Programma Informatievoorziening 2020-2025

Veelgestelde vragen

Versnellingsplan Informatieveiligheid

Versie 20211005

In deze vraag en antwoordenlijst wordt ook verwezen naar documenten die in de samenwerkingsomgeving van het Programma IV staan. Geen toegang, lukt het niet een document te openen of geeft deze FAQ nog geen antwoord op jouw vraag/vragen? Stuur een mail naar: programmaiv@ifv.nl

Vragen over het implementatieloket en de toolbox BIO	
Wat is het implementatieloket?	Het implementatieloket is dé ingang voor regio's naar informatie over het versnellingsplan, hulpmiddelen om te voldoen aan de BIO, communicatiemiddelen en meer. Ook kan je via dit loket je vragen kwijt. De startpagina van het loket staat op IFV.nl. Sommige (vertrouwelijke) documenten zijn alleen beschikbaar in een besloten omgeving waar het aanspreekpunt van de regio toegang toe heeft.
Wanneer is de toolbox van het Versnellingsplan beschikbaar gesteld?	De initiële toolbox is sinds 11 juni jl. online beschikbaar via het implementatieloket, nadat het Veiligheidsberaad positief over het versnellingsplan besloot. De toolbox zal steeds verder uitgebreid worden, ook naar gelang de behoefte van de regio's.
Hoeveel controls zijn er en wanneer moeten we aan welke controls voldoen?	Belangrijk is dat een regio zijn informatieveiligheid goed op orde heeft en dat het versnellingsplan niet leidt tot afvinken van een lijst van criteria. Er is afgesproken dat de regio's aan elkaar rapporteren over de voortgang van de implementatie van de BIO middels de indeling die het CIP (Centrum Informatiebeveiliging en Privacybescherming) hanteert bij de BIO Self Assessment. Deze indeling gaat uit van 110 controls in 16 categorieën.
Hoe is de subset van de BIO samengesteld waar regio's en het IFV per 30-06-2022 aan moeten voldoen?	Als verlengd lokaal bestuur zien we verschillende raakvlakken met het traject dat de VNG/IBD destijds heeft doorgemaakt (zij noemden het 'eigen huis op orde'.) Hierin hoeven wij het wiel niet opnieuw uit te vinden. Verschillende partijen (VNG/CIP/ Digitale overheid) hebben een geaggregeerde set van 16 criteria beschikbaar gesteld. Dit zijn de prioriteiten om te implementeren om te voldoen aan de BIO. Hiermee kun je themagericht te werk gaan. Daarnaast kan worden gekeken naar de resterende punten om volledig te voldoen aan de BIO. De Baseline Informatiebeveiliging Overheid (BIO) is de opvolger van eerder gebruikte normenkaders als BIWA, BIG, BIR en IBI, die worden gebruikt binnen de overheid voor informatiebeveiliging. De BIO vormt daarmee één gezamenlijk normenkader, gebaseerd op de ISO 27001. Het grote verschil is dat de huidige BIO meer op risicomanagement is gebaseerd en niet is bedoeld als afvinklijst. Een subset betekent dus niet dat je minder hoeft te doen.

Door wie en hoe wordt vastgesteld dat een regio per 01-01-2023 voldoet aan de BIO vastgesteld?	De verantwoordelijkheid en autonomie ligt bij de regio's. Het is dus de eigen verantwoordelijkheid om de 'basis aantoonbaar op orde' te krijgen. Op orde wil zeggen dat elke organisatie haar eigen informatiebeveiligingsrisico's inventariseert, beoordeelt en op basis daarvan vaststelt welke maatregelen passend zijn en deze implementeert. Aantoonbaar wil zeggen, d.m.v. auditing. Er zal wel monitoring plaatsvinden op de voortgang van de implementatie van de BIO binnen de regio's en daarmee voldoet aan de BIO. Dit volgt uit het besluit van het Veiligheidsberaad dat regio's aan elkaar rapporteren over hun eigen voortgang. De voortgang van de regionale implementatietrajecten wordt periodiek verzameld door het implementatieloket dat het IFV invult in opdracht van het POI. Er wordt gerapporteerd aan het POI, de RCDV en de BAC-IV.
Wat houdt 'voldoen aan de BIO' als mijlpaal exact in?	Wanneer de organisatie op basis van risicomanagement invulling heeft gegeven aan alle controls en maatregelen van de BIO die van toepassing zijn, én de organisatie hiervoor een goede PDCA-cyclus heeft ingeregeld om blijvend te voldoen, kan in elk geval geconcludeerd worden dat de organisatie voldoet aan de BIO. Certificeringen zijn uiteraard ook een vorm om aan te tonen dat men voldoet.
Is er een praktisch instrument voor het stapsgewijs implementeren van de BIO?	Ja, dat is de BIO Self-Assessment, te vinden op de website van het CIP (Centrum Informatiebeveiliging en Privacybescherming). Deze en meer links naar praktische informatie zijn ook te vinden via de toolbox van het implementatieloket.
Wat zijn de consequenties als een regio of het IFV niet aan de BIO voldoet per 01-01-2023?	Om aan te kunnen sluiten op het Nationaal Detectie Netwerk (NDN, waarmee cruciale dreigingsinformatie ter preventie van cyberincidenten kan worden verkregen) worden er aan de regio's en het IFV eisen gesteld, zoals het voldoen aan de BIO. BIO compliance zal ook de eis zijn voor deelname aan een SOC en CERT en mogelijk zelfs voor deelname aan (nieuwe) landelijke voorzieningen. Daarnaast wijzen alle landelijke ontwikkelingen (Tweede Kamer) erop dat de BIO sterker wettelijk verankerd zal worden (soort verplichte APK). Los van het risico op imagoschade loop je het risico dat de beveiliging niet op orde is met het risico op grote financiële schade als gevolg. Er zijn helaas al voorbeelden genoeg; Hof van Twente, Universiteit Maastricht en de VNOG, waarbij de schade in de miljoenen loopt.
Hoeveel kost een succesvolle implementatie van de BIO?	Hiervoor is de investeringsindicatie opgesteld, die als bijlage aan het Veiligheidsberaad is aangeboden. Afhankelijk van de 'staat van de regio' zal het meer of minder kosten aan capaciteit, inspanningen en investering. De vuistregel is dat de investering voor een groot deel afhangt van de staat van de infrastructuur.
Kan ik hulp inschakelen voor implementatie binnen onze regio?	Het programma IV geeft invulling aan het landelijke implementatieloket die -naast het bieden van informatie, handreikingen e.d. - dient als vraagbaak ter ondersteuning van de regionale implementatie van de BIO. Indien meerdere regio's dezelfde, specialistische vraag hebben, kan door de programmamanager externe expertise worden ingeschakeld. Er is in het Programma IV niet voorzien in individuele regionale implementatie ondersteuning.

Vragen over SOC/CERT	
In het versnellingsplan wordt gesproken over een landelijk haalbaarheidsonderzoek SOC/CERT. Door wie wordt een soortgelijke dienstverlening als het IBD gefaciliteerd? Wat zijn de vervolgstappen?	Wellicht dat haalbaarheidsstudie de lading niet dekt van het onderzoek. O.a. uit de oefening ISIDOOR 2021 is gebleken dat een CERT/SOC minimaal nodig is om mee te komen binnen het Landelijk Dekkend Stelsel (o.a. NCSC, IBD, Z-CERT, SURF-CERT) om veiligheidsregio's cyberweerbaar te maken. Als onderdeel van het Landelijk Dekkend Stelsel wordt het zelfs verwacht dat iedere sector een SOC & CERT sectoraal heeft geregeld. De VR-ISAC springt momenteel in een vacuüm bij gebrek aan een VR-CERT. We weten dat de functionaliteiten van een CERT & SOC nodig zijn, maar de vorm waarin we het gieten (governance model) is punt van onderzoek. Het is daarmee een inrichtingsvraagstuk. Naar aanleiding van de verschillende gesprekken die we tot op heden hebben gevoerd met oa de IBD, Z-CERT & &NCSC voorzien we een aantal scenario's met betrekking tot de inrichting waar op strategisch niveau (VB) een besluit dient te worden genomen door de Veiligheidsregio's en het IFV. Dit onderzoek wordt uitgevoerd in samenwerking met het lectoraat crisisbeheersing binnen het IFV.
Vragen over bewustwordingscampagnes	
Bewustwordingscampagnes zijn ook onderdeel van het versnellingsplan. Wat is hiervan al beschikbaar?	Met de collega's die aanspreekpunt van de regio's zijn, worden voorbeelden gedeeld, bijvoorbeeld uit andere regio's. Verder is het volgende beschikbaar: **Vragenlijst ten behoeve van opzet bewustwordingscampagne:** https://www.informatiebeveiligingsdienst.nl/product/handreiking-communicatieplan-informatiebeveiliging/ **Stappenplan opzetten bewustwordingscampagne:** https://www.digitaltrustcenter.nl/stappenplan-cyberbewustwordingscampagne **Waar gaat een bewustwordingscampagne mis?:** https://ib-p.nl/2018/05/waarom-bewustwordingscampagnes-mislukken/
Andere vragen	
Het is nu niet inzichtelijk in welke fases regio's zich onderling bevinden en wat voor tijd, geld en middelen zij tot hun beschikking hebben. Zou dit niet eerst helder moeten worden ten behoeve van bepalen van een gezamenlijk startpunt en samenwerking?	Dit is de afgelopen 5 jaar inzichtelijk gemaakt met behulp van de collegiale toetsing. Dit is ook de concrete aanleiding geweest voor het versnellingsplan, omdat niet alleen bleek dat dit een wettelijke taak is en er in de afgelopen jaren geen voortgang is geboekt, maar dat de onderlinge verschillen tussen regio's ook groeit. Op basis van een inventarisatie van het aantal FTE zijn we bijvoorbeeld tot de conclusie gekomen dat het merendeel van de regio's slechts 0,2 fte beschikbaar heeft op dit onderwerp. Daarbij gaat het solidariteitsprincipe uit van onderlinge afhankelijkheden en een intrinsieke motivatie om niet de zwakste schakel te willen zijn. In het kader van digitale weerbaarheid wordt namelijk gesproken van ketenafhankelijkheden waarbij je zo sterk bent als de zwakste schakel. De onderlinge samenwerking is gericht op een thematische aanpak van knelpunten.

Worden de collegiale toetsingen nu niet meer uitgevoerd?	We hebben ervaren dat deze methodiek werkt en heel waardevol is. Echter, we willen nu versnellen. Juist omdat uit de laatste collegiale toetsing bleek dat de onderlinge verschillen tussen de regio's toenamen. We gaan nu implementeren en dat kost tijd. Het rapporteren over de voortgang in de regio is geen collegiale toetsing. Samen met de vakgroep Informatieveiligheid zal eind 2022 worden gekeken naar een vervolg van de collegiale toetsing die in 2023 weer uitgevoerd zal worden, om daarmee ook structureel te organiseren dat we op niveau blijven.
Hoe blijf ik op de hoogte van ontwikkelingen rond het Versnellingsplan	Relevant nieuws delen we via het implementatieloket, in de Teams-samenwerkingsomgeving van het Programma IV en in de nieuwsbrief van het Programma IV.
Waar kan ik terecht met andere vragen?	Bij het landelijke implementatieloket of via programmaiv@ifv.nl

Dit is een levend document dat continu doorontwikkeld wordt naar aanleiding van de vragen die het implementatieloket ontvangt gedurende de regionale implementaties van de BIO.