Auditdienst Rijk
Ministerie van Financiën

> Retouradres Postbus 20201 2500 EE Den Haag

Ministerie van Binnenlandse Zaken en Koninkrijkrelaties
SSC-ICT HAAGLANDEN
10,2 e [redacted]
Koningskade 4
2596 AA DEN HAAG

Auditdienst Rijk
Turfmarkt 147
2511 DP Den Haag
Postbus 20201
2500 EE Den Haag
www.rijksoverheid.nl
Inlichtingen 10,2 e [redacted]

Ons kenmerk
ADR/2015/240 U
Uw brief (kenmerk)

Datum 17 februari 2015
Betreft Assurance rapport

10,2 e [redacted]

Hierbij doe ik u het Assurance Rapport van de IT-auditor van de Auditdienst Rijk toekomen over de implementatie van de BIR-maatregelen in het systeem Rijksconnect, die gekoppeld zijn aan de NOREA beheerprocessen: Generieke beheerproces, Capacity management en Change management zoals door u gevraagd in uw opdracht d.d. 09-10-2014.

Hoogachtend,

10,2 e [redacted]

Directeur Auditdienst Rijk

Auditdienst Rijk
Ministerie van Financiën

Assurance rapport van de Auditdienst Rijk: Generiek, Capacity management en Change management in het systeem Rijksconnect

Kenmerk	ADR/2015/240
Datum	17 februari 2015
Status	Definitief

Colofon

Titel	Assurance rapport van de Auditdienst Rijk: Generiek, Capacity management en Change management in het systeem Rijksconnect
Bijlagen	2
Inlichtingen	**Auditdienst Rijk** 070-3427700

Inhoud

1 Opdrachtomschrijving

Het onderzoek heeft zich gericht op het aantonen van de *BIR maatregelen (in opzet en bestaan),* die gekoppeld zijn aan de volgende beheerprocessen voor het systeem Rijksconnect:

- de generieke beheersprocessen;
- capacity management en;
- change management.

Voor de bovengenoemde beheerprocessen geldt dat deze staan beschreven in het studierapport 'Normen voor de beheersing van uitbestede ICT beheerprocessen' van NOREA. Bijlage 1 bevat een overzicht van de gecontroleerde BIR maatregelen.
Op basis van het bovenstaande zijn voor de assuranceverklaring de volgende onderzoeksvragen beantwoord:

a. Zijn de maatregelen die conform de BIR gekoppeld zijn aan de generieke beheersprocessen, capacity management en change management conform het NOREA normenkader voor uitbestede ICT beheerprocessen, *in opzet (lees formeel)* beschreven voor het systeem Rijksconnect *en voldoen* de beschreven maatregelen aan de normen die de BIR stelt aan deze maatregelen ;
b. Zijn de maatregelen, die confrom de BIR gekoppeld zijn aan de generieke beheersprocessen, capacity management en change management, *in bestaan (lees in de praktijk) bij het technisch beheer van* het systeem van Rijksconnnect1 aangetroffen *en voldoen de* aangetroffen maatregelen aan de normen die de BIR stelt aan deze maatregelen .

Bijlage 1 van deze verklaring bevat een overzicht van de getoetste BIR maatregelen, deze zijn als bijlage bij het plan van aanpak voorgelegd en afgestemd met alle betrokkenen.

1 Hierbij wordt met het systeem Rijksconnect bedoeld, het geheel van activiteiten, processen, maatregelen en techniek.

2 Verantwoordelijkheden

De verdeling van de verantwoordelijkheden is bij deze audit als volgt:

- Logius: is gemandateerd systeemeigenaar van Rijksconnect en ontvanger van de assuranceverklaring over Rijksconnect;
- SSC-ICT: is de technisch beheerder van Rijksconnect en opdrachtgever van de IT-audit inzake Rijksconnect, die de assuranceverklaring moet opleveren;
- ADR: is uitvoerder van de IT audit inzake Rijksconnect.

3 Verantwoordelijkheden van de IT-auditor

Het is onze verantwoordelijkheid om, op basis van onze werkzaamheden, een oordeel met een redelijke mate van zekerheid te geven over de aanwezigheid van de BIR maatregelen behorend tot de in punt 1 genoemde beheerprocessen van Rijksconnect, zoals opgenomen in het overzicht van bijlage 1.
We hebben onze opdracht uitgevoerd volgens Richtlijn 3000 "Richtlijn Assurance-opdrachten door IT-auditors" vastgesteld door Nederlandse Orde van Register EDP-auditors (NOREA). Dit vereist dat wij voldoen aan de voor ons geldende ethische voorschriften en onze werkzaamheden zodanig plannen en uitvoeren dat een redelijke mate van zekerheid wordt verkregen over de vraag of, in alle van materieel belang zijnde aspecten, de beschrijving getrouw is weergegeven en of de interne beheersmaatregelen op afdoende wijze zijn opgezet en in de periode van 15 december tot en met 19 december 2014 is vastgesteld dat deze maatregelen toen aantoonbaar aanwezig waren danwel hebben gewerkt.
Onze werkzaamheden hebben bestaan uit het uitvoeren van een documentanalyses, het houden van interviews en het uitvoeren van waarnemingen (testen van de opzet en het bestaan van de BIR-maatregelen) die wij noodzakelijk achten bij het verschaffen van een oordeel met een redelijke mate van zekerheid dat de opzet en het bestaan van de BIR maatregelen, die in het overzicht staan vermeld, kon worden aangetoond.
In dit onderzoek hebben wij voor een groot deel gebruik gemaakt van het rijksbrede BIR onderzoek dat in opdracht van BZK DGOBR bij SSC-ICT en ook voor Rijksconnect, in dezelfde periode in 2014 is uitgevoerd. In dit onderzoek zijn de BIR maatregelen per thema onderzocht.
Voor dit Assurance-onderzoek is bij de start van het onderzoek vastgesteld dat de alle maatregelen van de DGOBR thema's: 1. Patchmanagement, 2. Beheer van Koppelvlakken, 4. Pdca en 5.Logging&Monitoring van toepassing waren, aangevuld met een aantal extra BIR maatregelen.
Daarnaast hebben wij, in vergelijking met het DGOBR-onderzoek, voor alle BIR maatregelen naast het voeren van interviews en het ontvangen van bewijsmateriaal, voor zover mogelijk door middel van eigen waarnemingen, het bestaan vastgesteld. De waarnemingen zijn voor zover mogelijk uitgevoerd met een audittool. De resultaten ervan zijn apart op ieder formulier per BIR maatregel in een aparte rubriek vermeld. Wij zijn van mening dat wij daarmee bewijs hebben verkregen over de aanwezigheid van deze maatregelen gedurende de periode van 15 december 2014 tot en met 19 december 2014.
Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is om als onderbouwing voor ons oordeel te dienen.

4 Reikwijdte en inherente beperkingen

Het object van onderzoek wordt gevormd door de BIR maatregelen in de beheersprocessen die vermeld staan in punt 1 van deze notitie.
De reikwijdte van onze opdracht bevatte echter niet het uitvoeren van tests om de werking van de BIR maatregelen vast te kunnen stellen.
De beschrijving van BIR maatregelen van SSC-ICT is gedateerd op 11 januari 2015 en de informatie aangaande de waarnemingen m.b.t. het bestaan omvat de periode van 15 december 2014 tot en met 19 december 2014.
Iedere projectie van deze informatie naar de toekomst toe is onderhevig aan het risico dat door veranderingen de beschrijving niet langer de getroffen beheersmaatregelen weergeeft. De potentiële effectiviteit van de beschreven beheersmaatregelen van SSC-ICT kent inherente beperkingen, waardoor fouten en fraude kunnen voorkomen die niet ontdekt worden.
Tevens is de projectie van iedere conclusie, gebaseerd op onze bevindingen, naar de toekomst toe onderhevig aan het risico dat veranderingen in het stelsel van beheersmaatregelen, of het nalaten van noodzakelijke veranderingen daarin, de geldigheid van die conclusies kunnen ondergraven.

5 Oordeel

Ons oordeel is gevormd op basis van de werkzaamheden die in het bovenstaande van deze rapportage zijn uiteengezet. De criteria en de beoordelingsrichtlijnen die wij gehanteerd hebben bij het vormen van ons oordeel, staan in bijlage II beschreven.

opzet en bestaan
Wij zijn van oordeel dat wij met redelijke mate van zekerheid hebben kunnen vaststellen dat de BIR-maatregelen van Rijksconnect die conform de BIR gekoppeld zijn aan *de generieke beheersprocessen* (geclusterd per thema van maatregelen) en aan het beheer proces *change management* zoals verwoord in het NOREA normenkader voor uitbestede ICT beheerprocessen, in opzet **voldoen** aan de normen die de BIR stelt aan deze maatregelen.
Wij zijn van oordeel dat wij met redelijke mate van zekerheid hebben kunnen vaststellen dat de BIR-maatregelen van Rijksconnect die conform de BIR gekoppeld zijn aan de *generieke beheersprocessen* (geclusterd per thema van maatregelen), *het beheerproces capacity management en aan het beheer proces change management,* zoals verwoord in het NOREA normenkader voor uitbestede ICT beheerprocessen, in bestaan **voldoen** aan de normen die de BIR stelt aan deze maatregelen.

Beperking
Op grond van beoordelingen van documentatie, interviews met het personeel van SSC-ICT en waarnemingen ter plaatse hebben wij vastgesteld dat de BIR maatregelen binnen Rijksconnect voor het beheerproces *capacity management* in opzet **niet** aan de daar gestelde eisen in de BIR **voldoet**.

6 Beoogde gebruikers en doel

Het concept rapport is ter afstemming voorgelegd aan de gemandateerde vertegenwoordigers van de directeur SSC-ICT. De rapportage is daarna uitgebracht aan de directeur van SSC-ICT.
Na toestemming van de directeur van SSC-ICT is de rapportage met de assuranceverklaring aan de directeur Logius verstrekt.
De rapportage met de assuranceverklaring over Rijksconnect mag alleen door Logius aan de BA van BZK worden verstrekt. De verspreiding van deze assuranceverklaring aan andere organisaties mag alleen worden gedaan na toestemming van SSC-ICT. SSC-ICT en Logius zullen gezamenlijk moeten bepalen of de resultaten van deze audit mogen worden opgenomen in het jaarlijkse beheerverslag van SSC-ICT.

7 Ondertekening

Auditdienst Rijk,

Den Haag, 17 februari 2015

10,2 e

Bijlage 1: Overzicht BIR maatregelen per proces

Legenda gebruikte kleuren in overzicht:

1. Kleur Wit **per regel=**

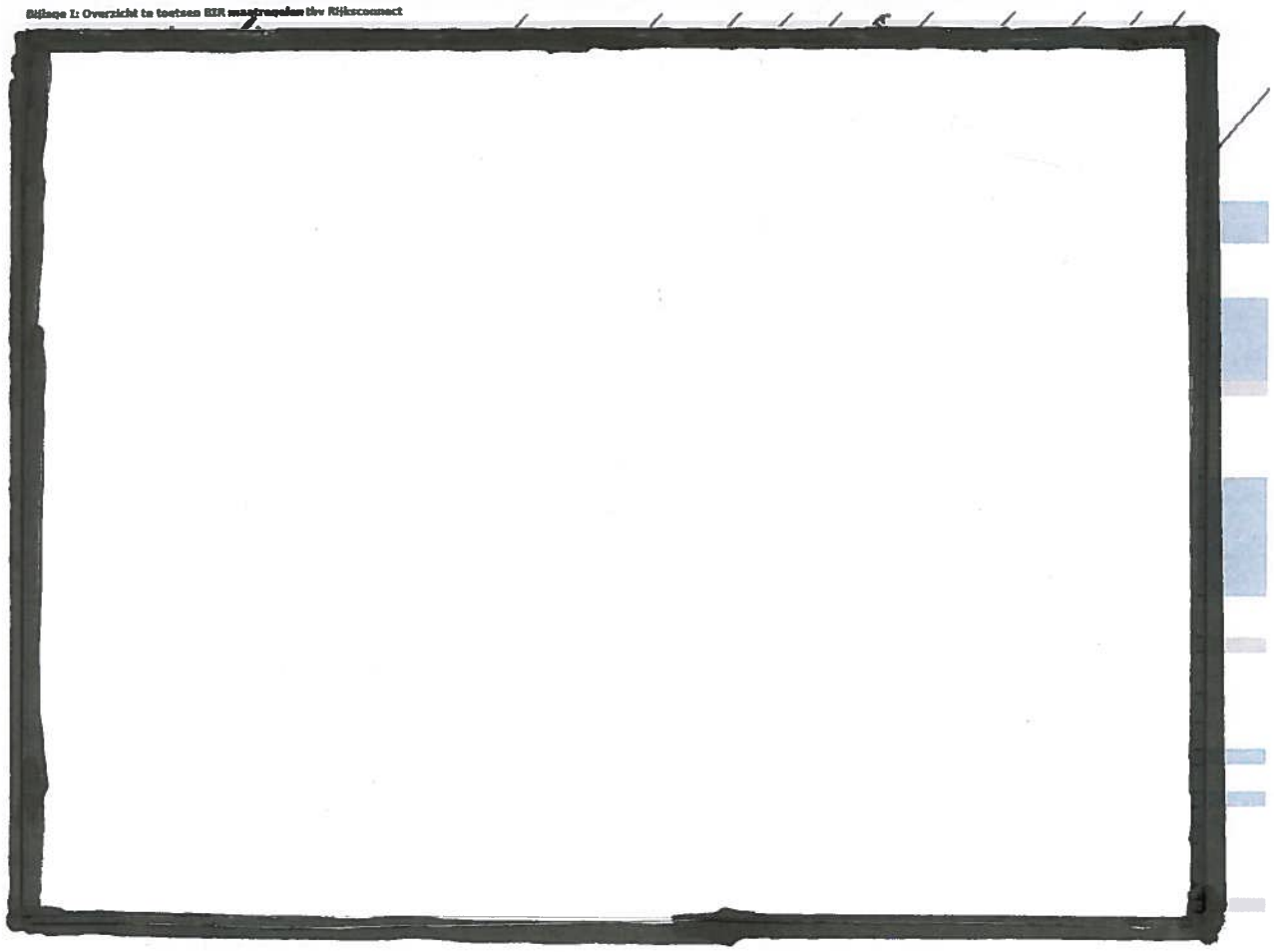
   de kleur voor alle BIR maatregelen die niet alleen bij een van de drie beheerprocessen onderzocht is, maar ook in het kader van het rijksbrede DGOBR onderzoek naar de BIR maatregelen (per thema);

2. kleur blauw per regel =

   de kleur voor de BIR maatregelen die alleen in het kader van het Rijksconnect onderzoek bij een van de drie beheerprocessen is onderzocht.

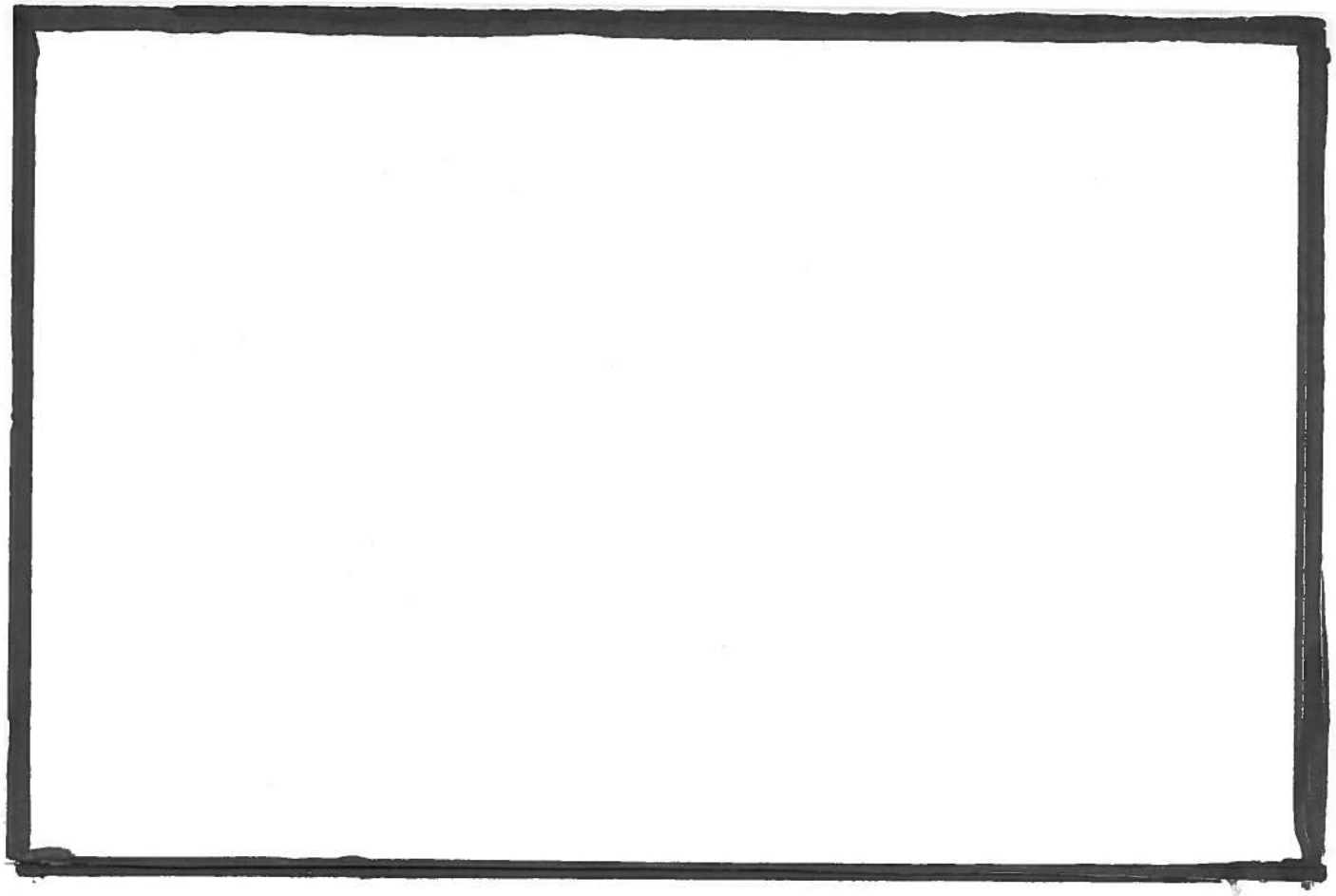
3. Kleur grijs =

   De kleur voor de oordelen in opzet en bestaan m.b.t. alle BIR maatregelen per beheerproces


Bijlage 1: Overzicht te toetsen BIR maatregelen tbv Rijksconnect

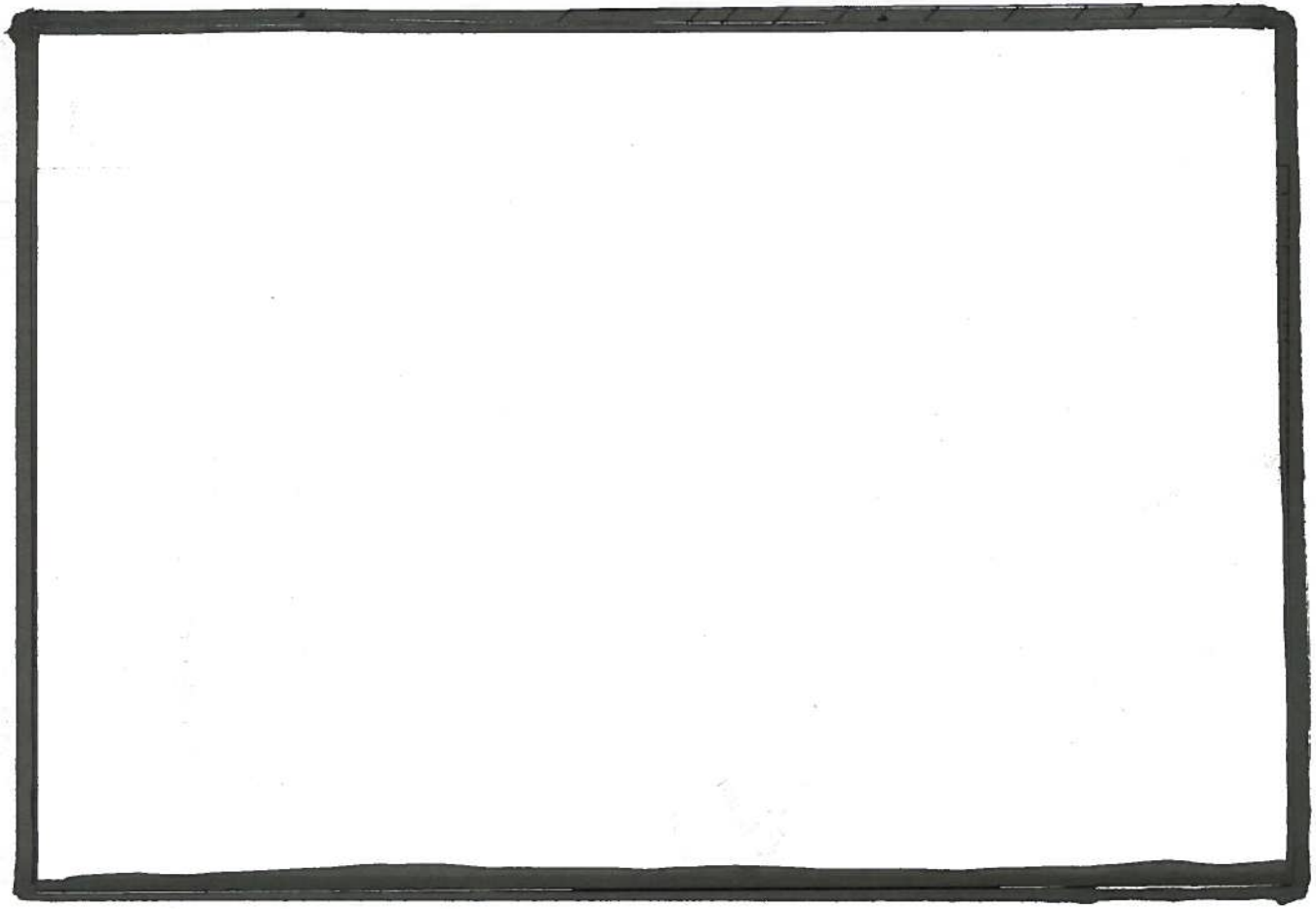
10,1,b +
10,2,8

Assurance rapport van de Auditdienst Rijk: Generiek, Capacity management en Change management in het systeem Rijksconnect



10, 1, b +
10, 2, 8

Assurance rapport van de Auditdienst Rijk: Generiek, Capacity management en Change management in het systeem Rijksconnect



10, 1, b +
10, 2, g

Assurance rapport van de Auditdienst Rijk: Generiek, Capacity management en Change management in het systeem Rijksconnect

Bijlage II: Criteria en richtlijnen inzake de weging van de BIR maatregelen.

Ten behoeve van de afgifte van de assuranceverklaring over Rijksconnect worden de uitkomsten van de beoordeling van de betrokken BIR maatregelen met elkaar vergeleken worden.

1 Criteria

Daarvoor worden in het onderstaande de criteria beschreven, die de zwaarte c.q. het belang van de ene BIR maatregel ten opzichte van de andere maatregelen aangeeft. Kortom welke maatregel(en) zijn belangrijker/essentiëler dan de overige categorieën maatregelen. De resultaten daarvan wegen zwaarder dan de overige twee onderscheiden categorieën: Belangrijk en Onderhouden.

De definities van de drie prioriteitscriteria luiden als volgt:

- Essentieel (E):
  - dit is een BIR maatregel waarvan de invulling voor een systeem Rijksconnect op het gebied van Informatiebeveiliging verplicht is (het is een zogenaamde showstopper). Bij het ontbreken ervan is onmiddellijk sprake van een 'onveilige' situatie. In essentie zijn dit alle maatregelen van niveau drie en van niveau vier met de indicatie R;
- Belangrijk (B):
  - dit is een BIR maatregel, waarvan de invulling voor een systeem Rijksconnect op het gebied van Informatiebeveiliging nodig is. Bij het ontbreken ervan is niet direct sprake van een 'onveilige' situatie, maar de omissie dient wel binnen 3 tot 6 maanden te zijn opgelost;
- Ondersteunend (O):
  - dit is een BIR maatregel, waarvan de invulling voor een systeem Rijksconnect op het gebied van Informatiebeveiliging niet direct nodig is. Bij het ontbreken ervan is niet direct sprake van een 'onveilige' situatie, maar de omissie dient wel op termijn, bij voorkeur binnen 12 maanden te zijn opgelost.

2 Richtlijnen inzake de weging van de BIR maatregelen

Daarnaast bevat deze paragraaf een beschrijving van beoordelingsrichtlijnen, die de ADR zal hanteren bij afweging van de uitkomsten van de gewogen BIR maatregelen om op deze manier te komen tot een oordeel voor de Assurance verklaring inzake de opzet en implementatie van de BIR maatregelen bij Rijksconnect.

De richtlijnen luiden als volgt:

1. Indien bij een thema een negatief beoordeling voor opzet of bestaan voorkomt bij een BIR maatregel met het criterium *Essentieel* dan zal het oordeel voor dat thema qua opzet of bestaan *als onvoldoende* luiden;
2. Indien bij een thema meer dan de helft van de BIR maatregelen met de indicatie *Belangrijk* negatief beoordeeld wordt, dan zal het oordeel voor dat thema qua opzet of bestaan *als onvoldoende* luiden
3. Bij een oordeel over een maatregel, wegen in geval van een BIR norm op het 3e niveau de bevindingen m.b.t. de opzet zwaarder dan m.b.t. het bestaan.

Bij een oordeel over een maatregel wegen in geval van een BIR norm op het 4e niveau de bevindingen m.b.t. het bestaan zwaarder dan m.b.t. de opzet