Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport

Toetsbaarheid BIO (O-maatregelen)

Uitgebracht aan: directeur-generaal Overheidsorganisatie (DGOO)

Kenmerk 2019-0000203594

Den Haag, 16 december 2019

Auditdienst Rijk
Ministerie van Financiën

Inhoud

- Aanleiding opdracht
- Samenvatting
- Onderzoeksvragen
- Bevindingen bij de O-maatregelen
- Verantwoording onderzoek
- Ondertekening
- Bijlage

Aanleiding opdracht

Het Directoraat-generaal Overheidsorganisatie (DGOO) heeft in 2018 een nieuwe Baseline opgesteld ter vervanging van diverse baselines informatiebeveiliging van de (Rijks-)overheid. De BIO is daarmee een gemeenschappelijk normenkader voor de beveiliging van de informatie(systemen) van de overheid. De interbestuurlijke werkgroep Normatiek onderhoudt de BIO (als onderdeel van het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO)).

De BIO beschrijft per basisbeveiligingsniveau (BBN) aan welke ISO27002 controls moet worden voldaan.

De werkgroep wil weten of het deel overheids specifieke maatregelen ((O) maatregelen) in de BIO (v1.0) toetsbaar zijn. De ADR is gevraagd deze toetsbaarheid te onderzoeken.

Samenvatting (1/2)

In de O-maatregelen zien wij toetsbare maatregelen en maatregelen die minder specifiek, realistisch en meetbaar zijn waardoor die maatregelen mogelijk verschillend geïnterpreteerd worden. Deels is dit inherent aan het tactische karakter van de BIO waarbij een nadere inrichting vereist is bij implementatie. De auditor zal deze vertaling en de context mee moeten nemen bij het toetsen.

Er zijn 66 controls met in totaal 137 O-maatregelen onderzocht. Deze maatregelen zijn voor BBN 1 en BBN 2. Voor 26 normen wordt een aanpassing in de norm en voor 88 normen een toelichting geadviseerd.

Samenvatting (2/2)

Gedurende het onderzoek is de BIO versie 1.0 in december 2018 geaccordeerd door de ministerraad. De werkgroep Normatiek wil mede naar aanleiding van onze bevindingen werken aan een implementatieplan waarbij gebruikers meer guidance krijgen door middel van toelichtingen, voorbeelden en handreikingen bij de BIO. Ook wil de werkgroep audits faciliteren door het ontwikkelen van een toetsingskader bij de BIO.

De belangrijkste punten zijn samengevat in dit rapport en details zijn te vinden in bijlage A.

De opdrachtgever kan de onderzoeksuitkomst gebruiken om de toetsbaarheid van de BIO te verbeteren.

Doelstelling en onderzoeksvragen

Het onderzoek moet inzicht geven of de in de BIO geformuleerde O-maatregelen SMART zijn geformuleerd zodat ze op een eenduidige wijze getoetst kunnen worden.

De volgende vragen zijn geformuleerd:

- *Welke bevindingen zijn er ten aanzien van de toetsbaarheid per O-maatregel in de BIO?*
- *Welke eventuele suggesties* zijn er per O-maatregel om ze beter toetsbaar te maken?*

Toetsbaarheid is de mate waarin een maatregel Specifiek, Meetbaar en Realistisch is.

* De suggesties richten zich niet inhoudelijk op het niveau van beveiliging in de maatregelen.

Bevindingen bij de O-maatregelen (1/5)

Per O-maatregel zijn 4 elementen toegevoegd als bijlage bij deze rapportage.

a) Opmerkingen zijn gemaakt bij de aspecten Specifiek, Realistisch en Meetbaar.
b) Middels categorieën is aangegeven wat voor soort opmerking dit betreft.
c) Aangegeven is of een toelichting meerwaarde heeft of dat een aanpassing in de norm gesuggereerd wordt.
d) Per norm is aangegeven door de werkgroep wat het plan is voor het onderhoud.

In de volgende sheets volgt de kwantitatieve opsomming en een toelichting.

Bevindingen bij de O-maatregelen (2/5)

A) Specifiek, Realistisch en Meetbaar?

Aspect	Toelichting	Aantal opmerkingen
Specifiek	De mate waarin duidelijk is wie wat wanneer moet uitvoeren.	86
Meetbaar	De mate waarin tests uitgevoerd kunnen worden om vast te stellen of aan de maatregel is voldaan.	58
Realistisch	De mate waarin het toetsen haalbaar is.	30

Uit onze werkzaamheden blijkt dat bij het merendeel van de normen er elementen zijn die zonder uitwerking het lastig maken “wat” de auditor moet toetsen om het beheersdoel te realiseren. Dit is deels inherent aan het tactische karakter van de BIO dat uit gaat van beveiligingsprincipes die door de auditee nader vorm worden gegeven.

Bevindingen bij de O-maatregelen (3/5)

B) Wat voor soort opmerkingen zijn er?

Categorie	Omschrijving	aantal
A	De normtekst verwijst naar andere regels, standaarden en voorschriften	15
B	De normtekst heeft een inconsistentie diepgang door specifieke als brede termen te gebruiken	30
C	De normtekst bevat termen contextgevoelig zijn.	6
D	De normtekst bevat begrippen waarvan niet duidelijk is wat er precies mee wordt bedoeld	46
E	Dezelfde normtekst komt al elders terug, verwijzing ontbreekt en er is sprake van overlap zonder argumentatie.	7
F	De normtekst zal in veel gevallen leiden tot een bevinding omdat het in de praktijk anders geimplementeerd zal zijn.	1
G	Vervallen	0
H	De normtekst heeft geen link met ICT of wordt afgedekt door andere regelgeving of normenkaders.	5
I	De normtekst beschrijft een specifieke uitkomst van risicoanalyse waardoor het nog niet specifiek is.	22
J.	Overig	29
K.	Maatregel vertoont grote overeenkomsten met doelstelling.	7

Uit onze werkzaamheden blijkt dat er vooral veel termen toelichting behoeven omdat ze anders verschillend geïnterpreteerd kunnen worden. Ook het verwijzen naar andere standaarden en brede doelstellingen behoeven een toelichting.

Bevindingen bij de O-maatregelen (4/5)

C) Waar zijn aanpassingen gewenst?

Acties	Aantal
Geen opmerkingen	24
Uitwerken in handreiking	69
Onderhoud BIO	26
Onderhoud + handreiking	18
Totaal	137

Uit onze werkzaamheden blijkt dat bij veel normen opmerkingen zijn gemaakt die in een handreiking verduidelijkt kunnen worden. Voor 1/5 van de normen zou in de normtekst verduidelijking gewenst zijn waarbij dit in veel gevallen gaat om normen waarbij een nadere risico analyse nodig is van de eigenaar om de norm specifiek en daarmee beter toetsbaar te maken.

Bevindingen bij de O-maatregelen (5/5)

D) Wat is de werkgroep van plan?

In 5 sessies zijn de bevindingen van de ADR besproken met leden van de werkgroep Normatiek. Per norm is een managementreactie gegeven.

De werkgroep geeft aan te willen komen tot een implementatieplan waarbij middels handreikingen en toelichtingen aanknopingspunten geformuleerd worden om de norm in te richten. Tevens is contact gelegd met de beroepsgroep om te kijken hoe de toetsing in de praktijk kan worden vormgegeven (onderhanden per schrijven van dit rapport)

Daarnaast is besproken dat een verduidelijking voor het begrip risico analyse en de voorwaarden die dat stelt aan de inrichting een grote bijdrage levert voor het uitvoeren van audits.

Verantwoording onderzoek

Uitgevoerde werkzaamheden

- 17 april 2018 is de initiële versie (1.0) van de BIO aan de ADR verstrekt
- In sessies in de periode augustus 2018-april 2019 zijn de bevindingen inhoudelijk besproken met de gedelegeerd opdrachtgever en één of twee vertegenwoordigers van de werkgroep Normatiek. In mei en juni 2019 zijn de bevindingen van de ADR besproken in de werkgroep Normatiek waarbij de ADR in de vergadering van de werkgroep in juni een toelichting heeft gegeven.
- 13 november jl. is het concept rapport besproken met de gedelegeerd opdrachtgever en een vertegenwoordiger van de werkgroep Normatiek

De O-maatregelen zijn onderzocht door meerdere auditors.

Verantwoording onderzoek

Afbakening

Buiten de scope van deze opdracht vallen:

- De onderliggende handreikingen en voorbeelden per O-maatregel.
- Bevindingen over activiteiten gericht op de juistheid en volledigheid van de controls (beheersmaatregelen) per basisset van de BIO.
- Bevindingen over de toetsbaarheid van de onderliggende ISO-27002 implementatierichtlijnen.
- De vraag of de normen aansluiten op het beveiligingsniveau.
- De aanvullende eisen die gelden vanaf BBN3 zijn in versie 1.0 van de BIO nog niet nader uitgewerkt.

Verantwoording onderzoek

Gehanteerde Standaard

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing.

Met deze rapportage wordt geen zekerheid verschaft, omdat geen assurance-opdracht wordt uitgevoerd. De rapportage bevat daarom geen samenvattende conclusie of eindoordeel.

De opdracht is afgestemd in de opdrachtbevestiging met nummer: 2018-0000143607.

Verantwoording onderzoek

Verspreiding rapport

De opdrachtgever, de directeur Informatiesamenleving en Overheid bij het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, is eigenaar van dit rapport.

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de ADR een rapport heeft geschreven, het rapport binnen zes weken op de website van de rijksoverheid plaatst, tenzij daarvoor een uitzondering geldt. De minister van Financiën stuurt elk halfjaar een overzicht naar de Tweede Kamer met de titels van door de ADR uitgebrachte rapporten en plaatst dit overzicht op de website.

Ondertekening

Dit rapport is opgesteld door:

Drs. C.L.J.C. Jacobs RE EMIA

IT audit manager

Den Haag, 16-12-2019

Auditdienst Rijk

Management reactie

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Ministerie van Financiën
Auditdienst Rijk
T.a.v. Drs. C.L.C.J. Jacobs RE EMIA
Postbus 20201
2500 EE Den Haag

DGOO
IDIO

www.rijksoverheid.nl
www.facebook.com/minbzk
www.twitter.com/minbzk

Contactpersoon
C.P.J. van der Maarel

T 06-18304234
kees.maarel@minbzk.nl

Kenmerk
2019-0000475921

Uw kenmerk

Datum 5 september 2019
Betreft Managementreactie bij het onderzoek toetsbaarheid BIO (O-maatregelen)

Geachte heer Jacobs,

Met interesse heb ik uw rapportage t.a.v. de toetsbaarheid BIO gelezen. De aanbevelingen die u in uw rapport doet, zijn bruikbaar bij het verder aanscherpen van de overheidsmaatregelen die in de BIO zijn opgenomen.

Daar waar mogelijk nemen we uw aanbevelingen al mee in de eerste onderhoudslag die we momenteel op de BIO uitvoeren. Waar dat nu niet mogelijk is, zullen we overwegen deze in de toekomstige onderhoudscycli op de BIO en haar handreikingen op te pakken.

Ik dank u voor uw bijdrage aan het verbeteren van de kwaliteit van de BIO.

Met vriendelijke groet,

Directeur Informatiesamenleving en Overheid
Bas den Hollander

Auditdienst Rijk
Ministerie van Financiën

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(070) 342 77 00

Bijlage

A. “Bevindingen BIO matrix per juni 2019.pdf”

Control		Overheidsmaatregel										
Nummer	**Tekst**	**Nummer**	**Tekst**	**BBN**	**Opmerking categorie**	**Aanvullende opmerking over specifiek**	**Aanvullende opmerking over realistisch**	**Aanvullende opmerking over meetbaar**	**ADR suggestie**	**Toelichting Onderhoud BIO**	**Toelichting Uitwerken in handreiking/toelichting/instructie**	**Management reactie OK= wordt aangepast of toegelicht NOK = wordt niet aangepast of toegelicht**
5.1.1	Beleidsregels voor informatiebeveiliging: Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	5.1.1.1	Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat tenminste de volgende punten: a) de strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in, en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid; b) de organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden; c) de toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers; d) de gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn;	1	J	Niet duidelijk is op welk niveau (Ministerie,DG, Directie, ZBO) het beveiligingsbeleid moet worden ontwikkeld.			Uitwerken in handreiking		Nadere uitwerking hoogste ambtelijke leiding	OK. Concreter worden is niet mogelijk omdat er verschillende organisaties bij zijn betrokken. Taken zijn verdeeld over de verantwoordelijken. In de BIO worden voorbeelden genoemd van functionarissen die het IB beveiligingsbeleid moeten accorderen. In het werkprogramma moet worden vastgelegd dat bv de gemeentesecretaris het beleid vaststelt. Tekstvoorstel uitwerken waarin wordt toegelicht wat wordt bedoeld met de daartoe bevoegde hoogste leiding. Is het voldoende vastgelegd dat de IC door de verschillende managementlagen moet worden afgegeven? Is helder beschreven wie het beleid moet uitvoeren? Is niet expliciet vastgelegd maar wel dat het beleid moet worden geëvalueerd. In woorden aanscherpen.
5.1.2	Beoordeling van het informatiebeveiligingsbeleid: Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	5.1.2.1	Het informatiebeveiligingsbeleid wordt minimaal één keer per drie jaar, of bij belangrijke wijzigingen als gevolg van reorganisatie of verandering in de verantwoordelijkheidsverdeling, beoordeeld en zo nodig bijgesteld.	1	D	Er is niet helder vastgelegd wat de criteria zijn voor een "belangrijke"wijziging. Dus niet duidelijk op welk moment het beleid moet worden beoordeeld/aangepast. Belangrijke wijzigingen in de IT infrastructuur kunnen ook leiden tot veranderingen in het informatiebeleid of het herzien van het informatiebeveiligingsbeleid. De focus wordt nu gelegd op organisatorische veranderingen.		Er kan worden vastgesteld wanneer het beleid is vastgesteld/bijgesteld. Niet duidelijk is of zichtbaar is op welk moment een 'belangrijke' wijziging heeft plaats gevonden.	Uitwerken in handreiking		Nader uitwerken belangrijke wijziging	Een belangrijke wijziging moet zijn uitgewerkt in het beleid. In de risico-analyse moet zijn uitgewerkt wat wijzigingen met een belangrijk risico zijn. De onderbouwing moet uit de risico-analyse komen. In handreiking specifiek maken.
6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging: Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	6.1.1.1	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.	1	K	Moet er ook een minimale set van verantwoordelijkheden en rollen worden vastgelegd?			Uitwerken in handreiking		In een handreiking verder duiding aan minimale verantwoordelijkheden geven.	OK. Er wordt gewerkt aan een CISO profiel. Onderdeel van een handreiking.
6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging: Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	6.1.1.2	De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.	1	B	Verwijzing naar voorschriften ontbreekt. Waarom niet de voorschriften noemen die minimaal in scope moeten zijn?		Niet duidelijk welke rollen/verantwoordelijk-heden er moeten zijn of wie dit vaststelt. Dus is de volledigheid ook niet vast te stellen.	Uitwerken in handreiking		Geef een overzicht van verantwoordelijkheden en rollen die minimaal moeten worden belegd en doe een suggestie van het niveau waarop deze moeten worden belegd.	OK. Uitwerken in handreiking/toelichting
6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging: Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	6.1.1.3	De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.	1	A	Welke rollen en verantwoordelijkheden horen minimaal in CISO profiel?			Uitwerken in handreiking		Voorbeeld CISO profiel. In de handreiking voorbeelden opnemen van rollen en verantwoordelijkheden die beschreven moeten zijn.	OK. Er wordt gewerkt aan een CISO profiel. Onderdeel van een handreiking.
6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging: Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	6.1.1.4	Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.	1	A			Is er rijksbreed een CISO profiel beschikbaar?	Uitwerken in handreiking		Zie 6.1.1.3	OK. Er wordt gewerkt aan een CISO profiel. Onderdeel van een handreiking.

Control		Overheidsmaatregel										
Nummer	**Tekst**	**Nummer**	**Tekst**	**BBN**	**Opmerking categ**	**Aanvullende opmerking over specifiek**	**Aanvullende opmerking over realistisch**	**Aanvullende opmerking over meetbaar**	**ADR suggestie**	**Toelichting Onderhoud BIO**	**Toelichting Uitwerken in handreiking/toelichting/instructie**	**Management reactie OK= wordt aangepast of toegelicht NOK = wordt niet aangepast of toegelicht**
6.1.2	Scheiding van taken: Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	6.1.2.1	Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.	1	I	Voor deze maatregel is nadere risico-analyse nodig			Onderhoud BIO	Voor deze maatregel is nadere risico-analyse nodig	In een handreiking beschrijven dat obv een risicoanalyse maatregelen worden bepaald en moeten worden getroffen. Daaruit blijken lancunes. Overwegen de overgang van deel 1 naar deel 2 in de BIO nader te duiden, nadere toelichting te geven. Eerst moet de risico-analyse worden opgevraagd. Vragen naar lijstje met bedrijfsmiddelen, risico-analyse en welke maatregelen zijn er? Dit vergt een goede toelichting. Er is een themagroep logische toegangsbeveiliging. Voorkeur te kiezen voor een toelichting dat kan worden aangevuld met handreikingen uit de themagroep. Norm opnemen in de BIO dat risico-analyse moet zijn uitgevoerd.	OK In deel 1 paragraaf 1.2 staat helder 'Het lijnmanagement stelt op basis van een expliciete risicoafweging de betrouwbaarheidseisen voor zijn informatiesystemen vast); & Op basis van de betrouwbaarheidseisen kiest, implementeert en draagt het lijnmanagement de maatregelen uit).' Door het centraal eenmaal te beschrijven, hoeft het niet steeds herhaald te worden. NOK, reeds opgenomen in QIS
6.1.3	Contact met overheidsinstanties: Er behoren passende contacten met relevante overheidsinstanties te worden onderhouden.	6.1.3.1	Er is door de organisatie uitgewerkt wie met welke (overheids)instanties en toezichthouders contact heeft ten aanzien van informatiebeveiligingsaangelegenheden (vergunningen/incidenten/calamiteiten) en welke eisen voor deze aangelegenheden relevant zijn.	2					Geen opmerkingen			
6.1.3	Contact met overheidsinstanties: Er behoren passende contacten met relevante overheidsinstanties te worden onderhouden.	6.1.3.2	Het contactoverzicht wordt jaarlijks geactualiseerd.	2					Geen opmerkingen			
6.2.1	Beleid voor mobiele apparatuur: Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	6.2.1.1	Mobiele apparatuur is zo ingericht dat geen bedrijfsinformatie onbewust wordt opgeslagen ('zero footprint'). Als zero footprint (nog) niet realiseerbaar is, biedt een mobiel apparaat (zoals een laptop, tablet en smartphone) de mogelijkheid om de toegang te beschermen door middel van een toegangsbeveiligingsmechanisme en, indien vertrouwelijke gegevens worden opgeslagen, versleuteling van die gegevens. In het geval van opslag van vertrouwelijke informatie moet op deze mobiele apparatuur 'wissen op afstand' mogelijk zijn.	2	D	Het gaat hier over het beleid van de apparatuur en telewerken en niet over de technische maatregelen die bijdragen aan het borgen van de naleving van het beleid.		Als er ook privé apparatuur gebruikt kan worden voor zakelijke doeleinden is het lastig een volledig beeld te krijgen en de inrichting te bewaken.	Uitwerken in handreiking		Beleid gebruik privé apparatuur voor zakelijke doeleinden nader uitwerken.	OK. Nader uitwerken in handreiking/toelichting/instructie
6.2.1	Beleid voor mobiele apparatuur: Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	6.2.1.2	Bij de inzet van mobiele apparatuur zijn minimaal de volgende aspecten geïmplementeerd: a) in bewustwordingsprogramma's komen gedragsaspecten van veilig mobiel werken aan de orde; b) het device maakt onderdeel uit van patchmanagement en hardening; c) het device wordt waar mogelijk beheerd en beveiligd via een MDM Mobile Device Management (MDM)-oplossing; d) gebruikers tekenen een gebruikersovereenkomst voor mobiel werken, waarmee zij verklaren zich bewust te zijn van de gevaren van mobiel werken en verklaren dit veilig te zullen doen. Deze verklaring heeft betrekking op alle mobiele apparatuur die de medewerker zakelijk gebruikt; periodiek wordt getoetst of de punten in lid b), c) en d) worden nageleefd.	2	C	-Zie opmerking bij 6. 2.1.1 -a) Welke gedragsaspecten moeten in het bewustwordingsprogramma zijn benoemd. Wie is verantwoordelijk voor de bewustwordingsaspecten ? c) Om een device uit te laten maken van patchmanagement en hardening moeten deze aspecten wel helder en eenduidig zijn geïmplementeerd en belegd. Hoe ga je om met de norm als hardening en patchmanagement niet zijn georganiseerd? e) Zijn er eisen aan een MDM oplossing of is elke organisatielaag vrij om dit zelf te implementeren?	Op welke wijze kan je het zakelijk gebruik beveiligen/monitoren? B)Hoe ga je om met het gebruik van privé devices voor zakelijke doeleinden en andersom?	"waar mogelijk" is niet te toetsen	Onderhoud + handreiking	"waar mogelijk" is niet te toetsen.	Nader uitwerken bewustwordingsprogramma, welke gedragsaspecten van belang zijn, uitwerken MDM oplossing.	OK Je zult altijd iets moeten doen om de mobile devices te beheersen. Niet opnemen in de toelichtinhg. Maatregel aanpassen in bij voorkeur MDM of een andere maatregel. Meenemen in onderhoud BIO.

Control		Overheidsmaatregel										
Nummer	**Tekst**	**Nummer**	**Tekst**	**BBN**	**Opmerking categorie**	**Aanvullende opmerking over specifiek**	**Aanvullende opmerking over realistisch**	**Aanvullende opmerking over meetbaar**	**ADR suggestie**	**Toelichting Onderhoud BIO**	**Toelichting Uitwerken in handreiking/toelichting/instructie**	**Management reactie OK= wordt aangepast of toegelicht NOK = wordt niet aangepast of toegelicht**
7.1.1	Screening: Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's te	7.1.1.1	Bij indiensttreding overleggen alle medewerkers (intern en extern) een specifiek voor de functie verstrekte Verklaring Omtrent het Gedrag (VOG).	1	D		Hoe realistisch is het om bij promotie een nieuwe VOG te laten tekenen? Is dit ook gevraagd?		Onderhoud BIO	De rubricering van informatie alsmede de frequentie waar een medewerker met gerubriceerde informatie in aanraking komt bepaalt het type screening dat een medewerker moet hebben. Dat kan zijn een VOG, een AIVD-screening, MIVD screening. Voor een incidentele aanraking met gerubriceerde informatie kan een geheimhoudingsverklaring voldoende zijn. Screening wordt veelal gekoppeld aan een (vertrouwens-)functie.		NOK Leidt hier niet tot aanpassing. Wel verderop in de BIO bij gevoelige informatie. Bij een nieuwe functie of promotie dient een medewerker een VOG te overleggen. OK in FAQ Toelichten dat bij wisselen van functie in de rijksoverheid een nieuwe VOG moet worden overlegd.
7.1.2	Arbeidsvoorwaarden: De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.	7.1.2.1	Alle medewerkers (intern en extern) zijn bij hun aanstelling of functiewisseling gewezen op hun verantwoordelijkheden ten aanzien van informatiebeveiliging. De voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging zijn eenvoudig toegankelijk.	1	C	Hoe stel je vast welke regelingen en instructies gelden voor de medewerkers?		Hoe stel je vast dat alle mede werkers deze verantwoordelijkheden hebben gezien en begrepen?	Uitwerken in handreiking		Laat medewerkers tekenen voor de geldende regels bij indiensttreding en daarna bij wijzigingen of in ieder geval jaarlijks ter herinnering. Bij weigering ondertekening toegang tot de systemen ontzeggen.	
7.2.1	Directieverantwoordelijkheden: De directie behoort van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.	7.2.1.1	Er is aansluiting bij een klokkenluidersregeling, zodat iedereen in staat is om anoniem en veilig beveiligingsissues te kunnen melden.	1				Is het de bedoeling om dit te controleren in het kader van de BIR? Dit is wettelijk geregeld.	Geen opmerkingen			
7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging: Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	7.2.2.1	Alle medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen	1	B	Hoe krijg je een overzicht van alle regels en verplichtingen met betrekking tot informatiebeveiliging?		Hoe toets je dat alle medewerkers de regels en verplichtingen kennen?	Uitwerken in handreiking		In de handreiking duiden welke aanknopingspunten er zijn om vast te stellen hoe iedereen de regels kent.	
7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging: Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	7.2.2.2	Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen- en diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd.	1	B	Is de training I-bewustwijn overheidsbreed aan te wijzen?			Geen opmerkingen			
7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging: Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	7.2.2.3	Het management benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij haar medewerkers en contractanten het belang van opleiding en training op het gebied van informatiebeveiliging en stimuleert hen actief deze periodiek te volgen.	1	D			Niet duidelijk is wat het benadrukken inhoud. Betekent dit dat eea wordt besproken in overleggen? Wat als er geen verslagen zijn? -Of moet er ook daadwerkelijk worden vastgesteld dat er opleiding en training worden gevolgd en door wie?	Uitwerken in handreiking		In de handreiking duiden welke aanknopingspunten er zijn om dit vast te stellen wat benadrukken is.	
8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen: Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten behoren regels te worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	8.1.3.1	Alle medewerkers zijn aantoonbaar gewezen op de gedragsregels voor het gebruik van bedrijfsmiddelen.	1	D	Dienen medewerkers expliciet te bevestigen dat zij kennis hebben genomen van de regels?		"Alle medewerkers" is niet realistisch als er 1 bv een cursus niet heeft gevolgd	Uitwerken in handreiking		In de handreiking duiden welke aanknopingspunten er zijn om vast te stellen wat aantoonbaar gewezen is.	
8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen: Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten behoren regels te worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	8.1.3.2	De gedragsregels voor het gebruik van bedrijfsmiddelen zijn voor extern personeel in het contract vastgelegd overeenkomstig de huisregels of gedragsregels.	1	B		Gedragregels of een verwijzing naar de gedragsregels? Vaak wordt gewerkt met raamcontracten.	Alle contracten moeten dan doorgenomen. Is het helder welke contracten er moeten zijn? Worden er in de contracten ook afspraken gemaakt over naleving en de consequenties van niet naleving? Dienen de gedragsregels te worden toegevoegd aan de contracten in een bijlage? Eis stellen dat alle contracten in een contractenregister zijn opgenomen. Is deze juist en volledig?	Uitwerken in handreiking		Voorbeelden uitwerken van de wijze waarop gedragsregels in contracten moeten worden vastgelegd en op welke maneir we dit kunnen toetsen.	

Control		Overheidsmaatregel										
Nummer	**Tekst**	**Nummer**	**Tekst**	**BBN**	**Opmerking categ...**	**Aanvullende opmerking over specifiek**	**Aanvullende opmerking over realistisch**	**Aanvullende opmerking over meetbaar**	**ADR suggestie**	**Toelichting Onderhoud BIO**	**Toelichting Uitwerken in handreiking/toelichting/instructie**	**Management reactie OK= wordt aangepast of toegelicht NOK = wordt niet aangepast of toegelicht**
8.2.1	Classificatie van informatie: Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	8.2.1.1	De informatie in alle informatiesystemen is door middel van een expliciete risicoafweging geclassificeerd, zodat duidelijk is welke bescherming nodig is.	1	IC	Betreft dit de systemen (applicaties?) die een directie gebruikt of Betreft een systemen (applicaties?) waarvoor de directie eigenaar is? Krijgt de onderliggende infrastructuur dezelfde classificatie? -Hoe moet de classificatie worden uitgevoerd?	De maatregeltekst is zo geformuleerd dat het lijkt alsof het toekennen van de juiste classificatie, automatisch leidt tot de juiste bescherming.	"altijd de juiste bescherming" is een doelstelling.	Onderhoud BIO	Voor deze norm is het uitvoeren van een risico-analyse van belang hetgeen geen norm op zich is. Informatie rubriceren ipv classificeren.		NOK, is reeds gedaan. Algemene formulering opstellen en daarnaar verwijzen. Moet worden vastgelegd. Volwassenheidsniveau organisatie speelt een rol.
8.3.1	Beheer van verwijderbare media: Voor het beheren van verwijderbare media behoren procedures te worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	8.3.1.1	Er is een verwijderinstructie waarin is opgenomen dat van herbruikbare media die de organisatie verlaten de onnodige inhoud onherstelbaar verwijderd (ISO27002 – implementatierichtlijn 8.3.1.a).	1	J	Dit betreft alle media (harde schijven, USB-sticks, cd's, etc.)? - Betekent de organisatie verlaten ook de overdracht aan externe partijen.Wat is niet meer nodig. Dat is voor veel intepretaties open		Media die de organisatie hebben verlaten zijn waarschijnlijk niet meer beschikbaar voor controle op evt aanwezige informatie (testen of verwijderen op de juiste manier is gebeurd). Meetbaar is dus lastig Voordat media de organisatie verlaten moet zijn vastgesteld en gedocumenteerd dat deze geen informatie meer bevat.	Uitwerken in handreiking		Uitwerken aanknopingspunten om deze norm vast te stellen. Mogelijk zeer lastig te controleren tenzij het alleen gaat om de instructie vast te stellen.	
8.3.1	Beheer van verwijderbare media: Voor het beheren van verwijderbare media behoren procedures te worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	8.3.1.2	De wijze waarop vertrouwelijk of hoger geclassificeerde informatie is opgeslagen, voldoet aan de eisen van het NBV.	2	A	Dit verwijst naar alle eisen NBV en is daarmee niet specifiek maar een doelstelling	NBV heeft niet voor alle producten en versies instructies.		Onderhoud + handreiking	Classificeren vervangen door rubriceren.	Nadere duiding geven aan rubriceringsniveaus en duiden welke NBV-eisen worden bedoeld.	OK. Is NBV van toepassing voor alle overheidslagen? Overwegen deze maatregelen naar het addendum te verhuizen.
8.3.2	Verwijderen van media: Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	8.3.2.1	Media die vertrouwelijke informatie bevatten zijn opgeslagen op een plek die niet toegankelijk is voor onbevoegden. Verwijdering vindt plaats op een veilige manier, bijv. door verbranding of versnippering. Verwijdering van alleen gegevens is ook mogelijk door het wissen van de gegevens voordat de media worden gebruikt voor een andere toepassing in de organisatie (ISO27002 – implementatierichtlijn 8.3.2.a)	2	J	Door wie en hoe wordt bepaald op welke manier media moeten worden opgeslagen -Zijn er eisen aan versnippering (snippergrote?) -Zijn er eisen aan het wissen	Ook als een apparaat wordt vernietigd moet de data worden gewist. Er is altijd een risico dat een aparaat niet wordt vernietigd.		Uitwerken in handreiking		Nader uitwerken op welke wijze kan worden vastgesteld dat aan deze norm wordt voldaan.	
8.3.2	Verwijderen van media: Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	8.3.2.2	Voor het wissen van alle data op het medium, wordt de data onherstelbaar verwijderd, bijvoorbeeld door minimaal twee keer te overschrijven met vaste data en één keer met random data. Er wordt gecontroleerd of alle data onherstelbaar verwijderd is.	2	J			Voor audit achteraf zeer lastig te toetsen als apparatuur is vernietigd	Uitwerken in handreiking		Is het toegestaan om alleen procedures in te zien want vaststellen achteraf is vrijwel onmogelijk.	
8.3.3	Media fysiek overdragen: Media die informatie bevatten, behoren te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	8.3.3.1	Er is voor de gehele organisatie beleid voor het fysiek transport van media vastgesteld.	2					Geen opmerkingen			
8.3.3	Media fysiek overdragen: Media die informatie bevatten, behoren te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	8.3.3.2	Het gebruik van koeriers of transporteurs voor vertrouwelijk of hoger geclassificeerde informatie voldoet aan vooraf opgestelde betrouwbaarheidseisen.	2	BD	Opgestelde betrouwbaarheidseisen is niet specifiek. Welke eisen worden er gesteld aan koeriers of transporteurs? Worden er ook eisen gesteld aan de wijze van transport?		Voldoet is heel groot en niet te toetsen . Moet er beleid zijn? Op welke wijze wordt gecontroleerd dat transporteurs voldoen aan de kwaliteitseisen	Uitwerken in handreiking		Eisen voor het gebruik van koeriers of transporteurs voor vertrouwelijke of hoger geclassificeerde of beter gerubriceerde informatie voldoet nader uitwerken.	
9.1.2	Toegang tot netwerken en netwerkdiensten: Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	9.1.2.1	Alleen geauthenticeerde apparatuur kan toegang krijgen tot een vertrouwde zone.	1	D	Wat is de definitie van een vertrouwde zone? Is dit op basis van een risicoanalyse? Op welke wijze wordt geauthenticeerde apparatuur herkend?		Welke architectuurprincipes dienen gevolgd te worden ivm zonering?	Uitwerken in handreiking		Uitwerken definities vertrouwde zones en uitwerken op welke wijze ongeauthenticeerde apparatuur wordt herkend.	
9.1.2	Toegang tot netwerken en netwerkdiensten: Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	9.1.2.2	Gebruikers met eigen of ongeauthenticeerde apparatuur (Bring Your Own Device) krijgen alleen toegang tot een onvertrouwde zone.	1	D	Wat is de definitie van een onvertrouwde zone? Is dit op basis van een risicoanalyse? Op welke wijze wordt niet geauthenticeerde	Is het realistisch om het gebruik van BYOD bij gegevens zo in te perken?	Welke architectuurprincipes dienen gevolgd te worden ivm zonering?	Uitwerken in handreiking		Uitwerken definities vertrouwde zones en uitwerken op welke wijze ongeauthenticeerde apparatuur wordt herkend.	
9.2.1	Registratie en afmelden van gebruikers: Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	9.2.1.1	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.	1	D	Sluitend is voor meerdere uitleg vatbaar. Wat is de procedure			Uitwerken in handreiking		Uitwerken in handreiking met sluitend is	
9.2.1	Registratie en afmelden van gebruikers: Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	9.2.1.2	Het gebruiken van groepsaccounts is niet toegestaan tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.	1	J		In de praktijk wel toegestaan maar zo minimaal mogelijk.		Onderhoud BIO	Gebruik groepsaccounts niet toestaan dan wel tot een minimum beperken en bij voortduring controleren/monitoren?		NOK, norm maatregel houden zoals deze is. Wat is minumum? Voorstel is noodzaak ipv minimum en logging plus controle.

Control		Overheidsmaatregel										
Nummer	Tekst	Nummer	Tekst	BBN	Opmerking categorie	Aanvullende opmerking over specifiek	Aanvullende opmerking over realistisch	Aanvullende opmerking over meetbaar	ADR suggestie	Toelichting Onderhoud BIO	Toelichting Uitwerken in handreiking/toelichting/instructie	Management reactie OK= wordt aangepast of toegelicht NOK = wordt niet aangepast of toegelicht
9.2.2	Gebruikers toegang verlenen: Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	9.2.2.1	Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris.	1	D				Geen opmerkingen		Uitwerken in handreiking	OK. Vastleggen in een toelichtend document. Toelichten dat het cruciaal is wie de bevoegden zijn. Uitwerken in bv best practices. We nemen dit mee in overwegingen in de implementatiecyclus.
9.2.2	Gebruikers toegang verlenen: Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	9.2.2.2	Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.	1	I	Wat verstaan we onder een risicoafweging? Is dit hetzelde als risico analyse?			Onderhoud BIO	Risico-analyse of risico-afweging?		NOK, algemene formulering is reeds doorgevoerd. Risico-afweging is juiste bewoording, is VIR term. Algemene formulering opstellen en daarnaar verwijzen. Moet worden vastgelegd. Volwassenheidsniveau organisatie speelt een rol.
9.2.2	Gebruikers toegang verlenen: Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	9.2.2.3	Er is een actueel mandaatregister waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten dan wel functieprofielen.	2					Geen opmerkingen			
9.2.3	Beheren van speciale toegangsrechten: Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.	9.2.3.1	De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld.	2	D	Tegen welke meetlat vindt de beoordeling plaats?		Beoordelen: Is dit inhoudelijk ernaar kijken en zichtbaar iets van vinden?	Onderhoud BIO	Beoordeeld en zonodig ingetrokken.		NOK maar wel opnemen in FAQ Beoordelen omvat ook verwijderen. Toelichten.
9.2.5	Beoordeling van toegangsrechten van gebruikers: Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	9.2.5.1	Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld.	1	D	Niet duidelijk is dat dit dan ook reactie verwacht en zichtbaarheid van deze controle		Beoordelen: Is dit inhoudelijk ernaar kijken en zichtbaar iets van vinden?	Uitwerken in handreiking	Beoordeeld en zonodig ingetrokken.		OK. Beoordelen omvat ook verwijderen. Toelichten.
9.2.5	Beoordeling van toegangsrechten van gebruikers: Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	9.2.5.2	De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident.	1	D	Wat is een beveiligingsincident.			Uitwerken in handreiking		Uitwerken definitie beveiligingsincident	
9.2.5	Beoordeling van toegangsrechten van gebruikers: Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	9.2.5.3	Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.	2	D			Beoordelen: Is dit inhoudelijk ernaar kijken en zichtbaar iets van vinden?	Uitwerken in handreiking		Uitwerken op welke wijze de beoordeling plaatsvindt.	
9.3.1	Geheime authenticatie-informatie gebruiken: Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.	9.3.1.1	Medewerkers worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordenkluis.	2					Geen opmerkingen			
9.4.1	Beperking toegang tot informatie: Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.	9.4.1.1	Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.	2	DIK	Wordt hier gedoeld op maatregelen ter voorkoming dan wel ter signalering van misbruik van de bevoegdheden door systeembeheerders?		meer een doelstelling	Onderhoud BIO	Dit is een uitkomst van de risico-analyse? Wordt gerubriceerde informatie bedoeld?	Duiden informatie met specifiek belang. Isoleren of afschermen?	NOK maar wel opnemen in FAQ Zie reactie bij 9.2.2.2 Duiden in de toelichting. Specifiek belang ruim opvatten. Betreft niet enkel bv gerubriceerde informatie maar ook privacy, commercieel vertrouwelijke informatie.
9.4.1	Beperking toegang tot informatie: Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.	9.4.1.2	Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.	2	KD	Wat is specifiek belang?		Heel brede norm. Wanneer is het voldoende	Onderhoud + handreiking	Dit is een uitkomst van de risico-analyse? Wordt gerubriceerde informatie bedoeld?	Duiden informatie met specifiek belang.	Zie 9.4.1.1
9.4.2	Beveiligde inlogprocedures: Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	9.4.2.1	Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.	1	D	Wanneer is het vertrouwd	Er zullen in de praktijk ook ander methodes worden gebruikt		Uitwerken in handreiking		Uitwerken methodes voor het verkrijgen van toegang.	
9.4.2	Beveiligde inlogprocedures: Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	9.4.2.2	Voor het verlenen van toegang tot het netwerk door externe leveranciers wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.	2	BD	Per keer toegang geven of monitoren werkzaamheden? Waarom wordt gesproken over een risico-afweging in plaats van een risico-analyse? Welke methode van risico-analyse wordt toegepast?		Is het voldoende om te zien dat in een call de toegang is verleend? Uit het wijzigingsverzoek blijkt enkel de gewenste toegangsrechten van de betreffende leverancier. Of de rechten daadwerkelijk zo zijn toegekend, blijkt uit de ingeregelde autorisaties.	Onderhoud + handreiking	Risico-afweging of risico-analyse.	Monitoren van het gebruik van de autorisaties?	Zie reactie bij 9.2.2.2

Control		Overheidsmaatregel										
Nummer	**Tekst**	**Nummer**	**Tekst**	**BBN**	**Opmerkingcategorie**	**Aanvullende opmerking over specifiek**	**Aanvullende opmerking over realistisch**	**Aanvullende opmerking over meetbaar**	**ADR suggestie**	**Toelichting Onderhoud BIO**	**Toelichting Uitwerken in handreiking/toelichting/instructie**	**Management reactie OK= wordt aangepast of toegelicht NOK = wordt niet aangepast of toegelicht**
9.4.3	Systeem voor wachtwoordbeheer: Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.	9.4.3.1	Als er geen gebruik wordt gemaakt van two factor authentication is de wachtwoordlengte minimaal 8 posities en complex van samenstelling. Vanaf een wachtwoordlengte van 20 posities vervalt de complexiteitseis. Het aantal inlogpogingen is maximaal 10. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen is vastgelegd.	1	J	Wanneer is het complex genoeg?			Uitwerken in handreiking		Best practices benoemen.	
9.4.3	Systeem voor wachtwoordbeheer: Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.	9.4.3.2	In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord vernieuwd (zie ook 9.4.2.1.).	2	J			Moet de auditor is ets zeggen of 2 factor mogelijk is? Beter om te zeggen ingericht is.	Uitwerken in handreiking		Moet de auditor controleren of 2 factor authentication mogelijk of ingericht is?	OK Constateren dat het niet mogelijk is. Vervolgens de instellingen nagaan of de procedures controleren.
9.4.3	Systeem voor wachtwoordbeheer: Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.	9.4.3.3	Het wachtwoordbeleid wordt geautomatiseerd afgedwongen.	2		Gaat het om de wachtwoord setting	Is dit altijd mogelijk?		Geen opmerkingen		Uitwerken best practices en controle.	
9.4.3	Systeem voor wachtwoordbeheer: Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.	9.4.3.4	Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van een werkdag en moeten bij het eerste gebruik worden gewijzigd.	2		Overlap met 9.4.3.3.		In sommige applicaties is dit niet goed achteraf te herleiden	Geen opmerkingen			
9.4.3	Systeem voor wachtwoordbeheer: Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.	9.4.3.5	Wachtwoorden die voldoen aan het wachtwoordbeleid hebben een maximale geldigheidsduur van een jaar. Daar waar het beleid niet toepasbaar is, geldt een maximale geldigheidsduur van 6 maanden.	2	D	Niet specifiek. Ook voor netwerkgebruikers toepasbaar?			Onderhoud BIO	Een half jaar is relatief lang. Waarom wordt niet geeist dat elk wachtwoord voldoet aan het wachtwoordbeleid?		NOK, deze maatregel eeft betrekking op bijzondere situatie waar geen beleid voor is. Oorspronkelijke tekst blijft gehandhaafd. Laatste zin weghalen.
9.4.4	Speciale systeemhulpmiddelen gebruiken: Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen behoort te worden beperkt en nauwkeurig te worden gecontroleerd.	9.4.4.1	Alleen bevoegd personeel heeft toegang tot systeemhulpmiddelen.	1	B	Wanneer is het personeel bevoegd?			Uitwerken in handreiking		Duiden speciale systeemhulpmiddelen en bevoegd personeel. In een eerste stap is belangrijk dat organisaties in kaart brengen welke beheersoftware het betreft.	
9.4.4	Speciale systeemhulpmiddelen gebruiken: Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen behoort te worden beperkt en nauwkeurig te worden gecontroleerd.	9.4.4.2	Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek.	2	D	Welke systeemmiddelen betreft het?	Soms is dit teveel om te loggen		Onderhoud + handreiking	Moet logging niet worden gecontroleerd?	Toelichten voorbeelden gebruik systeemhulpmiddelen	NOK maar wel opnemen in FAQ Het controleren van de logging is verankerd in de maatregel 9.4.4. In toelichting benadrukken dat je moet weten wat je hebt. Logging wordt vastgelegd en gecontroleerd. Een toelichting geven over de logging. Algemene constateringen. Nagaan wat dit betekent voor cloud-toepassingen. Zou vanzelfsprekend moeten zijn. In thema-uiwerkingen guidance aanpassen
10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen: Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	10.1.1.1	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: (a) wanneer cryptografie ingezet wordt; (b) wie verantwoordelijk is voor de implementatie; (c) wie verantwoordelijk is voor het sleutelbeheer; (d) welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het forum standaardisatie worden toegepast; (e) de wijze waarop het beschermingsniveau vastgesteld wordt; (f) bij inter-organisatie communicatie wordt het beleid onderling vastgesteld.	2	J	Wie stelt het beleid vast			Uitwerken in handreiking		Toelichten wie beleid vaststelt.	
10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen: Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	10.1.1.2	Crypografische toepassingen voldoen aan passende standaarden.	2	B	Wat zijn passende standaarden?			Uitwerken in handreiking		Wat wordt bedoeld met passende standaarden? Uitwerken op welke wijze deze norm kan worden getoetst.	

Control		Overheidsmaatregel										
Nummer	Tekst	Nummer	Tekst	BBN	Opmerking categ...	Aanvullende opmerking over specifiek	Aanvullende opmerking over realistisch	Aanvullende opmerking over meetbaar	ADR suggestie	Toelichting Onderhoud BIO	Toelichting Uitwerken in handreiking/toelichting/instructie	Management reactie OK= wordt aangepast of toegelicht NOK = wordt niet aangepast of toegelicht
10.1.2	Sleutelbeheer: Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld en geïmplementeerd.	10.1.2.1	Ingeval van PKI-overheid certificaten: hanteer de PKI-Overheid-eisen t.a.v. het sleutelbeheer. In overige situaties: hanteer de standaard ISO-11770 voor het beheer van cryptografische sleutels.	2	A	verwijst naar andere standaarden		Het meten van deze norm is omvangrijk omdat toetsen op alle eisen omvangrijk kan zijn.	Uitwerken in handreiking		Uitwerken van de toetselementen.	
10.1.2	Sleutelbeheer: Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld en geïmplementeerd.	10.1.2.2	Er zijn (contractuele) afspraken over reservecertificaten van een alternatieve leverancier als uit risicoafweging blijkt dat deze noodzakelijk zijn.	2	BI	Uitkomst van risico-analyse			Onderhoud BIO	Dit is een uitkomst van de risico-analyse. Risico-afweging of risico-analyse?		Zie reactie bij 9.2.2.2
11.1.1	Fysieke beveiligingszone: Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.	11.1.1.1	Er wordt voor het inrichten van beveiligde zones gebruik gemaakt van standaarden.	1	A	Welke type standaarden wordt gedoeld? Zijn dat standaarden die een organisatie zelf heeft gedefinieerd? Of door een derde partij?		Verwijzingen naar andere onderliggende normkaders maakt deze normtekst omvangrijk om te controleren.	Uitwerken in handreiking		Uitwerken welke type standaarden worden bedoeld en best practices benoemen.	
11.1.2	Fysieke toegangsbeveiliging: Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	11.1.2.1	In geval van concrete beveiligingsrisico's worden waarschuwingen, conform onderlinge afspraken, verzonden aan de relevante collega's binnen het beveiligingsdomein van de overheid.	2	D	Veel nader te duiden begrippen. Wat zijn relevante collega's?			Uitwerken in handreiking		Duiden beveiligingsrisico's, relevante collega's en beveiligingsdomein overheid.	
11.1.3	Kantoren, ruimten en faciliteiten beveiligen: Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.	11.1.3.1	Sleutelbeheer is ingericht op basis van een sleutelplan.	1								
11.1.4	Beschermen tegen bedreigingen van buitenaf: Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.	11.1.4.1	De organisatie heeft geïnventariseerd welke papieren archieven en apparatuur bedrijfskritisch zijn. Tegen bedreigingen van buitenaf zijn beveiligingsmaatregelen genomen op basis van een expliciete risicoafweging.	1	I	Uitkomst van risico-analyse			Onderhoud BIO	Dit is een uitkomst van de risico-analyse. Risico-afweging of risico-analyse? Gaat het om bedrijfskritisch zijn van apparatuur of archieven of gaat het om informatieveiligheid/rubricering?		NOK maar wel opnemen in FAQ Zie reactie bij 9.2.2.2 Is onderdeel van het thema fysieke beveiliging waar duiding wordt gegeven.
11.1.4	Beschermen tegen bedreigingen van buitenaf: Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.	11.1.4.2	Bij huisvesting van IT-apparatuur wordt rekening gehouden met de kans op gevolgen van rampen veroorzaakt door de natuur en menselijk handelen.	1	B			Rekening houden met is niet specifiek. Er moet een contingency plan zijn	Onderhoud + handreiking	Toespitsen op informatieveiligheid?	Uitwerken welke toetselementen er zijn in BCP.	Zie voorgaande opmerking
11.2.9	'Clear desk'- en 'clear screen'-beleid: Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten te worden ingesteld.	11.2.9.1	Een onbeheerde werkplek in een ongecontroleerde omgeving is altijd vergrendeld.	2	C			We kunnen alleen het beleid vaststellen en een waarneming ter plaatse doen	Uitwerken in handreiking		Uitwerken toetselementen	
11.2.9	'Clear desk'- en 'clear screen'-beleid: Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten te worden ingesteld.	11.2.9.2	Informatie wordt automatisch ontoegankelijk gemaakt met bijvoorbeeld een screensaver na een inactiviteit van maximaal 15 minuten.	2	CE		In de praktijk zijn uitzonderingen gewenst		Uitwerken in handreiking		Uitwerken uitzonderingen	
11.2.9	'Clear desk'- en 'clear screen'-beleid: Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten te worden ingesteld.	11.2.9.3	Sessies op remote desktops worden op het remote platform vergrendeld na 15 minuten. Het overnemen van sessies op remote desktops op een ander client apparaat is alleen mogelijk via dezelfde beveiligde loginprocedure als waarmee de sessie is gecreëerd.	2	B		Het is de vraag of het nodig is om een minimum norm te noemen op dit terrein. 15 minuten is zeer ruim en de norm in het veld is korter.		Onderhoud BIO	15 minuten is ruim		NOK
11.2.9	'Clear desk'- en 'clear screen'-beleid: Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten te worden ingesteld.	11.2.9.4	Bij het gebruik van een chipcardtoken voor toegang tot systemen wordt bij het verwijderen van de token de toegangsbeveiligingslock automatisch geactiveerd.	2					Geen opmerkingen			
12.1.2	Wijzigingsbeheer: Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.	12.1.2.1	In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan: (a) het administreren van wijzigingen; (b) risicoafweging van mogelijke gevolgen van de wijzigingen; (c) goedkeuringsprocedure voor wijzigingen.	1	J				Geen opmerkingen			

Control		Overheidsmaatregel										
Nummer	**Tekst**	**Nummer**	**Tekst**	**BBN**	**Opmerking categorie**	**Aanvullende opmerking over specifiek**	**Aanvullende opmerking over realistisch**	**Aanvullende opmerking over meetbaar**	**ADR suggestie**	**Toelichting Onderhoud BIO**	**Toelichting Uitwerken in handreiking/toelichting/instructie**	**Management reactie OK= wordt aangepast of toegelicht NOK = wordt niet aangepast of toegelicht**
12.1.3	Capaciteitsbeheer: Het gebruik van middelen behoort te worden gemonitord en afgestemd, en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.	12.1.3.1	In koppelpunten met externe of onvertrouwde zones zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden (bijv. DDoS attacks, Distributed Denial of Service) te signaleren en hierop te reageren.	1	DI	Wat is onvertrouwde zone?		Verwijst naar risicoanalyse	Onderhoud + handreiking	Verwijst naar risico-analyse	Toelichten onvertrouwde zone	NOK maar wel opnemen in FAQ
12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen: Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	12.1.4.1	In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hierop worden afgeweken.	2					Geen opmerkingen		Uitzonderingen duiden in de handreiking.	
12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen: Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	12.1.4.2	Wijzigingen op de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hierop worden afgeweken.	2	D		Vaak zal in een noodsituatie de goedkeuring achteraf plaatsvinden		Uitwerken in handreiking		Uitzonderingen duiden in de handreiking.	
12.2.1	Beheersmaatregelen tegen malware: Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	12.2.1.1	Het downloaden van bestanden is beheerst en beperkt op basis van risico en need-of-use.	1	D	Wat is beheerst?			Uitwerken in handreiking		Toetselementen benoemen die de omgeving beheerst maken	
12.2.1	Beheersmaatregelen tegen malware: Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	12.2.1.2	Gebruikers zijn voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende linken.	1	J			Is deze maatregel meetbaar? Gebruikers kunnen worden voorgelicht en moeten bevestigen dat zij de gedragsregels naleven. Mag het surf-/downloadgedrag preventief worden gemonitord?	Uitwerken in handreiking		Toetselementen benoemen	
12.2.1	Beheersmaatregelen tegen malware: Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	12.2.1.3	Software en bijbehorende herstelsoftware die malware opspoort zijn geïnstalleerd en worden regelmatig geüpdatet.	1	D		Dit moet toch zeer actueel zijn?		Onderhoud BIO	Vervang tekst door actueel zijn		OK
12.2.1	Beheersmaatregelen tegen malware: Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	12.2.1.4	Computers en media worden als voorzorgsmaatregel routinematig gescand. De uitgevoerde scan behoort te omvatten: (a) alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware scannen; (b) bijlagen en downloads vóór gebruik.	1	B			Volgens afgesproken frequentie gescand?	Uitwerken in handreiking		frequentie uitwerken in handreiking.	OK. Het moet in een routine zitten. Moet een standaardprocedure zjn en daarmee frequent. Onderdeel van toelichtng, verwijzen naar thema's.
12.2.1	Beheersmaatregelen tegen malware: Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	12.2.1.5	De malware scan wordt op verschillende omgevingen uitgevoerd, bijv. op mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie.	1	D	Alle omgevingen?		Er worden geen eisen gesteld aan de malware scans	Onderhoud + Handreiking	Verschillende omgevingen nader duiden	Eisen stellen aan de malwarescans (waarop moet worden gesand?) Worden de uitkomsten beoordeeld en bewaard?	OK Norm wordt aangepast. Malwarescanning moet op alle omgevingen worden geplaatst. Daar waar relevant is, bij zonering.
12.3.1	Back-up van informatie: Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	12.3.1.1	Er is een back-up beleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld.	1					Geen opmerkingen			
12.3.1	Back-up van informatie: Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	12.3.1.2	Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.	1	DI	Geldt dit voor alle data? Of wordt onderscheid gemaakt in categorieën data? Wat wordt bedoeld met risico-afweging?		Wordt data ingedeeld in categorieën?	Onderhoud + Handreiking	Verwijst naar risicoanalyses	Uitwerken dat data kan worden ingedeeld in categorieën als onderdeel van de risico-analyse.	Zie reactie bij 9.2.2.2
12.3.1	Back-up van informatie: Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	12.3.1.3	In het back-up beleid staan minimaal de volgende eisen: (a) dataverlies bedraagt maximaal 28 uur; (b) hersteltijd in geval van incidenten is maximaal 16 werkuren (2 dagen van 8 uur) in 85% van de gevallen.	2					Geen opmerkingen	(dit punt zou ook met risicoanalyse verder vorm gegeven kunnen worden)		
12.3.1	Back-up van informatie: Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	12.3.1.4	Het back-up proces voorziet in opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere.	2					Geen opmerkingen			

Control		Overheidsmaatregel										
Nummer	**Tekst**	**Nummer**	**Tekst**	**BBN**	**Opmerking categorie**	**Aanvullende opmerking over specifiek**	**Aanvullende opmerking over realistisch**	**Aanvullende opmerking over meetbaar**	**ADR suggestie**	**Toelichting Onderhoud BIO**	**Toelichting Uitwerken in handreiking/toelichting/instructie**	**Management reactie OK= wordt aangepast of toegelicht NOK = wordt niet aangepast of toegelicht**
12.3.1	Back-up van informatie: Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	12.3.1.5	De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de betrouwbaarheid te waarborgen als ze in noodgevallen uitgevoerd moet worden.	2	D			Wat wordt bedoeld met betrouwbaarheid?	Onderhoud BIO	Ipv betrouwbaarheid werking procedure waarborgen		OK
12.4.1	Gebeurtenissen registreren: Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	12.4.1.1	Een logregel bevat minimaal de gebeurtenis; de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; het gebruikte apparaat; het resultaat van de handeling; een datum en tijdstip van de gebeurtenis.	1	B			"hoge mate van zekerheid" is toetsmethode.	Uitwerken in handreiking		Hoge mate van zekerheid duiden.	
12.4.1	Gebeurtenissen registreren: Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	12.4.1.2	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	1	D				Uitwerken in handreiking		Voorbeelden van onnodige gegevens vastgelegd zoals wachtwoorden. Geldt dit ook voor privacygevoelige gegevens?	Ok. In een toelichting voorbeelden geven.
12.4.1	Gebeurtenissen registreren: Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	12.4.1.3	De informatieverwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectie-voorzieningen, zoals het Nationaal Detectie Netwerk, die worden ingezet op basis van een risico-inschatting, mede aan de hand van en de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.	2	I	Waarom wordt gesproken over risico-inschatting en elders over risico-afweging? Waarom niet over het uitvoeren van risicoanalyse? Op basis van een risico inschatting is een meta norm.			Onderhoud BIO	Risico-inschatting en risico-afweging worden door elkaar gebruikt. Wordt bedoeld de uitkomsten van de risico-analyse?	De toetselementen in deze norm nader toelichten.	Zie reactie bij 9.2.2.2
12.4.1	Gebeurtenissen registreren: Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	12.4.1.4	Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of via de sectorale CERT (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen.	2	AB	Hiervoor is juridische kennis dan wel inzet van een jurist benodigd. Welke informatie gedeeld moet worden met wie is achteraf moeilijk te toetsen.		Het is een onderzoek an sich om vast te stellen welke juridische kaders van toepassing zijn. Bij voorkeur is lastig vast te stellen.	Uitwerken in handreiking		Uitwerken op welke wijze juridische kaders getoetst worden.	
12.4.1	Gebeurtenissen registreren: Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden	12.4.1.5	De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	2	C	"helder" is voor meerdere uitleg vatbaar			Uitwerken in handreiking		Voorbeelden van procedures en regels SIEM rapporteert niet zelf aan MT.	
12.4.2	Beschermen van informatie in logbestanden: Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	12.4.2.1	Er is een overzicht van logbestanden die worden gegenereerd.	1	K	Feitelijk is dit een randvoorwaarde, geen control.	Logbestanden worden vaak samengebracht in een centrale voorziening (datawarehouse). Een overzicht hiervan maken heeft geen toegevoegde waarde.		Onderhoud BIO	Gegenereert en geanalyseerd		NOK, het analyseren valt niet onder deze maatregel. OK, moet een aparte maatregel worden.
12.4.2	Beschermen van informatie in logbestanden: Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	12.4.2.2	Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.	1	I	Wat wordt bedoeld met risicoafweging? Is loginformatie gelijk aan logging? Is het voldoende als er een beleidsstuk is? Wat is expliciet?			Onderhoud BIO	Uniformiteit in terminologie risico-afweging, risico-analyse, logging, loginformatie ontbreekt.		Zie reactie bij 9.2.2.2
12.4.2	Beschermen van informatie in logbestanden: Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	12.4.2.3	Er is een (onafhankelijke) interne audit procedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden.	2	J	Zie de opmerking bij 12.4.2.1. Een best practice is hier dat modificatie van logbestanden in de bronsystemen als optie is uitgezet of zelfs niet mogelijk is. In het logging datawarehouse is toegang tot de logging beveiligd. Modificatie kan niet en het weggooien wordt opgemerkt doordat er gaten in de logging zichtbaar worden.		Soms is dit niet te achterhalen.	Onderhoud BIO	Bv toetsen dat de organisatie twee keer per jaar vaststelt dat de logbestanden niet zijn aangepast. Norm lijkt te suggereren dat je alleen een procedure moet hebben. Niet dat het wordt getoetst.		NOK - als er een procedure is, zal deze ook uitgevoerd worden.
12.4.2	Beschermen van informatie in logbestanden: Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	12.4.2.4	Oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten conform hoofdstuk 16.	2	AB		Het is de vraag of oneigenlijk wijzigen van logbestanden (altijd) kan worden vastgesteld.		Uitwerken in handreiking		Voorbeelden van oneigelijk wijzigen en hoe dat kan worden vastgesteld.	

Control		Overheidsmaatregel										
Nummer	**Tekst**	**Nummer**	**Tekst**	**BBN**	**Opmerking categorie**	**Aanvullende opmerking over specifiek**	**Aanvullende opmerking over realistisch**	**Aanvullende opmerking over meetbaar**	**ADR suggestie**	**Toelichting Onderhoud BIO**	**Toelichting Uitwerken in handreiking/toelichting/instructie**	**Management reactie OK= wordt aangepast of toegelicht NOK = wordt niet aangepast of toegelicht**
12.6.1	Beheer van technische kwetsbaarheden: Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.	12.6.1.1	Als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC classificatie kwetsbaarheidswaarschuwingen), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.	1	DI	Norm verwijst naar risicoafweging		Hoe stel je de kans op misbruik vast?	Onderhoud + Handreiking	Uniformiteit in terminilogie risico-afweging, risico-analyse ontbreekt.	Toelichten dat de werkwijze moet zijn vastgelegd in een procedure en duiden hoe de kans op misbruik kan worden vastgesteld.	Zie reactie bij 9.2.2.2
12.6.2	Beperkingen voor het installeren van software: Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.	12.6.2.1	Gebruikers kunnen op hun werkomgeving niets zelf installeren, anders dan via de ICT-leverancier wordt aangeboden of wordt toegestaan (whitelist).	2	K				Geen opmerkingen	(Maatregel voegt weinig toe aan de doelstelling)		NOK. Norm handhaven. Maatregel voegt whitelisting toe.
13.1.2	Beveiliging van netwerkdiensten: Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	13.1.2.1	Het dataverkeer dat de organisatie binnenkomt of uitgaat wordt bewaakt / geanalyseerd op kwaadaardige elementen middels detectie-voorzieningen (zoals beschreven in de richtlijn voor implementatie van detectie-oplossingen), zoals het Nationaal Detectie Netwerk, die worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen.	2	ID	Wordt verwezen naar andere richtlijn. Waarom wordt gesproken over risico-inschatting en elders over risico-afweging? Waarom niet over het uitvoeren van risicoanalyse? Op basis van een risico inschatting is een meta norm.	Wordt uitgaand verkeer vaak gescand?	Dataverkeer kan versleuteld zijn en het kan zijn dat het niet mag of kan worden versleuteld.	Onderhoud + Handreiking	Norm is onduidelijk. Risico-inschatting en risico-afweging worden door elkaar gebruikt. Wordt bedoeld de uitkomsten van de risico-analyse?	Duiden op welke wijze deze norm moet worden getoetst.	NOK. Zie reactie bij 9.2.2.2
13.1.2	Beveiliging van netwerkdiensten: Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	13.1.2.2	Bij ontdekte nieuwe dreigingen vanuit 13.1.2.1 worden deze, rekening houdend met de geldende juridische kaders, verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT, bij voorkeur door geautomatiseerde mechanismen (threat intelligence sharing).	2	AD	Wat zijn threat intelligence sharing mechanismen?	De toetsing van deze norm door auditors is moeilijk. Hoe weet je of er sprake was van nieuwe dreigingen die doorgegeven hadden moeten worden?		Uitwerken in handreiking		Duiden wanneer het voldoende gedeeld wordt.	
13.1.2	Beveiliging van netwerkdiensten: Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	13.1.2.3	Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied, wordt gebruik gemaakt van encryptie middelen waarvoor het NBV een positief inzetadvies heeft afgegeven.	2	AB	Gecontroleerd gebied kan verschillend geintepreteerd worden	Toegang tot alle adviezen NBV is niet eenvoudig	Wat is gecontroleerd gebied? En welke eisen worden gesteld op koppelvlakken van ongecontroleerd naar gecontroleerd?	Uitwerken in handreiking		Duiden wat met gecontroleerd gebied wordt bedoeld.	
13.1.3	Scheiding in netwerken: Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.	13.1.3.1	Alle gescheiden groepen hebben een gedefinieerd beveiligingsniveau.	2	K				Geen opmerkingen	O-norm voegt niet veel toe aan doelstelling		NOK. Norm handhaven
13.2.3	Elektronische berichten: Informatie die is opgenomen in elektronische berichten behoord passend te zijn beschermd.	13.2.3.1	Voor de beveiliging van elektronische berichten gelden de vastgestelde standaarden tegen phishing en afluisteren op pas-toe-of-leg-uit lijst van het forum standaardisatie.	1	DE	Het onderscheid tussen deze norm en 13.2.3.2 is niet scherp. Wat zijn vastgestelde standaarden?	De term 'elektronische berichten' is verouderd en niet specifiek genoeg. Worden e-mail berichten bedoeld?	Phishing als aanvalstechniek richt zich op het misleiden van eindgebruikers. Is beveiliging van elektronische berichten een passende maatregel tegen phising?	Uitwerken in handreiking		Duiden op welke wijze deze norm moet worden getoetst.	
13.2.3	Elektronische berichten: Informatie die is opgenomen in elektronische berichten behoord passend te zijn beschermd.	13.2.3.2	Voor veilige berichtenuitwisseling met basisregistraties, wordt conform de pas-toe-leg-uit-lijst, gebruik gemaakt van de actuele versie van Digikoppeling	2	AB	Waarom wordt Digikoppeling in de norm genoemd? Dit kan applicatiegebonden zijn. Wat is de maatregel in de Digikoppeling?			Geen opmerkingen			
13.2.3	Elektronische berichten: Informatie die is opgenomen in elektronische berichten behoord passend te zijn beschermd.	13.2.3.3	Maak gebruik van PKI-Overheid certificaten bij web- en mailverkeer van gevoelige gegevens. Gevoelige gegevens zijn o.a. digitale documenten binnen de Rijksdienst waar gebruikers rechten aan kunnen ontlenen.	2	D	Wat zijn gevoelige gegevens? Is een definitie voor handen?			Uitwerken in handreiking	Gevoelige gegevens of gerubriceerde gegevens?	Gevoelige gegevens duiden. Wat voor soort gegevens moeten via PKI certificaat worden geduid.	

Control		Overheidsmaatregel										
Nummer	Tekst	Nummer	Tekst	BBN	Opmerking categ...	Aanvullende opmerking over specifiek	Aanvullende opmerking over realistisch	Aanvullende opmerking over meetbaar	ADR suggestie	Toelichting Onderhoud BIO	Toelichting Uitwerken in handreiking/toelichting/instructie	Management reactie OK= wordt aangepast of toegelicht NOK = wordt niet aangepast of toegelicht
13.2.3	Elektronische berichten: Informatie die is opgenomen in elektronische berichten behoord passend te zijn beschermd.	13.2.3.4	Om zekerheid te bieden over de integriteit van het elektronische bericht wordt voor elektronische handtekeningen gebruik gemaakt van de AdES Baseline Profile standaard of de of de ETSI TS 102 176-1	2	D	Wat is zekerheid bieden?			Onderhoud BIO	Zekerheid vervangen door waarborgen?		OK Zekerheid vervangen door waarborgen in de norm.
14.1.1	Analyse en specificatie van informatiebeveiligingseisen: De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	14.1.1.1	Bij nieuwe informatiesystemen en bij wijzigingen op bestaande informatiesystemen moet een expliciete risicoafweging worden uitgevoerd ten behoeve van het vaststellen van de beveiligingseisen, uitgaande van de BIO.	1	BI	Waarom wordt gesproken over risico-afweging? Waarom niet over het uitvoeren van risicoanalyse? Op basis van een risico afweging is een meta norm.			Onderhoud BIO	Risico-analyse en risico-afweging worden door elkaar gebruikt. Wordt bedoeld de uitkomsten van de risico-analyse?		Zie reactie bij 9.2.2.2
14.2.1	Beleid voor beveiligd ontwikkelen: Voor het ontwikkelen van software en systemen behoren regels te worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie te worden toegepast.	14.2.1.1	De gangbare principes rondom Security by design zijn uitgangspunt voor de ontwikkeling van software en systemen	1	BI	Is security inclusief privacy?		Wat zijn gangbare principes?	Uitwerken in handreiking		Toelichten gangbare principes	
14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen: Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.	14.2.2.1	Voor het wijzigingsbeheer gelden de algemeen geaccepteerde beheerframeworks, zoals ITIL, ASL of BiSL.	1	ADE	Wat is gelden? "afgeleid zijn van?" Het verwijzen naar ander standaarden is lastig. Moeten deze standaarden altijd en volledig zijn geïmplementeerd? ASL, ITIL en BiSL vuilen elkaar aan.			Uitwerken in handreiking	Het gaat om het op een beheerste wijze doorvoeren van wijzigingen. Is het realistisch te verwachten dat elke overheidsorganisatie ITIL, ASL of BiSL volledig invoert?	Toelichten wanneer aan de norm wordt voldaan.	NOK. Kijk kritisch naar beheer en zorg dat je een framework/standaard. Zo laten staan.
14.2.5	Principes voor engineering van beveiligde systemen: Principes voor de engineering van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.	14.2.5.1	Zie overheidsmaatregel 14.2.1.1	1	AD	Wat wordt bedoeld met engineering?			Uitwerken in handreiking	Waarom verwijzing opnemen naar andere maatregel?	Engineering duiden, definitie opnemen.	NOK. Laten staan, wellicht in volgende versie weghalen.
14.2.6	Beveiligde ontwikkelomgeving: Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de	14.2.6.1	Uitgangspunt voor systeemontwikkeltrajecten is een expliciete risicoafweging. Deze heeft zowel de ontwikkelomgeving als ook het te ontwikkelen systeem in scope.	1	I	Wederom het gebruik van het begrip 'expliciete risico afweging'. Wordt hier risico-analyse bedoeld? Verwijzen naar risicoafweging is meta niveau.		Risico-analyse vormt het uitgangspunt van de BIO.	Onderhoud BIO	Risico-analyse vormt het uitgangspunt van de BIO.		Zie reactie bij 9.2.2.2
14.2.7	Uitbestede softwareontwikkeling: Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie.	14.2.7.1	Een voorwaarde voor uitbestedingstrajecten is een expliciete risicoafweging. De noodzakelijke beveiligingsmaatregelen die daaruit volgen worden aan de leverancier opgelegd.	1	I	Wederom het gebruik van het begrip 'expliciete risico afweging'. Wordt hier risico-analyse bedoeld? Verwijzen naar risicoafweging is meta niveau.	Dit betreft mogelijk een beheersmaatregel in het inkoopproces. Op welke wijze wordt deze overlap met het inkoopproces geborgd?		Onderhoud BIO	In BIO zelf staat dat je met leveranciers afspraken moet maken. Risico-analyse vormt het uitgangspunt van de BIO.		Zie reactie bij 9.2.2.2
14.2.9	Systeemacceptatietests: Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.	14.2.9.1	Voor acceptatietesten van systemen worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.	1	J			In nieuwe ontwikkelmethoden zoals Agile en Scrum is de structuur minder of niet gedocumenteerd. Dit zal deze normtekst naar de toekomst toe steeds moeilijker meetbaar	Uitwerken in handreiking		Beschrijf op welke wijze deze norm kan worden getoetst als methoden zoals Agile en Scrum worden gebruikt.	
14.2.9	Systeemacceptatietests: Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.	14.2.9.2	Van de resultaten van de testen wordt verslag gemaakt.	1	J	Een verslag opstellen op zich is geen control. Eerder een randvoorwaarde voor een control.		In nieuwe ontwikkelmethoden zoals Agile en Scrum is de structuur minder of niet gedocumenteerd. Dit zal deze normtekst naar de toekomst toe steeds moeilijker meetbaar	Uitwerken in handreiking		Beschrijf op welke wijze deze norm kan worden getoetst als methoden zoals Agile en Scrum worden gebruikt. Toetselementen testverslag vaststellen.	
15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties: Met de leverancier behoren de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, te worden overeengekomen en gedocumenteerd.	15.1.1.1	Bij offerteaanvragen waar informatie(voorziening) een rol speelt, worden eisen t.a.v. informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) benoemd. Deze eisen zijn gebaseerd op een expliciete risicoafweging.	1	DI	Wederom het gebruik van het begrip 'expliciete risico afweging'. Wordt hier risico-analyse bedoeld? Verwijzen naar risicoafweging is meta niveau. Wanneer is het voldoende?			Onderhoud + Handreiking	Risico-analyse vormt het uitgangspunt van de BIO.	Beschrijf de samenhang of overlap met 15.1.1.2	Zie 9.2.2.2
15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties: Met de leverancier behoren de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, te worden overeengekomen en gedocumenteerd.	15.1.1.2	Op basis van een expliciete risicoafweging worden de beheersmaatregelen met betrekken tot leverancierstoegang tot bedrijfsinformatie vastgesteld.	2	DI	Wederom het gebruik van het begrip 'expliciete risico afweging'. Wordt hier risico-analyse bedoeld? Verwijzen naar risicoafweging is meta niveau. Wanneer is het voldoende? Is er een overlap of samenhang met 15.1.1.1?			Onderhoud + Handreiking	Risico-analyse vormt het uitgangspunt van de BIO.	Beschrijf de samenhang of overlap met 15.1.1.1.	Zie 9.2.2.2

Control		Overheidsmaatregel										
Nummer	Tekst	Nummer	Tekst	BBN	Opmerking categ...	Aanvullende opmerking over specifiek	Aanvullende opmerking over realistisch	Aanvullende opmerking over meetbaar	ADR suggestie	Toelichting Onderhoud BIO	Toelichting Uitwerken in handreiking/toelichting/instructie	Management reactie OK= wordt aangepast of toegelicht NOK = wordt niet aangepast of toegelicht
15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties: Met de leverancier behoren de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, te worden overeengekomen en gedocumenteerd.	15.1.1.3	Met alle leveranciers die als verwerker voor of namens de organisatie persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld.	2	H	Dit is toch de wet? Moet dit in de BIO? Waarom slechts enkele elementen van de AVG noemen?	AVG compliancy is een onderzoek op zich.	Geen inhoudelijk onderzoek verwerkerovereenkomsten?	Uitwerken in handreiking		Toelichten waarom één onderdeel van de AVG moet worden onderzocht. Toelcihten dat gebruik kan worden gemaakt van compliancy audits als deze zijn uitgevoerd.	
15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten: Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	15.1.2.1	De beveiligingseisen uit de offerteaanvraag worden expliciet opgenomen in de (inkoop)contracten waar informatie een rol speelt.	1					Geen opmerkingen			
15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten: Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	15.1.2.2	In de inkoopcontracten worden expliciet prestatie-indicatoren en de bijbehorende verantwoordingsrapportages opgenomen.	1	H	Is dit een inkoopmaatregel?		Dient de auditor enkel vast te stellen dat de prestatie-indicatoren worden opgenomen of dienen de prestatie-indicatoren ook inhoudelijk te worden getoetst?	Uitwerken in handreiking		Toelichten of de auditor enkel moet toetsen dat prestatie-indicatoren zijn opgenomen in de inkoopcontracten of dat ook een inhoudelijke toets op de prestatie-indicatoren moet plaatsvinden.	Wordt opgevolgd
15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten: Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	15.1.2.3	In situaties waarin contractvoorwaarden worden opgelegd door leveranciers, is voorafgaand aan het tekenen van het contract met een risicoafweging helder gemaakt wat de consequenties hiervan zijn voor de organisatie. Expliciet is gemaakt welke consequenties geaccepteerd worden en welke gemitigeerd moeten zijn bij het aangaan van de overeenkomst.	1	HI	Is dit een inkoopmaatregel? Wederom het gebruik van het begrip 'risico afweging'. Wordt hier risico-analyse bedoeld? Verwijzen naar risicoafweging is meta niveau.			Onderhoud BIO	Risico-analyse vormt het uitgangspunt van de BIO.		Zie 9.2.2.2
15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten: Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	15.1.2.4	Ter waarborging van vertrouwelijkheid of geheimhouding worden bij IT-inkopen standaard voorwaarden voor inkoop gehanteerd.	1	H	Is dit een inkoopmaatregel?		Welke standaardvoorwaarden zijn er?	Uitwerken in handreiking		Duiden welke standaardvoorwaarden er zijn.	
15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten: Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	15.1.2.5	Voordat een contract wordt afgesloten wordt in een risicoafweging bepaald of de afhankelijkheid van een leverancier beheersbaar is. Een vast onderdeel van het contract is een expliciete uitwerking van de exit-strategie.	2	H	Is dit een inkoopmaatregel? Wederom het gebruik van het begrip 'risico afweging'. Wordt hier risico-analyse bedoeld? Verwijzen naar risicoafweging is meta niveau.		Beheersbaar lastig te toetse	Onderhoud + Handreiking	Risico-analyse vormt het uitgangspunt van de BIO. Is de tweede zin niet voldoende?	Toelichten wat in de risicoanalyse moet worden vastgelegd.	Zie 9.2.2.2
15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten: Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	15.1.2.6	In inkoopcontracten wordt expliciet de mogelijkheid van een externe audit opgenomen waarmee de betrouwbaarheid van de geleverde dienst kan worden getoetst. Een audit is niet nodig als de contractant d.m.v. certificering aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd.	2	BDI		Ook als een certificaat beschikbaar is kan het nodig zijn een audit uit te laten voeren.	Wat is de betrouwbaarheid van de geleverde dienst?	Onderhoud BIO	In contracten altijd afspraken maken over het 'right to audit'. Bv ISO certificeringen voldoen niet aan de internationele audit standaarden. Daarnaast kan de scope van een certificaat of auditrapport sterk verschillen met de benodigde informatie.		NOK maar wel opnemen in FAQ Wordt dit altijd door de leverancier geaccepteerd? Moet strakker worden geformuleerd. Toelichting op geven in handreiking. Leverancier moet op onafhankelijke wijze moet aantonen dat aan de normen wordt voldaan. Onafhankelijke aantoonbaarheid. Altijd afspraken maken over het 'right to audit'.
15.1.3	Toeleveringsketen van informatie- en communicatietechnologie: Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.	15.1.3.1	Leveranciers moeten hun keten van toeleveranciers bekend maken en transparant zijn over de maatregelen die zij genomen hebben om de aan hun opgelegde eisen ook door te vertalen naar hun toeleveranciers.	2	BI	Hoe vaak moet dit worden geactualiseerd? Actualiteit van de informatie moet zijn geborgd. Dus aangeven op welk moment de overzichten worden bijgesteld		Moeilijk/niet meetbaar met name doordat niet duidelijk is op welke wijze beveiligingsmaatregelen in de keten worden gecommuniceerd en getoetst op de naleving ervan. Dient de auditor bij een leverancier de naleving van maatregelen vast te stellen?	Onderhoud + Handreiking	Ketenverantwoordelijkheid en risico analyse breder uitwerken dan in maatregel.	Toelichten uit welke toetselementen de toets moet bestaan.	OK Ook toeleveranciers moeten aan jouw eisen in continuiteit blijven voldoen. In de contracten voorwaarden stellen aan de dienstverlening. De leveranciers moeten ook aantonen dat aan de maatregelen wordt voldaan en leveranciers moeten dat inzichtelijk maken. Primair is de contractpartij verantwoordelijk.
15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers: Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.	15.2.1.1	Jaarlijks wordt de prestatie van leveranciers op het gebied van informatiebeveiliging beoordeeld op vooraf vastgestelde prestatie-indicatoren, zoals in het contract opgenomen is.	2	E	Wat is de samenhang met norm 15.1.2.2? Wie bepaalt de prestatie-indicatoren en de vereiste waarde ervan? Wie is verantwoordelijk voor de meting van deze indicatoren?		De meetbaarheid is afhankelijk van de definitie van de indicatoren en de afspraken die zijn gemaakt over het rapporteren en de controle op de rapportage. Of is het de bedoeling om enkel vast te stellen dat het contract prestatie-indicatoren bevat?	Uitwerken in handreiking		Samenhang met norm 15.1.2.2 beschrijven. Toelichten of enkel dient te worden vastgesteld dat wordt gerapporteerd over prestatie-indicatoren of moet een inhoudelijke toets op de rapportage plaatsvinden?	

Control		Overheidsmaatregel										
Nummer	Tekst	Nummer	Tekst	BBN	Opmerking categorie	Aanvullende opmerking over specifiek	Aanvullende opmerking over realistisch	Aanvullende opmerking over meetbaar	ADR suggestie	Toelichting Onderhoud BIO	Toelichting Uitwerken in handreiking/toelichting/instructie	Management reactie OK= wordt aangepast of toegelicht NOK = wordt niet aangepast of toegelicht
16.1.1	Verantwoordelijkheden en procedures: Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	1		1								
16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen: Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	16.1.2.1	Er is een meldloket waar beveiligingsincidenten kunnen worden gemeld.	1	E	Wat zijn de eisen aan registraties van meldingen?			Uitwerken in handreiking		Voorbeelden registraties en hanteren classificatietoekenning.	OK. Norm bezien in combinatie met andere normen onder 16
16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen: Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	16.1.2.2	Er is een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.	1	D	Welke taken en verantwoordelijkheiden worden minimaal verwacht			Uitwerken in handreiking		Voorbeelden taken en verantwoordelijkheden van security officers en hun rol in de meldprocedures.	
16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen: Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	16.1.2.3	Alle medewerkers en contractanten hebben aantoonbaar kennis genomen van de meldingsprocedure van incidenten.	1	B		Alle is 100%.	Kennis nemen hoeft niet gedocumenteerd te zijn.	Uitwerken in handreiking	Wellicht alle weglaten?	"Kennis nemen" uitwerken in voorbeelden.	OK. Norm handhaven. In best practices toelichting geven op'alle' . Waarom moeten alle medewerkers deze kennis hebben.
16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen: Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	16.1.2.4	Incidenten worden zo snel als mogelijk, maar in ieder geval binnen 24 uur na bekendwording, gemeld bij het meldloket.	1	B			Zie opmerking bij 16.1.2.1. Auditor gaat uit van de informatie die al gemeld is.	Uitwerken in handreiking		Handreiking hoe de volledigheid van de meldingen kan worden gecontroleerd.	
16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen: Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	16.1.2.5	De proceseigenaar is verantwoordelijk voor het oplossen van beveiligingsincidenten.	1	K	Wat voegt deze maatregel toe aan de norm? Moet dit in een procedure staan?	In de praktijk is dit vaak lastig zichtbaar.		Uitwerken in handreiking		Voorbeelden van de wijze waarop dit belegd kan worden en hoe de proceseigenaar invulling kan geven aan deze verantwoordelijkheid.	
16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen: Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	16.1.2.6	De opvolging van incidenten wordt maandelijks gerapporteerd aan de verantwoordelijke.	1	B	Het lijkt alsof er wordt teruggerapporteerd aan de verantwoordelijke voor het incident.			Onderhoud + Handreiking	...aan de verantwoordelijke proceseigenaar.	Voorbeelden diepgang incidentrapportages.	NOK maar wel opnemen in FAQ Toelichten in de handreiking. Belangrijkste incidenten moeten worden gemeld aan het hoogste management.
16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen: Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	16.1.2.7	Informatie afkomstig uit de responsible disclosure procedure zijn onderdeel van de incidentrapportage.	1	F	Welke informatie betreft dit? Intern of van extern ontvangen?	Hoe weet je of je volledig bent. Moet er een registratie zijn van ontvangen meldingen?		Uitwerken in handreiking		Voorbeelden van hoe organisaties hier invulling aan kunnen geven.	
16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging: Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren	16.1.3.1	Een responsible disclosure procedure is gepubliceerd en ingericht.	1	D	Definitie van responsible disclosure procedure kan verschillen.			Uitwerken in handreiking		Voorbeelden esponsible disclosure procedure opnemen.	
16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen: Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.	16.1.4.1	Informatiebeveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatie verwerkende systemen, behoren zo snel mogelijk (binnen 72 uur) al dan niet geautomatiseerd te worden gemeld aan het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT.	2	B	Worden hackpogingen bedoeld?		De volledigheid valt moeilijk te toetsen.	Uitwerken in handreiking		Uitwerken hoe te toetsen. Is afspraak of procedure met NCSC voldoende? Toets zeer afhankelijk wat er wordt geregistreerd.	
16.1.6	Lering uit informatiebeveiligingsincidenten: Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	16.1.6.1	Beveiligingsincidenten worden geanalyseerd met als doel te leren en het voorkomen van toekomstige beveiligingsincidenten.	2	B			Mogen incidenten ook in totaal geanalyseerd worden en hoe diep moet je gaan?	Uitwerken in handreiking		Handreiking hoe zo'n analyse er dan uit moet zien en wie die uit moet voeren.	
16.1.6	Lering uit informatiebeveiligingsincidenten: Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	16.1.6.2	De analyses van de beveiligingsincidenten worden gedeeld met de relevante partners om herhaling en toekomstige incidenten te voorkomen.	2	B	Wat zijn relevante partners en wanneer is het zwaar genoeg om te delen?	Dient de auditor bij de partners vast te stellen dat actie wordt ondernomen met de verstrekte informatie?		Uitwerken in handreiking		Handreiking hoe te toetsen dat er gedeeld wordt. Is procedure voldoende?	

Control		Overheidsmaatregel										
Nummer	Tekst	Nummer	Tekst	BBN	Opmerking categ...	Aanvullende opmerking over specifiek	Aanvullende opmerking over realistisch	Aanvullende opmerking over meetbaar	ADR suggestie	Toelichting Onderhoud BIO	Toelichting Uitwerken in handreiking/toelichting/instructie	Management reactie OK= wordt aangepast of toegelicht NOK = wordt niet aangepast of toegelicht
16.1.7	Verzamelen van bewijsmateriaal: De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	16.1.7.1	In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar.	2	J		Indien er sprake is van een incident met juridische gevolgen geldt mogelijk een andere bewaartermijn.		Onderhoud BIO	Nagaan of minimaal 3 jaar altijd een valide termijn is		NOK, hoeft niet tot onderhoud te leiden.
17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren: De organisatie behoort de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig te verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.	17.1.3.1	Continuïteitsplannen worden jaarlijks getest op geldigheid en bruikbaarheid.	1	D	Waarom wordt er geldigheid en bruikbaarheid gehanteerd als begrippen? Is toepasbaarheid niet het begrip waar op wordt gedoeld?		Wanneer is voldoende getest? Is proceduretest voldoende?	Uitwerken in handreiking		Handreiking wat er dan minimaal jaarlijks getest en vastgelegd moet zijn.	
17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren: De organisatie behoort de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig te verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.	17.1.3.2	Door het uitvoeren van een expliciete risicoafweging worden de bedrijfskritische procesonderdelen met hun bijbehorende betrouwbaarheidseisen geïdentificeerd.	2	DE	Hier is sprake van woorden zoals 'expliciete risico afweging' en 'bedrijfskritische procesonderdelen'. Deze woorden kunnen onduidelijk zijn. Waarom is hier niet gekozen voor risico-analyse?			Onderhoud BIO	Voor deze norm is het uitvoeren van een risico-analyse van belang hetgeen geen norm op zich is.		NOK, algemene formulering is reeds doorgevoerd. Risico-afweging is juiste bewoording, is VIR term. Algemene formulering opstellen en daarnaar verwijzen. Moet worden vastgelegd. Volwassenheidsniveau organisatie speelt een rol.. Voor BBN2 normen geldt dat het systeem binnen een week up and running is.
17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren: De organisatie behoort de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig te verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.	17.1.3.3	De dienstverlening van de bedrijfskritische onderdelen wordt bij calamiteiten minimaal binnen een week hersteld.	1	D	Deze normtekst is een uitwerking van 17.1.3.2. en heeft daarmee overlap. Gaat het hier om minimaal of maximaal. Wat is bedrijfskritisch?	Voor de hoogste categorie bedrijfskritische onderdelen is het denkbaar dat herstel minder dan een week moet plaatsvinden.	Wanneer is herstel gelukt? Ook als gegevens verloren zijn gegaan?	Onderhoud + Handreiking	Maximaal als term hanteren	Uitwerken hoe bedrijfskritische onderdelen kunnen worden gedefinieerd. Ook uitwerken wat bedoeld wordt met hersteld. Bijvoorbeeld door Recovery Point Objective (RPO) en Recovery Time Objective (RTO) te definieren.	OK Toelichten dat het in een week moet plaatsvinden. Minimaal moet weg. Het moet uiterlijk in een week zijn geregeld.
18.1.3	Beschermen van registraties: Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	18.1.3.1	De proceseigenaar heeft per soort informatie inzichtelijk gemaakt wat de bewaartermijn is.	2	D			Inzichtelijk gemaakt' is een moeilijk vast te stellen status. Duidelijker is 'geinventariseerd'.	Onderhoud BIO	Inzichtelijk maken aanpassen in inventariseren		NOK. Het moet per soort informatie duidelijk zijn. Inventariseren is niet scherp genoeg. Moet vanuit de AVG schriftelijk ook vanuit de archiefwet.
18.1.4	Privacy en bescherming van persoonsgegevens: Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	18.1.4.1	In overeenstemming met de AVG heeft iedere organisatie een Functionaris Gegevensbescherming (FG) met voldoende mandaat om zijn/haar functie uit te voeren.	1	AD	Wat is voldoende mandaat?	Nagaan of aan de AVG wordt voldaan is een onderzoek op zich.		Uitwerken in handreiking		Handreiking hoe voldoende mandaat kan worden vastgesteld.	
18.1.4	Privacy en bescherming van persoonsgegevens: Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	18.1.4.2	Organisaties controleren regelmatig de naleving van de privacy regels en informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	2	AB	Wanneer is er voldoende gecontroleerd?	Nagaan of aan de AVG wordt voldaan is een onderzoek op zich.		Uitwerken in handreiking		Handreiking om vast te stellen waneer er voldoende controle wordt uitgevoerd.	
18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen: Cryptografische beheersmaatregelen behoren te worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	18.1.5.1	Cryptografische beheersmaatregelen moeten expliciet aansluiten bij de standaarden op de pas-toe-of-leg-uit lijst van het forum standaardisatie.	1	AB	Forum standaardisatie is doorverwijzing.		Is het de bedoeling dat de auditor enkel vaststelt dat er voorschriften zijn?	Uitwerken in handreiking		Handreiking hoe het forum standaardisatie kan aansluiten op eigen standaarden. Handreiking hoe de pas toe-of-leg-uit regel expliciet wordt gemaakt.	
18.2.1	Onafhankelijke beoordeling van informatiebeveiliging: De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheerdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen te worden beoordeeld.	18.2.1.1	Er is een information security information system (ISMS) waarmee aantoonbaar de gehele plan-do-check-act cyclus op gestructureerde wijze wordt afgedekt.	2	J				Geen opmerkingen			
18.2.1	Onafhankelijke beoordeling van informatiebeveiliging: De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheerdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen te worden beoordeeld.	18.2.1.2	Er is een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.	2	EJ				Geen opmerkingen			

Control		Overheidsmaatregel										
Nummer	**Tekst**	**Nummer**	**Tekst**	**BBN**	**Opmerking categorie**	**Aanvullende opmerking over specifiek**	**Aanvullende opmerking over realistisch**	**Aanvullende opmerking over meetbaar**	**ADR suggestie**	**Toelichting Onderhoud BIO**	**Toelichting Uitwerken in handreiking/toelichting/instructie**	**Management reactie OK= wordt aangepast of toegelicht NOK = wordt niet aangepast of toegelicht**
18.2.2	Naleving van beveiligingsbeleid en -normen: De directie behoort regelmatig de naleving van de informatieverwerking en - procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	18.2.2.1	In de P&C cyclus wordt gerapporteerd over informatiebeveiliging, resulterend in een jaarlijks af te geven In Control Verklaring (ICV) over de informatiebeveiliging. Indien voldoende herkenbaar kan de ICV voor informatiebeveiliging onderdeel zijn van de reguliere, generieke verantwoording.	1	D	De BIR zal zelf aanleiding zijn voor het auditplan. De vraag komt op of het handig is om hier een norm voor te benoemen of dat dit onderdeel is van het framework rond de BIR.		Er wordt in de normtekst een onduidelijke voorwaarde gesteld 'voldoende herkenbaar'.	Uitwerken in handreiking		Handreiking wat "voldoende herkenbaar" is en hoe het getoetst kan worden.	OK. Risico-afweging is juiste bewoording, is VIR term. Algemene formulering opstellen en daarnaar verwijzen. Moet worden vastgelegd. Volwassenheidsniveau organisatie speelt een rol.
18.2.3	Beoordeling van technische naleving: Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	18.2.3.1	Informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijv door (geautomatiseerde) kwetsbaarheidsanalyses of	2	BI	Bgrip 'feitelijke veiligheid' niet duidelijk.		Deze norm is zeer algemeen geformuleerd (metanorm) en omvat het hele proces rond de BIR.	Onderhoud + Handreiking	Voor deze norm is het uitvoeren van een risico-analyse van belang hetgeen geen norm op zich is.	Handreiking met uitwerking over het begrip "feitelijke veiligheid".	NOK, algemene formulering is reeds doorgevoerd. Risico-afweging is juiste bewoording, is VIR term. Algemene formulering opstellen en daarnaar verwijzen. Moet worden vastgelegd. Volwassenheidsniveau organisatie speelt een rol.

Categorie	Omschrijving	Aantal
A	De normtekst verwijst naar andere regels, standaarden en voorschriften	15
B	De normtekst heeft een inconsistentie diepgang door brede termen te gebruiken	30
C	De normtekst bevat woorden die sterk plaats en tijdsgebonden zijn.	6
D	De normtekst bevat bepaalde begrippen die zonder dat duidelijk is wat er precies mee wordt bedoeld.	46
E	Dezelfde normtekst komt al elders terug, verwijzing ontbreekt en er is sprake van overlap zonder argumentatie.	7
F	De normtekst zal in veel gevallen leiden tot een bevinding omdat het in de praktijk anders geimplementeerd zal zijn.	1
G	Vervallen	0
H	De normtekst heeft geen link met ICT of wordt 1 op 1 afgedekt door andere regelgeving of normenkader.	5
I	De normtekst beschrijft een specifieke uitkomst van risicoanalyse en niet dat het onderwerp van de tekst onderdeel zou moeten zijn van een risico analyse om te komen tot een goede invulling van de maatregel.	22
J.	Overig	29
K.	Maatregel vertoont grote overeenkomsten met doelstelling.	7