Centrale
Commissie
Mensgebonden
Onderzoek

Notitie

In Control verklaring informatiebeveiliging

De Algemeen Secretaris van de Centrale Commissie Mensgebonden Onderzoek (CCMO) verklaart dat over 2020:

De Centrale Commissie Mensgebonden Onderzoek in control is ten aanzien van het Voorschrift Informatiebeveiliging Rijksdienst (VIR 2007). Dit houdt het volgende in:

- De CCMO heeft een managementsysteem voor informatiebeveiliging op basis van risicobeheer, waarmee in voldoende mate op de maatregelen ter borging van de vertrouwelijkheid, integriteit en de beschikbaarheid van informatie wordt gestuurd. De implementatie van maatregelen is gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO, voorheen BIR2012 of BIR2017);
- De interne beheersing heeft zodanig gefunctioneerd dat er voldoende zekerheid is verkregen dat de bedrijfsvoering voldoet aan het VIR 2007 / BIO en - waar nodig - aanvullende maatregelen zijn getroffen, behoudens de hieronder genoemde risico's. Deze risico's zijn van zodanig belang dat ze ook zijn opgenomen in de bedrijfsvoeringmededeling in het jaarverslag van de CCMO.

Met het managementsysteem voor informatiebeveiliging is geborgd dat er verbeterplannen zijn om deze risico's weg te nemen. De aspecten waarop daartoe gestuurd wordt zijn opgenomen in bijlage 1 van dit model.

Ter onderbouwing van deze verklaring zijn de volgende bijlagen opgenomen:

- Een lijst met onderkende kritieke en bedrijfskritische processen/systemen en bijbehorende risico's, inclusief de definities en gehanteerde criteria.
- Een overzicht van de belangrijkste informatieketens en netwerksamenwerkingsverbanden van de organisatie, en zo mogelijk het belang daarvan voor de organisatie met de daaraan gekoppelde zeer hoge risico's en de inrichting van de governance.
- Een toelichting op de reikwijdte van de ICV.

De inspanningen in 2020 op het gebied van informatiebeveiliging en de

ontwikkelingen die in 2021 worden verwacht, zijn beschreven in het document Verantwoording en Vooruitblik 2021 welke is bijgevoegd.

Ondertekening Algem[redacted] Secretaris

[redacted]

5.1.2.e

Bijlage 1: Aspecten van het managementsysteem rond informatiebeveiliging

De opzet van het managementsysteem[1] voor de informatiebeveiliging is zodanig, dat minimaal de volgende punten kunnen worden onderbouwd:

1. Het bestaan van een departementsbrede PDCA-cyclus voor het onderwerp informatiebeveiliging en het functioneren van een departementsbrede beveiligingsorganisatie. Het departement stuurt planmatig (bijv. met jaar- en verbeterplannen), zodat duidelijk is wat er wordt gedaan om de informatiebeveiliging op orde te krijgen dan wel te houden. Over de uitvoering en de voortgang van de plannen en de status van de informatiebeveiliging wordt periodiek, minimaal jaarlijks, aan de departementsleiding gerapporteerd;
2. Een actueel overzicht van de kritieke en bedrijfskritische bedrijfsprocessen / informatiesystemen en informatieketens;
3. Voor alle kritieke en bedrijfskritische processen cq. informatiesystemen bestaat een actuele risicoafweging, waardoor bekend is welke risico's bestaan en al dan niet worden geaccepteerd;
4. Een overzicht van op basis van risicoafwegingen geselecteerde en geïmplementeerde maatregelen uit de BIO en eventueel aanvullende maatregelen. Voor niet relevante maatregelen is geen explain nodig;
5. Het risico van het (nog) niet operationeel zijn van beveiligingsmaatregelen voor een kritiek en bedrijfskritisch proces (c.q. informatiesysteem en keten);
6. De nog te implementeren maatregelen (niveau control inclusief toepasselijke rijksmaatregelen van de BIO) zijn onderdeel van een verbeterplan;
7. Een (actieplan om te komen tot een) set van afspraken voor informatieketens over het gewenste beveiligingsniveau. Het van kracht zijn van een stelsel van generieke beheersmaatregelen waarmee de basisbeveiliging van de gehele informatievoorziening wordt afgedekt;
8. De borging dat voor nieuwe ontwikkelingen rond (of inkoop van) informatiesystemen op basis van een risicoafweging wordt bepaald welke maatregelen van toepassing zijn;
9. Het periodiek testen van de goede werking van geïmplementeerde maatregelen. De selectie van te testen maatregelen vindt plaats aan de hand van een risicoafweging;

[1] Een managementsysteem is een stelsel van processen waarmee volgens een eenduidige systematiek de informatiebeveiliging op basis van risicobeheer (departements) breed wordt geborgd.

10. Een afloopsysteem waaruit blijkt dat bevindingen n.a.v. het periodiek testen zijn opgenomen in een verbeterplan c.q. zijn opgelost.
11. Een concreet actieplan om de BIO voor de gehele informatievoorziening te implementeren dat is opgenomen in de departementsbrede PDCA-cyclus.

Tabel 1	Met het managementsysteem voor informatiebeveiliging is geborgd dat er verbeterplannen zijn om deze risico's weg te nemen. De aspecten waarop daartoe gestuurd wordt zijn opgenomen in de ICV onderbouwing. Ter onderbouwing van deze verklaring zijn de volgende bijlagen opgenomen:	Aanwezig ja / nee	Naam en Datum document
1	Een lijst met onderkende kritieke, bedrijfskritisch of belangrijke* processen/systemen en bijbehorende risico's, inclusief de definities en gehanteerde criteria. * Zie toelichting bij de uitvraag.	Ja	- Processen CCMO (2017) - QS-IB Viadesk (2017) - QS-AVG ROMERO (2019) - PIA ROMERO (2019) - BIO-analyse ROMERO (2019) - V&V 2019 - A&K analyse ToetsingOnline (2013)
	Toelichting: Er zijn geen kritieke processen/systemen onderkend bij CCMO. Een lijst met de in kaart gebrachte processen/systemen is bijgevoegd. Er is in 2017 een Quickscan BIR uitgevoerd voor de applicatie Viadesk. Voor de nieuwe applicatie ROMERO is een Quickscan AVG en PIA uitgevoerd in 2019. ROMERO is ter vervanging van onder andere ToetsingOnline en Viadesk. Quickscans voor de overige systemen staan op de planning.		

2	Een overzicht van de belangrijkste informatieketens en netwerksamenwerkingsverbanden van de CCMO, en zo mogelijk het belang daarvan voor de CCMO met de daaraan gekoppelde zeer hoge risico's en de inrichting van de governance.	Ja	- Processen CCMO (2017) - QS-IB Viadesk (2017) - QS-AVG ROMERO (2019) - PIA ROMERO (2019) - V&V 2019 - A&K analyse ToetsingOnline (2013)
	Toelichting: Er zijn geen (kritieke) informatieketens / samenwerkingsverbanden. Een lijst met in kaart gebrachte processen/systemen is bijgevoegd. Er is in 2017 een Quickscan BIR uitgevoerd voor de applicatie Viadesk. Voor ROMERO is een Quickscan AVG en PIA uitgevoerd in 2019. De CCMO werkt samen met regionale toetsingscommissies (METC's) met de applicaties Viadesk en ToetsingOnline. In Q2 2020 zal de samenwerking in ROMERO van start gaan.		
3	Een toelichting op de reikwijdte van de ICV.	Ja	N.v.t.
	Toelichting: De ICV is van toepassing op het zelfstandig bestuursorgaan Centrale Commissie Mensgebonden Onderzoek (CCMO).		

Bijlage 1	ICV onderbouwing: **Bijlage 1: Aspecten van het managementsysteem rond informatiebeveiliging**	Aanwezig ja / nee	Naam en Datum document
De opzet van het managementsysteem voor de informatiebeveiliging is zodanig, dat minimaal de volgende punten kunnen worden onderbouwd:			

Bijlage 1	ICV onderbouwing: **Bijlage 1: Aspecten van het managementsysteem rond informatiebeveiliging**	Aanwezig ja / nee	Naam en Datum document
1	Het bestaan van een organisatie PDCA-cyclus voor het onderwerp informatiebeveiliging en het functioneren van een departementsbrede beveiligingsorganisatie. De organisatie stuurt planmatig (bijv. met jaar- en verbeterplannen), zodat duidelijk is wat er wordt gedaan om de informatiebeveiliging op orde te krijgen dan wel te houden. Over de uitvoering en de voortgang van de plannen en de status van de informatiebeveiliging wordt periodiek, minimaal jaarlijks, aan de departementsleiding gerapporteerd;	Ja	- ICV CCMO 2018 - V&V 2019
	Toelichting: De CCMO hanteert de PDCA-cyclus en bijbehorende systematiek van het kerndepartement Ministerie VWS. Het management wordt maandelijks geïnformeerd a.d.h.v. het verslag van het PIIT-team.		
2	Een actueel overzicht van de kritieke bedrijfsprocessen / informatiesystemen en informatieketens;	Ja	- Processen CCMO (2017) - QS-IB Viadesk (2017) - QS-AVG ROMERO (2019) - PIA ROMERO (2019) - V&V 2019 - A&K analyse ToetsingOnline (2013)
	Toelichting: Er zijn geen kritieke processen/systemen onderkend bij CCMO. Een lijst met de belangrijkste in kaart gebrachte processen/systemen is bijgevoegd. Er is in 2017 een Quickscan BIR uitgevoerd voor de applicatie Viadesk. Voor ROMERO is een Quickscan AVG en PIA uitgevoerd in 2019. Quickscans voor de overige systemen staan op de planning.		

Bijlage 1	ICV onderbouwing: **Bijlage 1: Aspecten van het managementsysteem rond informatiebeveiliging**	Aanwezig ja / nee	Naam en Datum document
3	Voor alle kritieke processen cq. informatiesystemen bestaat een actuele risicoafweging, waardoor bekend is welke risico's bestaan en al dan niet worden geaccepteerd;	Nee	
	Toelichting: Er zijn geen kritieke processen/systemen onderkend bij CCMO.		
4	Een overzicht van op basis van risicoafwegingen geselecteerde en geïmplementeerde maatregelen uit de BIR en eventueel aanvullende maatregelen. Voor niet relevante maatregelen is geen explain nodig;	Ja	- ICV SSC-ICT 2019 - A&K analyse ToetsingOnline (2013)
	Toelichting: Er zijn geen ICV's van andere organisaties ontvangen, behalve voor SSC-ICT over het jaar 2019.		
5	Het risico van het (nog) niet operationeel zijn van beveiligingsmaatregelen voor een kritiek proces (cq. informatiesysteem en keten);	Nee	
	Toelichting: Er zijn geen kritieke processen/systemen onderkend bij CCMO.		
6	De nog te implementeren maatregelen (niveau beheersdoelstelling inclusief toepasselijke O-maatregelen van de BIO) zijn onderdeel van een verbeterplan;	Ja	- ICV SSC-ICT 2019 - QS-IB Viadesk (2017) - QS-AVG ROMERO (2019) - PIA ROMERO (2019) - V&V 2019 - A&K analyse ToetsingOnline (2013)
	Toelichting: ROMERO is de nieuwe applicatie voor ToetsingOnline/Viadesk/CCMO-register en wordt verwacht in Q2 2020.		

Bijlage 1	ICV onderbouwing: **Bijlage 1: Aspecten van het managementsysteem rond informatiebeveiliging**	Aanwezig ja / nee	Naam en Datum document
7	Een (actieplan om te komen tot een) set van afspraken voor ketens over het gewenste beveiligingsniveau. Het van kracht zijn van een stelsel van generieke beheersmaatregelen waarmee de basisbeveiliging van de gehele informatievoorziening wordt afgedekt;	Nee	
	Toelichting: Er zijn geen belangrijke informatieketens/samenwerkingsverbanden.		
8	De borging dat voor nieuwe ontwikkelingen rond of inkoop van informatiesystemen op basis van een risicoafweging wordt bepaald welke maatregelen van toepassing zijn;	Ja	- QS-AVG ROMERO (2019) - PIA ROMERO (2019) - V&V 2019
	Toelichting: De CCMO sluit aan bij de standaard inkoopprocessen van VWS (HIS).		
9	Het periodiek testen van de goede werking van geïmplementeerde maatregelen. De selectie van te testen maatregelen vindt plaats aan de hand van een risicoafweging;	Ja	- ICV SSC-ICT 2019 - V&V 2019
	Toelichting:		
10	Een afloopsysteem waaruit blijkt dat bevindingen n.a.v. het periodiek testen zijn opgenomen in een verbeterplan c.q. zijn opgelost.	Ja	- ICV SSC-ICT 2019 - V&V 2019
	Toelichting:		
11	Een concreet actieplan om de BIO voor de gehele informatievoorziening te implementeren dat is opgenomen in de departementsbrede PDCA-cyclus.	Nee	
	Toelichting: Het actieplan wordt in de komende periode gemaakt op basis van de voorgenomen inventarisaties (quickscans) op alle systemen.		