Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

Datum
16 oktober 2017

memo

Transitieplan BIR2017

Van BIR:2012 naar BIR2017

Na de vaststelling van de BIR2017 volgt de toepassing daarvan in de praktijk. Het is aan de ministeries zelf om te bepalen op welke wijze de overgang van de BIR:2012 naar de BIR2017 optimaal kan verlopen. Dit document dient ter ondersteuning van de gewenste verandering. Het gaat in op de volgende punten:

- een globaal tijdpad voor de implementatie;
- ondersteunende middelen bij de implementatie.

Dit transitieplan is bedoeld voor degene(n) die belast is (zijn) met de invoering van de BIR2017. In veel gevallen zal dit de Chief Information Officer (CIO) dan wel de Chief Information Security Officer (CISO) van de betreffende organisatie zijn.

Bij de ontwikkeling van de BIR2017 is doorgebouwd op de lijn van de BIR:2012. 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 R-maatregelen zijn opgeschoond;
- De ISO controls worden in de BIR2017 ongewijzigd gehanteerd. Waar de BIR:2012 diverse interpretaties van de ISO27002 tekst bevat, wordt in de BIR2017 alleen verwezen naar de oorspronkelijke ISO tekst, aangevuld met specifiek voor de Rijksdienst geldende (R-)maatregelen. Het voordeel van deze benadering is dat de afstemming met leveranciers daardoor vereenvoudigd wordt;
- De R-maatregelen zijn gesaneerd. R-maatregelen die zijn overgebleven komen voort uit:
    - IB-aspecten uit specifieke wet- en regelgeving;
    - gemeenschappelijk eisen t.a.v. veiligheid van informatieketens;
    - fundamentele eisen die aan een betrouwbare c.q. professionele informatievoorziening moeten worden gesteld.

- BBN 2 komt op hoofdlijnen overeen met het beschermingsniveau van de BIR:2012. Met de toevoeging van BBN3 biedt de BIR2017 straks de mogelijkheid om hogere dreigingsniveaus (bijvoorbeeld van statelijke actoren) te kunnen pareren.

Wat er precies in de BIR2017 ten opzichte van de BIR:2012 is veranderd, is weergegeven in de zogenaamde transitietabel. Deze is onderdeel van een Excel sheet waarin ook alle controls en maatregelen zijn opgenomen.

Globaal tijdpad implementatie

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:

1. de BIR2017 per 1-1-2018 van kracht is;
2. over 2018 de eventuele vraaggestuurde ADR-onderzoeken en het ICV proces op het gebied van informatiebeveiliging de BIR2017 als uitgangspunt zullen hebben.

Voor de bestaande informatiesystemen geldt dat:

1. elk ministerie in 2018 start met het implementeren van de BIR2017;
2. elk ministerie, zo spoedig mogelijk, doch uiterlijk per 1-1-2019 inzichtelijk heeft gemaakt wanneer ze voor welke informatiesystemen overstappen op de BIR2017;
3. elk ministerie bij het opstellen van deze planning zelf rekening moet houden met het op tijd alloceren van capaciteit en budget voor 2018 en verder, ten behoeve van het uitvoeren van de benodigde acties;
4. in de overgangsfase, bij eventuele vraaggestuurde ADR-onderzoeken op het gebied van informatiebeveiliging, in overleg met de eigenaar van het informatiesysteem wordt bepaald of door de ADR de BIR:2012 dan wel de BIR2017 als uitgangspunt wordt gehanteerd. Voor het ICV-proces in de overgangsfase zullen nog nadere afspraken gemaakt worden.

Over 2017 zullen de eventuele vraaggestuurde ADR-onderzoeken en het ICV proces op gebied van informatiebeveiliging de BIR:2012 nog als uitgangspunt hebben.

Voor systemen in de categorie BBN3 geldt vooralsnog het VIR-BI in combinatie met BBN2. Met de exacte bepaling van de toepasselijke NAVO *enclosures* en *directives* zal ook de transitie naar BBN3 worden bepaald. Naar verwachting zal dit einde van 2017 klaar zijn om via het onderhoudsproces aan de BIR2017 toegevoegd te worden.

Ondersteunende middelen

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. Deze producten worden nog dit jaar opgeleverd:

- een aangepaste Quickscan BIR voor het uitvoeren van globale risicoanalyses (met de BBN-toets hierin geïncorporeerd);
- een handreiking met daarin een RACI-tabel voor de verdere uitwerking van de rollen die in de BIR20127 worden onderkend.

In de BIR2017 zijn al enkele handreikingen opgenomen rondom het uitvoeren van risicomanagement. Naar aanleiding van de discussie in de Subcommissie Informatiebeveiliging (SIB) over het vereiste niveau van volwassenheid ten aanzien van risicomanagement, zal in overleg met de community bepaald worden op welke wijze, aanvullend op de genoemde handreikingen en de Quickscan BIR, de benodigde ondersteuning geboden kan worden op dit gebied.

De ervaringen die worden opgedaan bij de implementatie en toepassing van de BIR2017 kunnen leiden tot nieuwe inzichten ten aanzien van de te stellen eisen op het gebied van de rijksmaatregelen. Deze nieuwe inzichten kunnen leiden tot aanpassingsvoorstellen voor de BIR die worden meegenomen in het reguliere evaluatie- en bijstellingsproces van de BIR zoals in de BIR staat beschreven.