

Ministerie van Volksgezondheid,
Welzijn en Sport

5.1.2.e, Directeur CCMO

**Centrale Commissie
Mensgebonden Onderzoek**

Bezoekadres:

Parnassusplein 5
2511 VX Den Haag
T 070 340 79 11
Postbus 20350
2500 EJ Den Haag
www.rijksoverheid.nl

Inlichtingen bij

5.1.2.e

5.1.2.e

5.2.1.e@minvws.nl

Datum

28 februari 2023

Aantal pagina's

4

memo

Het IB-Beeld 2022 van de CCMO

Inleiding IB-Beeld

Het IB-Beeld is de vervanger van de In Control Verklaring ('ICV'). De ervaring leerde dat bedrijfsonderdelen regelmatig meer bezig waren om op papier te kunnen verklaren dat zij hun informatiebeveiliging ('IB') onder controle hadden dan het daadwerkelijke doel om in de praktijk IB onder controle te hebben. Dit heeft geleid tot de vervanging van de ICV naar het opstellen van een IB-Beeld. Het doel van het IB-Beeld is het schetsen van een beeld hoe het ervoor staat met IB in het bedrijfsonderdeel, ongeacht hoe goed dat is. Het IB-Beeld heeft daarmee geen toetsende aard en geeft ruimte aan openheid, wat dan vervolgens ruimte geeft om vast te leggen welke verbetermogelijkheden er zijn.

De uiteindelijke formele uitvraag voor het opstellen van het IB-Beeld is relatief laat in het jaar verzonden. Er is daarom gekozen niet het volledige IB spectrum in kaart te brengen en een beperkt aantal onderwerpen uit te vragen. In de komende jaren zal de scope van het IB-Beeld verder uitgebreid worden. De onderwerpen van het IB-Beeld 2022 zijn Bestuur, Organisatie, Risicobeheer, Bewustzijn en Logging. Daarnaast zijn diverse zaken uitgevraagd zoals incidenten, datalekken en informatie m.b.t. processen en informatiesystemen.

Methode

Het CISO en PO (Privacy Officer) team van het kerndepartement heeft een vragenlijst opgesteld en naar de coördinator IB&P gestuurd ter voorbereiding op een interview met de coördinator en directeur. De vragen uit de vragenlijst stonden vervolgens centraal tijdens het interview. Na het interview is vervolgens deze memo opgesteld ter vaststelling van het IB-Beeld 2022. Tot slot is deze ter beoordeling gestuurd naar de coördinator IB&P voor de laatste aanpassingen, waarna de memo die voor u ligt definitief is gemaakt.

Algemeen IB-Beeld CCMO 2022

Het algemene IB-Beeld van de CCMO is goed. De werkzaamheden en doelen van de CCMO zorgen ervoor dat IB&P belangrijk zijn en dit zijn ze zich dan ook terdege bewust. De organisatie hecht veel belang aan IB&P en dit is op alle lagen geborgd. De coördinator IB&P gaat ook serieus om met het onderwerp en wat hij weet of aan instructies ontvangt, implementeert hij. Daar liggen dan ook gelijk de verbeterkansen, wat hij niet weet, kan hij ook niet uitvoeren. Dus regelmatig sparren met het IB&P Office en het structureel bijwonen van de trainingen voor de coördinatoren IB&P zal verdere informatie en instructies verschaffen om te overwegen waar de CCMO nog verbeterkansen heeft.

Samenvatting verbeterkansen

Deze verbeterkansen zijn op basis van de scope van het IB-Beeld 2022, dit omvat niet het volledig IB spectrum. Zie de specifieke onderwerpen voor verdere uitleg.

- Implementeren IB strategie en beleid. Het aanleveren van de strategie en beleid van het kerndepartement als kaders en richtlijnen ligt bij het IB&P Office van het kerndepartement.
- De meeste hoofdprocessen is al een QuickScan op uitgevoerd, er worden nu een aantal processen geautomatiseerd, zodra nodig hier ook QuickScans op uitvoeren.
- Een bewustwordingsplan opstellen en uitvoeren. Plannen hiervoor zijn een IB&P bureauoverleg voor alle medewerkers te plannen, IB&P basisprincipes toe te voegen aan het gesprekslijstje voor het inwerkgesprek en de implementatie van een e-learning. Het IB&P Office is ook bezig met de implementatie van een algemene kernbrede e-learning.

Datum
28 februari 2023

IB-Beeld CCMO 2022

Bestuur

Geeft richting en ondersteuning aan informatiebeveiliging c.q. cyber security in lijn met bedrijfsdoelstellingen, risicobereidheid en van toepassing zijnde wet- en regelgeving en vergewist zich van de effectieve naleving ervan.

Het kerndepartement is in het leven geroepen om (kleine) beleidsdirecties, programmadiirecties, raden en andere kleine bedrijfsonderdelen binnen het Ministerie van VWS te voorzien van ondersteuning en of te ontlasten op specialistische onderwerpen vanuit een centraal punt. Eén van de specialistische onderwerpen waar er vanuit een centraal punt ondersteuning wordt aangeboden is Informatiebeveiliging en Privacy ('IB&P').

De CCMO sluit aan bij de standaardisatie vanuit het IB&P Office op het gebied van strategie, visie en beleid met betrekking tot IB, zoals ze dit ook doen met onder andere inkoop en informatie management.

De kansen voor verbetering liggen voor de inrichting van IB bestuur voornamelijk bij het IB&P kernteam. Het kernteam is gestart met richting te geven aan en documentatie op te stellen voor IB bestuur voor de bedrijfsonderdelen van het kerndepartement. Het kernteam streeft ernaar dit in de eerste twee kwartalen van 2023 op te leveren. Na de oplevering zal toepassing van de instructies door de CCMO moeten volgen.

Organisatie

Informatiebeveiliging (inclusief cyber security) is op het hoogst mogelijk organisatieniveau geadresseerd en het beheer van informatiebeveiliging is in lijn met de bedrijfsdoelstellingen en van toepassing zijnde risico's en compliance eisen.

Het IB&P kernteam zorgt voor kaders en richtlijnen voor IB en stelt instructies op om deze kaders en richtlijnen toe te passen en te implementeren in de bedrijfsonderdelen van het kerndepartement. Dit neemt echter niet weg dat de CCMO verantwoordelijk is voor IB&P binnen de organisatie. IB&P zijn gericht op de bescherming van (persoons)gegevens en de commissie is eigenaar van haar

(persoons)gegevens. Het is daarom belangrijk dat taken en verantwoordelijkheden m.b.t. IB goed belegd worden.

**Centrale Commissie
Mensgebonden Onderzoek**

Het onderwerp en recht van bestaan van de CCMO heeft tot gevolg dat ze met gevoelige (persoons)gegevens werken. Er is daarom ook een Privacy Officer ('PO') in dienst als ook verschillende juristen. De PO is er in principe voor de commissie en in mindere mate voor het secretariaat. De commissie is meer onafhankelijk en het secretariaat is het onderdeel dat onder de paraplu van het kerndepartement valt. Alsnog heeft de coördinator IB&P, 5.1.2.e, hierdoor de mogelijkheid om voor privacy zaken met vragen terecht te kunnen bij de PO en juristen.

Datum
28 februari 2023

Directeur/Algemeen Secretaris 5.1.2.e neemt IB&P serieus en ziet hier het belang van in. Er is namelijk veel Dep.V. en er zijn serieuze risico's, inclusief financiële risico. Daardoor wordt IB&P als belangrijk gezien. Dit heeft er ook voor gezorgd dat de CCMO in het nieuwe pand (B30) een apart afsluitbare ruimte heeft bedongen als onderdeel van informatiebeveiliging by design.

Coördinator IB&P 5.1.2.e krijgt voldoende ruimte en middelen om zijn taak goed uit te voeren.

Risicobeheer

Draagt zorg voor het op gestructureerde wijze identificeren en beheersen van informatiebeveiligings- en cyber securityrisico's zodanig dat de risico's in lijn zijn met de risicobereidheid en het risicoframework van de organisatie.

Het kerndepartement hanteert een risicoframework waarin risico's worden geïdentificeerd op proces- en informatiesysteemniveau. De te bewandelen stappen hiervoor zijn daarmee eerst het in kaart brengen van de processen binnen de organisatie, QuickScans uitvoeren op de processen, waarmee ook in kaart wordt gebracht of diepgaandere analyses moeten worden uitgevoerd en welke informatiesystemen worden gebruikt bij het proces. De informatiesystemen worden vervolgens tegen het licht van de BIO (Baseline Informatiebeveiliging Overheid) aangehouden. Dit gebeurt veelal door het I-Team voor functioneel beheer van de Directie OBP omdat zij de meeste applicaties in beheer hebben. Tijdens de analyses wordt ook direct stilgestaan of gevonden (extra) risico's moeten worden gemitigeerd en hoe. De uitkomst hiervan kan een maatregel of een acceptatie zijn. En tot slot worden de gekozen maatregelen en of acceptaties gedocumenteerd in een verbeterplan.

De CCMO heeft hun processen reeds in kaart gebracht. Er zijn op de meeste processen ook al QuickScans uitgevoerd. De CCMO hecht ook veel waarde aan deze QuickScans om zo goed classificaties en risico's in kaart te brengen vanwege de (financiële) risico's die spelen. Er zijn nog een aantal hoofdprocessen die nog niet zijn geautomatiseerd, zodra dat gebeurt zullen QuickScans op deze processen worden uitgevoerd. Informatiemanager 5.1.2.e ziet hier ook goed op toe als onderdeel van het CIO advies.

Bewustzijn

Draagt er zorg voor dat alle medewerkers, inhuurkrachten en derde partijen zich bewust zijn van informatiebeveiligings- en cyber securityrisico's.

Er zijn verschillende middelen die ingezet kunnen worden om een bedrijfsonderdeel te helpen om het bewustzijn van de medewerkers te verbeteren

en vervolgens in stand en up to date te houden. Een onderdeel hiervan dient VWS breed, of ten minste kern breed, geregeld te worden. En daarnaast zijn er verantwoordelijkheden voor het bedrijfsonderdeel. Dit alles moet omschreven zijn in een bewustzijn programma.

**Centrale Commissie
Mensgebonden Onderzoek**

Datum
28 februari 2023

Gezien de aard en onderwerp van de commissie is er een prima basisbewustwording aanwezig. 5.1.2.e ziet verbetering in omgang met documenten, de documenten worden steeds meer digitaal behandeld en niet meer uitgeprint. Er heerst een cultuur om elkaar aan te spreken op bijvoorbeeld het vergrendelen van beeldschermen wanneer de werkplek wordt verlaten.

Uiteraard is er altijd ruimte voor verbetering en is herhaling een belangrijk devies. De CCMO heeft plannen om in 2023 een bureauoverleg voor alle medewerkers te organiseren over het onderwerp en de medewerkers een e-learning te laten volgen. Daarnaast gaat 5.1.2.e aan het lijstje dat wordt besproken met nieuwe medewerkers basis IB&P onderwerpen toevoegen die besproken worden tijdens het inwerkgesprek.

Het IB&P Office is bezig met het ontwikkelen van een VWS brede e-learning voor IB&P. Het organiseren van deze e-learning neemt meer tijd in beslag dan verwacht vanwege afhankelijkheden van leveranciers. Het streven is dit zo snel mogelijk in 2023 geregeld te hebben.

Informatiesystemen en processen

De processen van de CCMO zijn vastgesteld. Er zijn processen van TBB3, maar niet hoger. De volgende informatiesystemen worden gehanteerd naast de standaard kantoorautomatisering.

- ToetsingOnline

Deze applicatie is niet in beheer bij de CCMO, maar bij VKNA/Bionics. Het I-Team voor functioneel beheer van de Directie OBP beheert de meeste applicaties die de CCMO van de standaard KA gebruikt en het I-Team controleert ook of de applicaties aan de BIO voldoen. Het is daarmee wel bekend dát er logging is, maar niet hoe deze logging in elkaar zit.

Incidenten en datalekken

Er zijn wat kleine incidenten geweest, maar er zijn geen incidenten of datalekken met grote impact opgetreden bij de CCMO.

5.1.2.e