIR 2017 niet opgenomen, omdat deze binnen de specifieke context van de Rijksdienst onvoldoende toegevoegde waarde kunnen bieden.

BasisBeveiligingsNiveau's BBN's

Nr	Vraag	Antwoord
22.	**Waarom zijn er drie BBN's?**	Het onderscheid in drie BBN's voorkomt dat voor eenvoudige systemen zonder vertrouwelijke informatie teveel administratieve last wordt opgeroepen. Om risicomanagement hanteerbaar en efficiënt te houden, kiest de BIR voor een diepgang van de uitwerking van het risicomanagement die proportioneel is aan de te beschermen belangen in combinatie met relevante dreigingen.
23.	**Wat is het verschil tussen BBN2 en BBN3?**	BBN2 richt zich o.a. op departementaal vertrouwelijke informatie waarvan is vastgesteld dat die documenten niet interessant zijn voor statelijke actoren of criminele organisaties. Daarom zijn detectieve maatregelen voldoende voor BBN2. BBN3 gaat ook om departementaal vertrouwelijke informatie waarvan is vastgesteld dat deze wél interessant zijn voor o.a. statelijke actoren. Daarom worden in BBN3 maatregelen opgenomen die weerstand tegen deze actoren bieden.
24.	**Hoe moet ik het juiste BBN kiezen?**	De BIR gaat vergezeld van de BBN-toets. In deel 2 van de BIR is deze toets opgenomen.
25.	**Wat is de relatie tussen rubricering en de in de BIR beschreven schadescenario's voor vertrouwelijkheid?**	Als informatie als staatsgeheim (Stg) is gerubriceerd dan komt het systeem uit op een schadescenario dat hoger ligt dan vertrouwelijkheid Hoog. Dat betekent dat altijd BBN3 van toepassing is en dat dit aangevuld moet worden met maatregelen voor Stg. conform het VIRBI. Als informatie Departementaal Vertrouwelijk (DepV) gerubriceerd is dan zal bepaald moeten worden in hoeverre dit valt binnen het schadescenario M of H in de BIR2017. Ook in dit geval is het VIRBI van toepassing.
26.	**Als ik een systeem heb dat DepV informatie bevat, in welk BBN val ik dan?**	Op een dergelijk informatiesysteem is BBN2 of BBN3 van toepassing. Het verschil tussen BBN2 en BBN3 wordt in een andere vraag toegelicht.
27.	**Welk BBN moet ik kiezen als ik een hoge beschikbaarheid nodig heb?**	Dat is beschreven in stap 3 van de BBN-toets.
28.	**Als informatie DepV is gerubriceerd, wordt dan voldaan aan het VIRBI als alle rijksmaatregelen uit BBN 2 worden toegepast?**	Nee. Als informatie DepV is gerubriceerd dan dient tevens voldaan te worden aan de aanvullende eisen die het VIRBI stelt aan het beveiligen van bijzondere informatie.
29.	**Als informatie Stg of hoger is gerubriceerd, wordt dan voldaan aan het VIRBI als alle rijksmaatregelen uit BBN 3 worden toegepast?**	Nee. Als informatie Stg. of hoger is gerubriceerd dan dient tevens voldaan te worden aan de aanvullende eisen die het VIRBI stelt aan het beveiligen van bijzondere informatie.
30.	**Waarom zijn de BBN's vooral gebaseerd op vertrouwelijkheidniveaus?**	De BBN's zijn ook gebaseerd op verschillende niveaus van beschikbaarheid en integriteit. Verschillende niveaus van vertrouwelijkheid leiden tot grotere verschillen in te nemen maatregelen. Daarom komt dit in de verschillende BBN's meer tot uiting.
31.	**Wat is het nut van BBN1?**	Met de oude BIR moest elk systeem op een hoog basisniveau worden beveiligd. Met BBN1 is het mogelijk om voor eenvoudigere systemen zonder vertrouwelijke informatie aan minder complexe risicomanagement en verantwoordingseisen te voldoen, waarbij nog altijd wel een minimum beveiligingsniveau wordt gewaarborgd.
32.	**Op welk BBN wordt de generieke infrastructuur beveiligd?**	Het BBN van de generieke infrastructuur wordt door het collectief van opdrachtgevers bepaald.

Nr	Vraag	Antwoord
33.	**Wat is risicomanagement nu eigenlijk precies?**	Risicomanagement betreft het inzichtelijk en systematisch inventariseren, beoordelen en – door het treffen van maatregelen – beheersbaar maken van risico's en kansen, die het bereiken van de doelstellingen van de organisatie bedreigen dan wel bevorderen, op een zodanige wijze dat verantwoording kan worden afgelegd over de gemaakte keuzes. (Beveiligingsvoorschrift Rijksdienst, art.1 sub d) Onderdeel van risicomanagement is het uitvoeren van risicoanalyses.
34.	**Hoe gebruik je risicomanagement om tot maatregelselectie te komen?**	Een eerste stap om te komen tot maatregelselectie is het uitvoeren van een kwalitatieve risicoanalyse zoals de Quickscan Information Security (QIS, zie handreiking). Vervolgens kunnen aan de hand van een kwantitatieve risicoanalyse, bijvoorbeeld IRAM of de ISO-27005, de feitelijk benodigde maatregelen worden bepaald.
35.	**Is er een standaardmethode beschikbaar voor het uitvoeren van risicoanalyses?**	Er is geen standaardmethode verplicht gesteld. In de ISO-27005 wordt risicomanagement uitgewerkt. Het uitvoeren van een risicoanalyse is daar een onderdeel van. Binnen de Rijksoverheid wordt ook IRAM gehanteerd als standaardmethode.
36.	**Vervangt de BBN-toets de oude Quickscan BIR?**	Nee, de BBN-toets wordt gebruikt om het juiste BBN te selecteren en om te bepalen of er nog aanvullende maatregelen nodig zijn in het kader van beschikbaarheid of integriteit. Dit vervangt de Quickscan niet. De BBN-toets wordt wel geïntegreerd in de vernieuwde Quickscan.
37.	**Wordt de Quickscan BIR aangepast aan de BIR2017.**	Ja, de Quickscan wordt aangepast aan de nieuwe systematiek en krijgt daarom ook een nieuwe naam: Quickscan Information Security (QIS).
38.	**Wanneer wordt BBN3 verder uitgewerkt?**	BBN3 wordt op dit moment verder uitgewerkt en zal in 2018 worden opgeleverd.
39.	**Vervangt de BBN-indeling het uitvoeren van een risicoanalyse?**	Nee, het maakt alleen het proces eenvoudiger door al met voorgedefinieerde niveaus te komen. Daarbinnen moet op grond van een risicoafweging worden bepaald welke maatregelen per control moeten worden genomen om deze af te dekken.
40.	**Hoe verloopt de communicatie tussen informatie-systemen met verschillende BBN's? Kan een BBN2-informatiesysteem bijvoorbeeld met een BBN3-informatiesysteem communiceren?**	Informatie-uitwisseling tussen verschillende BBN's kan plaatsvinden na uitvoering van een risicoanalyse en het treffen van aanvullende maatregelen om te waarborgen dat het lagere systeem het hogere systeem niet kan besmetten.
41.	**Waarom zijn de betrouwbaarheids-aspecten Beschikbaarheid en Integriteit alleen op "Laag" en "Midden" te bepalen en niet op "Hoog"?**	Deze niveaus zijn gebaseerd op de geldende niveaus die door de grote interne dienstenleveranciers worden gehanteerd.
42.	**Waarom wordt in de BBN-toets gevraagd of weerbaarheid tegen APT's van statelijke actoren en/of criminele organisaties gewenst is? Dat heb je toch altijd nodig?**	In een ideale situatie zouden alle informatiesystemen altijd weerbaar zijn tegen APT's. De maatregelen die hiervoor getroffen moeten worden zijn echter relatief kostbaar en hebben soms een grote impact op bijvoorbeeld het gebruiksgemak. Het is daarom van belang om een risicoafweging te maken, waarbij de mogelijke schade van een aanval wordt meegewogen. Dit heeft geleid tot de huidige indeling in drie BBN's.

Controls

Nr	Vraag	Antwoord
43.	**Waarom is er geen onderscheid tussen systeemspecifieke controls en organisatiebrede controls?**	Dit onderscheid wordt gemaakt door de toewijzing van de controls aan de rollen SG (organisatiebreed), proceseigenaar (specifiek) en dienstenleverancier (specifiek). Als blijkt dat er behoefte is aan een dergelijke nadere uitsplitsing, dan zal hier een handreiking voor opgesteld worden.
44.	**Waarom zijn sommige control-teksten zo out-of-date (bijvoorbeeld telewerken)?**	Bij het opstellen van de BIR2017 is de meest recente Nederlandstalige versie van ISO 27002 gehanteerd (2015). Zodra er een nieuwe versie van de ISO beschikbaar is zal de BIR daarop worden aangepast.
45.	**Hoe weet ik of een control helemaal is afgedekt?**	De eigenaar van een informatiesysteem bepaalt op basis van een risicoafweging welke maatregelen per control moeten worden genomen om deze af te dekken. De implementatierichtlijnen uit de ISO27002 kunnen daarbij als inspiratiebron worden gebruikt. De verzameling te nemen maatregelen per control omvat in ieder geval de bij die control behorende rijksmaatregelen.
46.	**Wat moet ik doen als een control niet van toepassing is?**	Als een control voor een specifiek geval niet van toepassing kan zijn, vervalt de verplichting. Dit geldt bijvoorbeeld bij een control die betrekking heeft op een externe koppeling, terwijl het betreffende systeem geen externe koppeling heeft.

Rijksmaatregelen

Nr	Vraag	Antwoord
47.	**Als ik alle rijksmaatregelen heb geïmplementeerd, ben ik dan klaar?**	Nee, na bepaling van het gewenste BBN moet op basis van een risicoafweging worden bepaald welke maatregelen noodzakelijk zijn in aanvulling op de bij dat BBN-behorende rijksmaatregelen.
48.	**Wat moet ik doen als bij een control geen rijksmaatregelen staan?**	De eigenaar van een informatiesysteem of proces bepaalt op basis van een risicoafweging welke maatregelen per control moeten worden genomen om deze af te dekken. De implementatierichtlijnen uit de ISO27002 kunnen daarbij als inspiratiebron worden gebruikt.
49.	**Dekken de rijksmaatregelen de hele control af?**	Nee, de eigenaar van een informatiesysteem bepaalt op basis van een risicoafweging welke maatregelen per control moeten worden genomen om deze af te dekken. De implementatierichtlijnen uit de ISO27002 kunnen daarbij als inspiratiebron worden gebruikt. De verzameling te nemen maatregelen per control omvat in ieder geval de bij die control behorende rijksmaatregelen.
50.	**Moet ik voor BBN2 ook de rijksmaatregelen uit BBN1 implementeren?**	Ja.
51.	**Waarom zijn sommige rijksmaatregelen zo gedetailleerd uitgewerkt?**	De rijksmaatregelen zijn zo concreet mogelijk uitgewerkt om interpretatieverschillen te voorkomen.
52.	**Kun je aangeven welke rijksmaatregelen bij welke wetgeving horen?**	Waar van toepassing zijn in de rijksmaatregelen verwijzingen gemaakt naar wet- en regelgeving.
53.	**Wat moet ik doen als een rijksmaatregel niet van toepassing is?**	Als een maatregel voor een specifiek geval niet van toepassing kan zijn, vervalt de verplichting. Dit geldt bijvoorbeeld bij een maatregel die betrekking heeft op een externe koppeling, terwijl het betreffende systeem geen externe koppeling heeft.
54.	**Kan ik voorstellen indienen voor verbetering van bestaande of introductie van nieuwe rijksmaatregelen?**	Ja, via het evaluatie- en bijstellingsproces zoals beschreven in de BIR.
55.	**Hoe wordt omgegaan met verouderde rijksmaatregelen?**	Via het evaluatie- en bijstellingsproces zoals beschreven in de BIR worden deze aangepast.

Handreikingen

Nr	Vraag	Antwoord
56.	**Waarom zijn niet overal handreikingen opgenomen?**	Niet overal zijn handreikingen van toepassing of beschikbaar.
57.	**Moet ik alle handreikingen verplicht implementeren?**	Nee, de handreikingen dienen ter inspiratie.
58.	**Kan ik nieuwe handreikingen aanleveren voor opname in de BIR?**	Ja, via het evaluatie- en bijstellingsproces zoals beschreven in de BIR.
59.	**Waar moet een nieuwe handreiking aan voldoen?**	Er zijn geen vastomlijnde criteria voor. Voorstellen worden behandeld via het evaluatie- en bijstellingsproces zoals beschreven in de BIR.

Rollen

Nr	Vraag	Antwoord
60.	**Hoe moet ik omgaan met de controls en rijksmaatregelen die door de SG moeten worden uitgevoerd?**	De SG is eindverantwoordelijk (responsible) voor die maatregelen, maar bepaald moet worden welke functionaris binnen het departement accountable is. Dit kan bijvoorbeeld de BVA, CISO of de Directeur Inkoop zijn. Er zal nog een handreiking worden opgesteld waarin dit verder wordt uitgewerkt (RACI-tabel).
61.	**Waarom ontbreken rollen zoals de medewerker, de CIO en de CISO?**	De BIR onderscheidt drie (hoofd)rollen: de SG, de proceseigenaar en de dienstenleverancier. Er zijn uiteraard meer rollen betrokken bij informatiebeveiliging, zoals toezichthouder en medewerker, maar het gaat hier om de verantwoordelijke voor de uitvoering van de control.
62.	**Waarom is de rol van toezichthouder niet opgenomen?**	De BIR kan niet de rol van de toezichthouder regelen.
63.	**Waarom is er geen onderscheid tussen interne en externe dienstleveranciers?**	Interne en externe leveranciers leveren producten en diensten die aan dezelfde betrouwbaarheidseisen moeten voldoen.
64.	**Welke interne dienstenleveranciers kennen we?**	Bijvoorbeeld SSC-ICT, DICTU, RGD, RBO en P-Direkt.
65.	**Hoe moet ik de BIR2017 aan externe dienstenleveranciers voorleggen?**	Bij offertestelling verzoekt de eigenaar van een informatiesysteem aan potentiële leveranciers om in hun aanbieding aan te geven hoe zij de vereiste controls / maatregelen invullen als onderdeel van hun dienstverlening.
66.	**Wat moet ik doen bij bestaande contracten die nog niet op de BIR2017 zijn afgesloten?**	Bij vernieuwing van contracten geldt de situatie zoals geldig bij offertestelling. Als vernieuwing niet aan de orde is, zal de opdrachtgever in overleg met de leverancier bepalen welke aanvullende maatregelen gewenst zijn. Als om wat voor reden dan ook bestaande contracten niet aangepast (kunnen) worden, bepaalt de opdrachtgever welke compenserende maatregelen getroffen moeten worden of dat een explain ingediend moet worden.
67.	**Wat moet de medewerker doen met de BIR-maatregelen?**	Het is aan de SG, proceseigenaar of dienstenleverancier om de medewerkers te instrueren ten aanzien van werkzaamheden die voortkomen uit de toepassing van BIR-maatregelen.
68.	**Waarom staan er soms meerdere rollen bij een control genoemd?**	In een aantal situaties zijn de maatregelen om een control in te vullen verdeeld over meerdere rollen. Vaak gaat het hier om een deel dat beleidsmatig is en een deel dat de uitvoering betreft. Ook zijn ministeries veelal pluriform georganiseerd.
69.	**Houdt de BIR 2017 er rekening mee dat veel organisaties hun ICT-dienstverlening geheel of gedeeltelijk hebben uitbesteed?**	Ja, de BIR geeft expliciet aan welke maatregelen voor de dienstenleverancier zijn. De BIR maakt daarbij geen onderscheid tussen interne en externe diensten-leveranciers.
70.	**Als mijn leverancier een ISO27001-certificering heeft, is dat dan ook goed?**	Het is mogelijk dat een (externe) diensten-leverancier beschikt over een ISO27001-certificering, ISAE3402-certificering of een ander kwaliteitskeurmerk. Een dergelijk keurmerk geeft een waarborg over het proces dat bij de dienstenleverancier is ingericht, maar geeft niet aan op welk niveau de beveiliging is gerealiseerd. Hoewel dit dus wel meerwaarde heeft, overlap kent met de BIR-controls en gebruikt kan worden als onderdeel van de Statement of Compliancy, omvat en vervangt het niet volledig de verantwoording over de rijksmaatregelen uit de BIR. Er zullen altijd aanvullende afspraken gemaakt moeten worden en hierover moet aanvullend worden verantwoord.

Verantwoording

Nr	Vraag	Antwoord
71.	**Wat is een Statement of Compliancy?**	Dat is een document waarin een externe dienstenleverancier aan zijn opdrachtgever(s) verklaart in control te zijn over de uitvoering van de overeengekomen beveiligings-maatregelen met betrekking tot de geleverde diensten. In het geval een interne dienstenleverancier is dit de deel-ICV.
72.	**Wat moet ik doen als ik niet aan een control c.q. maatregel kan/wil voldoen?**	Het niet invullen van een control moet intern kunnen worden toegelicht. Alleen voor het niet of anders toepassen van een rijksmaatregel moet een explain worden gemaakt. De explains worden in het ISMS van het departement geregistreerd en kunnen onderwerp van onderzoek door de AR of ADR zijn.
73.	**Moet ik een explain indienen als ik ergens niet aan voldoe?**	Als het niet of anders toepassen van een rijksmaatregel een departement overstijgend effect heeft, moet de explain worden voorgelegd aan de Security Accreditation Authority.
74.	**Moet ik over alle controls en rijksmaatregelen een verantwoording afleggen?**	Ja, in alle gevallen moet verantwoording afgelegd kunnen worden, zodanig dat de ADR er de juiste werking/toepassing uit kan afleiden.
75.	**Is de huidige comply or explain afspraak ook van toepassing op BBN1?**	De comply or explain afspraak is van toepassing op de rijksmaatregelen van alle BBN's.
76.	**Hoe gaan auditors met de nieuwe BIR om?**	Deze BIR noodzaakt tot een ander gesprek met de auditor. Het is de lijnmanager die bepaalt d.m.v. risicomanagement hoe de controls worden ingevuld door welke maatregelen. Alleen deze maatregelen kunnen in het kader van de BIR door de auditor getoetst worden. Voor de transitieperiode is in het transitieplan aandacht gegeven hoe met de oude en de nieuwe BIR wordt omgegaan.
77.	**Welk toetskader hanteren de auditors bij vraaggestuurde onderzoeken naar de BIR tijdens de transitieperiode?**	In de transitieperiode wordt in overleg met de eigenaar van het informatiesysteem bepaald welk toetskader (BIR:2012 dan wel de BIR2017) zal worden gehanteerd.
78.	**In de BIR staat niet duidelijk aangegeven hoe de verantwoording over de BIR in de toekomst er uit gaat zien?**	Verantwoording over de BIR is onderdeel van het proces van verantwoording over informatiebeveiliging. Momenteel vind dat plaats d.m.v. het ICV-proces en de jaarrapportage bedrijfsvoering.
79.	**Moet ik ook explains indienen als een rijksmaatregel niet van toepassing is?**	Nee. Als een maatregel voor een specifiek geval niet van toepassing kan zijn, vervalt de verplichting. Dit geldt bijvoorbeeld bij een maatregel die betrekking heeft op een externe koppeling, terwijl het betreffende systeem geen externe koppeling heeft.
80.	**Wanneer voldoet een organisatie aan de BIR**	Met "voldoen aan" of "compliant zijn met" de BIR 2017 wordt bedoeld dat de eigenaar van het informatiesysteem het BBN heeft bepaald, eventueel noodzakelijke aanvullende maatregelen heeft bepaald en alle bij het BBN behorende rijksmaatregelen en aanvullende maatregelen heeft geïmplementeerd danwel, ingeval van outsourcing, heeft toegezien op juiste implementatie.

Transitie BIR2012-BIR 2017

Nr	Vraag	Antwoord
81.	**Wat is de transitieperiode?**	Voor de invoering van de BIR2017 geldt een globale tijdlijn. De ministeries stellen zelf in lijn daarmee detailplanningen op, waarmee ze de invoering van de BIR2017 inpassen in hun eigen pdca-planning. Zie voor verdere details het transitieplan.
82.	**Wanneer moet ik voldoen aan de BIR2017?**	Voor de invoering van de BIR2017 geldt een globale tijdlijn. De ministeries stellen zelf in lijn daarmee detailplanningen op, waarmee ze de invoering van de BIR2017 inpassen in hun eigen pdca-planning. Voor nieuwe informatiesystemen waarvoor de functionele en technische eisen nog niet zijn vastgesteld, geldt dat de BIR2017 per 1-1-2018 van kracht is; Voor de bestaande informatiesystemen geldt dat: elk ministerie in 2018 start met het implementeren van de BIR2017; elk ministerie, zo spoedig mogelijk, doch uiterlijk per 1-1-2019 inzichtelijk heeft gemaakt wanneer ze voor welke informatiesystemen overstappen op de BIR2017; Verdere details zijn opgenomen in het transitieplan.
83.	**Als ik nu voldoe aan BIR2012 wat moet ik dan extra doen om aan BIR2017 te voldoen?**	In de Is/was-lijst staat aangegeven welke controls en maatregelen nieuw of aangepast zijn t.o.v. de BIR2012.
84.	**Is er ondersteunende tooling beschikbaar voor overgang van BIR2012 naar BIR2017?**	Ter ondersteuning van de implementatie van de BIR2017 is een aantal hulpmiddelen beschikbaar: • een Excel sheet met alle controls en rijksmaatregelen uit de BIR2017. De Excel sheet maakt het mogelijk controls en rijksmaatregelen te filteren op rol, BBN etc.; • een Is/was–lijst. Deze lijst maakt duidelijk welke feitelijke veranderingen zijn doorgevoerd ten opzichte van de BIR:2012. De Is/was–lijst is opgenomen in de hierboven genoemde Excel sheet; • veel gestelde vragen (FAQ's). Gedurende het ontwikkelproces van de BIR2017 zijn vragen verzameld. Deze vragen worden beantwoord in een document met veel gestelde vragen. Dit document wordt ook op Rijksportaal gepubliceerd om het mogelijk te maken zo nodig eenvoudig en snel wijzigingen en aanvullingen te doen; • verwijzingen naar relevante handreikingen. Deze helpen bij de uitwerking van de controls en rijksmaatregelen. De verwijzingen zijn als hyperlinks opgenomen in de wordversie van de BIR2017 en in de Excel sheet met alle controls en rijksmaatregelen. Naast de producten die ondersteunen bij de implementatie van de BIR2017, is tijdens de uitvoeringstoetsen gebleken dat er behoefte is aan enkele producten die ondersteunen bij het gebruik van de BIR2017, zoals een herziene Quickscan en een RACI-tabel. Deze worden z.s.m. opgeleverd.

Baseline Informatiebeveiliging Overheid (BIO)

Nr	Vraag	Antwoord
85.	**Wat is de relatie tussen de BIR en de BIO?**	In overheidsbreed verband wordt gewerkt aan de ontwikkeling van een Baseline Informatiebeveiliging Overheden (BIO). De BIR2017 wordt als basis gehanteerd voor de BIO.
86.	**Verdwijnt de BIR als de BIO uit komt?**	Uiteindelijk zal de BIR volledig onderdeel worden van het BIO-stelsel. Er zal dan een deel zijn dat ook voor alle andere overheden van toepassing is en een deel dat rijksspecifiek blijft, gezien specifieke rijksregelgeving.

Dit is een uitgave van:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Turfmarkt 147
2511 DP Den Haag

Januari 2018 | 110023