BIR comply or explainprocedure

Datum: 7 januari 2014
Versie: 1.0

Inleiding

In 2012 is de Baseline Informatiebeveiliging Rijksdienst (BIR) van kracht geworden. De Baseline gaat uit van een “comply or explain-regiem”. Deze nota bevat een voorstel voor de explainprocedure voor de BIR. De nota omvat zowel de explainprocedure voor de departementen (specifieke voorzieningen) als de explainprocedure voor Shared Service Organisaties (generieke of gemeenschappelijke voorzieningen).

Behandeling van explains

Voor de BIR geldt: comply or explain

In de BIR is het volgende beschreven inzake de explains (hoofdstuk 2.1):

> **Vertrouwen in toetsing**
> Als ministeries hun informatievoorziening en IT inrichten volgens de BIR:2012 (in opzet, bestaan en werking) dan moet dat voldoende garantie bieden dat ministeries hun eigen informatie en die van andere ministeries veilig (beschikbaar, integer en vertrouwelijk) behandelen. Ministeries moeten elkaar hierop kunnen aanspreken. Bij de implementatie geldt voor de tactische normen en eisen een comply or explain regime. Het toetsen vindt plaats aan de hand van de in-control verklaring. De in-control verklaring moet dus inzicht geven aan welke BIR:2012 normen wordt voldaan en voor welke BIR:2012 normen een explain is gedefinieerd. Er wordt, buiten het kader van BIR, bij de Rijksdienst een accreditatieproces ontwikkeld waarin departementen elkaar kunnen aanspreken op explains die de vertrouwelijkheid van berichtenverkeer over meerdere ministeries heen nadelig beïnvloeden.

Wat is een explain?

Een explain is een door de verantwoordelijke lijnmanager[1] geaccepteerde verklaring waarom aan bepaalde normen uit de BIR niet wordt voldaan.

Wat betekent “voldoen aan BIR normen”?

In de BIR (hoofdstuk 2.3: controleerbaarheid en auditeerbaarheid) staat beschreven dat voldaan moet worden aan ISO27002/bijlage A + de R-normen. Dit is leidend om te voldoen aan de BIR normen.
De BIR bevat de hoofdstukindeling en de normen uit ISO27001/bijlage A. Alle 1, 2 en 3-cijferige hoofdstukjes zijn direct uit ISO27001/bijlage A overgenomen. Hieraan moet, samen met de R-normen dus verplicht worden voldaan.

[1] Verantwoordelijke lijnmanager: dit is de lijnmanager die door de SG, die volgens het VIR verantwoordelijk is, is gemandateerd. Hij heeft het niveau van directeur of DG,.

Daarnaast bevat de BIR normen met een 4 cijferige nummering die niet met een R zijn gemerkt. Dat zijn suggesties voor een goede invulling van de BIR, afgeleid van de implementatierichtlijnen uit ISO 27002. Die normen zijn niet verplicht maar wel een handige handreiking.

Waarvoor moet een explain worden opgesteld?

Een explain moet worden opgesteld voor elk restrisico of niet ingevulde BIR maatregel (zie BIR hoofdstuk 4, figuur 3):

1. Een BIR norm die voor de betreffende situatie (organisatie, systeem) wel van toepassing is maar waar niet aan voldaan wordt
2. Een BIR norm die volgens de eigenaar van een systeem voor de betreffende situatie niet van toepassing is
3. Overige bij een risicoanalyse gesignaleerde restrisico's.

De BIR-toets en het risicoafwegingsproces (zoals voorgeschreven door het VIR:2007 en in hoofdstuk 2, figuur 3 van de BIR) moet plaatsvinden voor informatieverwerkende systeemen. En informatieverwerkend systeem bestaat niet alleen uit techniek maar ook uit de betrokken fysieke omgeving, organisatie en mensen.

Een explain-verklaring bevat:

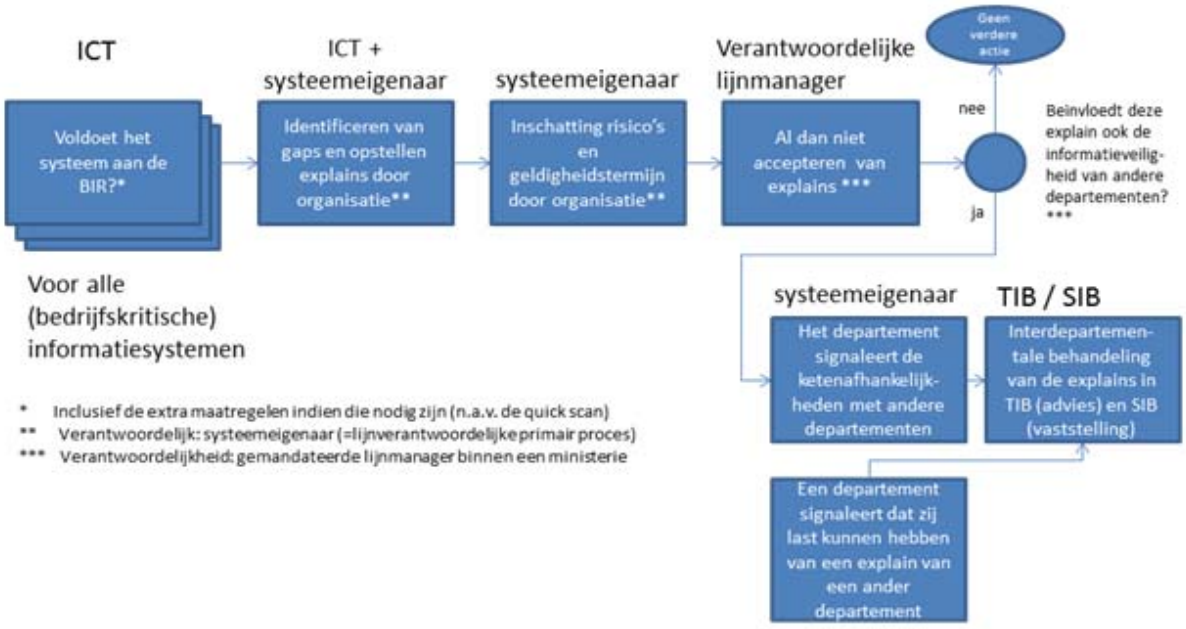
- De BIR norm of aanvullende noodzakelijk geachte maatregel waaraan niet wordt voldaan. Voldoende begrijpelijk geformuleerd en reden waarom nog niet kan worden voldaan.
- Risico van de explain
    - Voor de eigen organisatie
    - Voor andere organisaties (+ verklaring welke organisaties)
- Reden van acceptatie van de explain.
- Geldigheid (duurzaam of tijdelijk met vermelding van einddatum)
- Verantwoordelijke organisatie, actiehouder (=contactpersoon) en lijnmanager
- Refentienummer en datum van de explain
- Status (kan tussentijds worden bijgehouden)

Moeten alle systemen aantoonbaar BIR compliant zijn?

VIR spreekt over "de systemen" in een organisatie. Dit kunnen voor de hele rijksoverheid duizenden systemen zijn.

Het is dus praktisch om een prioriteit te stellen bij de "bedrijfskritische" systemen. Dat wil zeggen bij systemen die bij falen de tijdigheid en kwaliteit van het product of de dienst van een organisatie in gevaar brengen.

De organisatie moet alle systemen uiteraard wel in kaart hebben gebracht en moet dit ook inzichtelijk kunnen maken voor interne of externe audits.



Explainprocedure voor departementen

Bij de specifieke systemen, van een departement legt de systeemeigenaar (=lijnfunctionaris) de explain voor aan het verantwoordelijke lijnmanagement (directeur of DG). De verantwoordelijke lijnmanager bepaalt of een explain al dan niet wordt geaccepteerd. Ook bepaalt hij of de explain consequenties kan hebben voor andere ministeries of ketenpartners.

In dit proces wordt de verantwoordelijke lijnmanager geadviseerd door de CIO. De CIO monitort ook de compleetheid van de explains en de voortgang m.b.t. de oplossing van de explains.

Als een explain gevolgen kan hebben voor een ander ministerie legt de lijnmanager de explain voor aan de TIB (expertgroep Tactische InformatieBeveiliging) van TBGI.

Toetsing door de TIB

Inhoudelijk wordt de explain op de volgende wijze getoetst door de TIB:

- Is een 'niet van toepassing' onderbouwd en correct?
- Is de explain inhoudelijk goed (/ voldoende)?
- Zijn van de explain de restrisico's duidelijk, en is de tijdsduur bepaald (met verbeterplanning)?
- Zijn er risico's van een explain die invloed of potentieel invloed op andere departementen hebben?
- Is de verwachting van de indiener dat een explain binnen een half jaar verandert in een comply? In dit geval wordt de explain beschouwd als een comply.

De TIB adviseert aan de SIB om explains goed of af te keuren en meldt dit terug aan de indiener. Indien er een explain is ingediend waarbij er risico's voor andere departementen bestaan (ketenafhankelijkheid) dan zal dit advies, onderbouwd door TIB, de volgende besluitvorming kennen:

- Het TIB adviseert de opdrachtgever (en rapporteert deze aan de SIB.)
- De explain wordt, samen met het advies van de TIB, aan de SIB, in haar rol als Security Accreditation Authority, voorgelegd ter afweging, risico acceptatie en besluitvorming.
- Besluiten van het SIB worden als hamerstuk geagendeerd bij de ICCIO en (afhankelijk van de impact) ter kennisneming naar de ICBR gezonden.

Explainprocedure voor SSO's

Bij een SSO kan sprake zijn van dienstverlening door middel van een generiek of een gemeenschappelijk systeem. Voor generieke systemen is een explainprocedure vastgesteld in het ICCIO van augustus 2012, waarbij de expertgroep TIB is gemandateerd als 'Security Advisory Accreditation Panel'. In deze beschrijving wordt dat proces uitgebreid voor gemeenschappelijke systemen.

Het ICCIO besluit over welke systemen generiek zijn, en daarvan wordt een overzicht bijgehouden met de (gedelegeerd) opdrachtgevers. Dit overzicht dient te worden aangevuld met systemen die als 'gemeenschappelijk' zijn aangemerkt.

Afnemerskant

De gebruikersorganisaties zijn eindverantwoordelijk (Accountable) voor het risicomanagement van een gemeenschappelijke dienst. Deze verantwoordelijkheid ligt formeel bij de SG maar wordt vaak aan de pSG's of integraal managers gedelegeerd. De gebruikersorganisaties blijven eindverantwoordelijk en dienen inzichtelijk te maken hoe zij deze eindverantwoordelijkheid invulling geven.

Bij een gemeenschappelijke dienst is een opdrachtgevend orgaan, het opdrachtgeversberaad (OGB), verantwoordelijk voor het opstellen van een pakket van eisen en wensen, het inrichten van de vraagarticulatie en de functionele behoeftestelling richting de dienstverlener. De afnemers treden gezamenlijk op in het OGB. Eisen en kaders ten aanzien van de te leveren beveiliging op het gebied van ondermeer vertrouwelijkheid, integriteit, beschikbaarheid en toezicht maken hiervan onderdeel uit.

Met de opdrachtnemer (SSO) worden afspraken gemaakt over de wijze waarop deze inzicht verschaft hoe hij de uitvoering van deze eisen borgt binnen de organisatie.

Het feit dat een collectief verantwoordelijk is voor de opdrachtverstrekking kan voor onduidelijkheden zorgen.

Invoering van Wifi in het verzorgingsgebied van SSC-ICT heeft aangetoond, dat de opdrachtnemer baat heeft bij een éénduidige sturingslijn.

Daarom is het aan te bevelen als opdrachtgevende organen, zoals een OGB, voor gemeenschappelijke voorzieningen steeds één van de departementen mandateren als de opdrachtgever door die betreffende dienst, namens de gemeenschappelijke afnemers.

Daarmee zijn zowel de IB compliance verantwoordelijkheid als de opdrachtverstrekking éénduidig belegd.

Aanbiederskant

De dienstenleverancier, als uitvoerende partij, is verantwoordelijk voor het afgesproken resultaat en moet aan de opdrachtgever laten zien dat hij op dit punt *in control* is.

Tevens heeft de dienstenleverancier een belangrijke taak om te *signaleren* als er veiligheidsrisico's bestaan. Deze kunnen bijvoorbeeld ontstaan door integratie van diensten zowel binnen het eigen domein van een SSO als met de domeinen van collega dienstverleners.

De aanbieder zal inzichtelijk maken welke gemeenschappelijke diensten worden aangeboden.

Verantwoordelijkheden bij explains

Evenals bij een ministerie is, bij een SSO, het lijnmanagement verantwoordelijk voor BIR compliancy, risicoanalyses, de opstelling van explains en het al dan niet accepteren van de explains. De CIO adviseert het lijnmanagement daarbij.

Toezicht en monitoring

De CIO heeft een adviserende, controlerende en monitorende taak.

De BVA's van de departementen die gemeenschappelijke diensten afnemen zijn verantwoordelijk voor het toezicht (op afstand) op de integrale beveiliging binnen het eigen departement. Hieronder vallen ook de diensten die door het departement worden afgenomen.

Zo mogelijk wordt het toezicht bij een gemeenschappelijke dienst door de betrokken BVA's op een gecoördineerde wijze vorm gegeven.

Te volgen proces

Voorgesteld wordt om voor de IB compliancytoetsing (d.w.z. toetsing op BIR compliancy), voor de eenvoud, het proces te volgen dat voor generieke systemen gebruikelijk is:

De SSO zal van de generieke of gemeenschappelijke dienst aangeven waar deze wel aan de BIR voldoet (comply) of niet (explain, met één of meerdere restrisico's), of niet van toepassing is, met een toelichting.

De opdrachtgever van de SSO zal deze comply or explain voor elke dienst voorleggen aan de expertgroep Tactische InformatieBeveiliging (TIB) van het TBGI. De TIB behandelt de explains op de wijze zoals eerder in dit document is uiteengezet in het hoofdstuk “Toetsing door de TIB”.

Bijlage 1: Begrippen

Algemene uitgangspunten

Begrippen

Generieke dienst
Een generieke dienst is een dienst die door een SSO aan alle onderdelen van de rijksoverheid wordt geleverd.

Gemeenschappelijke dienst
Een gemeenschappelijke dienst is een dienst die door een SSO aan meerdere onderdelen van de rijksoverheid wordt geleverd.

Specifieke dienst dienst
Een departementale, ofwel specifieke, dienst is een dienst die aan of door één departement wordt geleverd.

SSO (Shared Service Organisatie)
Een SSO is een serviceorganisatie, in dit geval binnen de Rijksoverheid, die aan meerdere ministeries diensten verleent. Voorbeelden: SSC-ICT, P-direct, Logius.

Verantwoordelijkheden

Ministeriele verantwoordelijkheid:
Informatiebeveiliging, en daarmee de implementatie van de BIR, is een verantwoordelijkheid van het lijnmanagement van de ministeries, met als hoogste lijnmanager de SG (gebaseerd op VIR:2007 artikel 4).

Systeemverantwoordelijkheid en verantwoording
De minister van BZK is systeemverantwoordelijk voor de bedrijfsvoering van het Rijk, incl. ICT en de beveiliging daarvan zoals vastgelegd in het “coördinatiebesluit organisatie en bedrijfsvoering rijksdienst 2011” (20 januari 2011, STB 13864, ISSN 0920-2064). Dat wil zeggen dat de Minister van BZK jaarlijks publiceert over de organisatie van de bedrijfsvoering van de ministeries (art 5) en daartoe ook de informatie van de ministeries ontvangt (art 6).

Minister BZK (DGOBR) ondersteunt de ministeries bij de invoering en naleving van de BIR.

Verantwoordelijkheid voor generieke en gemeenschappelijke diensten
Op het eerste gezicht is de ministeriële verantwoordelijkheid strijdig met de systeemverantwoordelijkheid van BZK. Dit is niet het geval. Het hoofdstuk “explainprocedure voor SSO’s” van dit document gaat hierop in.

Verantwoordelijke Lijnmanager
Het lijnmanagement – van het primaire proces - is verantwoordelijk voor de kwaliteit van zijn eindproduct en daarmee ook voor de beveiliging van zijn informatiesystemen (conform VIR:2007, art 4). De verantwoordelijke lijnmanager heeft altijd het niveau van directeur of DG.

Systeemeigenaar

Elk systeem moet een eigenaar hebben. Aangezien het systeem de kwaliteit van het eindproduct van de organisatie betreft is de verantwoordelijke lijnmanager uiteindelijk de eigenaar van het systeem. Bij ketens, generieke diensten en gezamenlijke diensten wordt een partij gemandateerd om op te treden als eigenaar namens de verschillende betrokken lijnmanagers. De lijnmanagers houden dan wel toezicht op de goede uitvoering van het systeemeigenaarschap.

CIO en CISO

De CIO adviseert en ondersteunt het departement met kaders, concrete adviezen en houdt toezicht op de goede uitvoering van informatievoorziening binnen zijn departement. De CIO heeft tevens de rol van CISO (Chief Information Security Officer). In die rol ondersteunt hij de business op het gebied van informatiebeveiliging (adviezen en toezicht op goede uitvoering). Voor explains is een advies van de CIO daarom noodzakelijk.

BVA, RijksBVA en IBR

BVA's, IBR en RijksBVA houden toezicht. Zij monitoren of alle partijen hun rollen en verantwoordelijkheden t.a.v. beveiliging goed invullen. De RijksBVA houdt toezicht op de werking van het systeem van integrale beveiliging. Daarvoor krijgt/vraagt hij informatie van de departementale BVA's en van de CIO Rijk. De BVA's krijgen dit op hun beurt ook weer van de departementale CIO's. Dit systeem van BVA toezicht moet dus gevoed worden door informatie over BIR compliance uit het CIO/SIB/TIB domein.

Bijlage 2: Voorbeeld explainformulier

Dit formulier is een voorbeeld. Voor een zeer eenvoudige manier van elektronisch registreren en rapporteren kan de methode van MinVenJ als voorbeeld dienen, zie: http://ciso-venj.rijksweb.nl/index.html

Aanvrager

Algemene gegevens aanvrager.

Organisatie:	
Verantwoordelijke lijnmanager (directeur of DG):	
Contactpersoon:	
Datum:	

BIR-TNK Norm

De BIR norm uit het Tactisch Normen Kader (TNK) waar de 'Explain' op van toepassing is.

BIR Norm:	
Eventueel geconstateerd restrisico n.a.v. risicoanalyse	

Proces / Informatiesysteem:

Proces en informatiesysteem waar de Explain op van toepassing is.

Informatiesysteem:	
Doel informatiesysteem:	

Afwijking

Beschrijving van de afwijking, toelichting, risico's van het niet voldoen aan de BIR-norm, mitigerende maatregelen en duur van de afwijking.

Beschrijving:	
Reden/toelichting:	
Risico's:	
Oplossing / Mitigerende maatregel(en):	
Hoe lang blijft afwijking bestaan?	0 – Duurzaam 0 – Tijdelijk tot [datum]
Interdepartementale effecten:	0 – Niet aanwezig 0 – Wel aanwezig, namelijk ….

Advies CIO

Advies (goedkeuring *Explain*, Akkoord J/N)	
Geldigheidsduur:	0 – Duurzaam 0 – Tot [datum]

Datum:	
Toelichting:	-

Besluit Verantwoordelijke lijnmanager

Besluit van de verantwoordelijke lijnmanager.

In de praktijk kan dit een geaggregeerde goedkeuring zijn voor een bundeltje explains)

Overname Advies:	
Geldigheidsduur:	
Toelichting:	-
Handtekening + datum	

Advies TIB

Advies (voorzitter) TIB.

Advies:	
Geldigheidsduur:	
Datum:	

Toelichting:	-

Besluit voorzitter SIB

Besluit voorzitter SIB.

In de praktijk kan dit een geaggregeerde goedkeuring zijn voor een bundeltje explains)

Besluit	
Geldigheidsduur:	
Datum:	
Toelichting:	-