De Baseline Informatie-beveiliging Overheid is meer dan een jaarlijkse In Control Verklaring

In dit artikel wordt de achtergrond van de Baseline Informatiebeveiliging Overheid (hierna: BIO) toegelicht. De lezer wordt daarnaast geadviseerd over belangrijke keuzes die voorafgaand aan de daadwerkelijke BIO-implementatie moeten plaatsvinden. Diverse keuzes en overwegingen worden uiteengezet, ter voorbereiding op een weloverwogen implementatie. Uiteraard volgen ook adviezen over de uitvoering van de BIO-implementatie.

BIO | Baseline Informatiebeveiliging Overheid

Nog geen drie jaar geleden werden binnen de overheid verschillende baselines gehanteerd voor informatiebeveiliging. Afhankelijk van de overheidsorganisatie was de BIG, BIWA, BIR of IBI van toepassing. Sinds januari 2019 is er echter één basisniveau van informatiebeveiliging voor de overheid: de Baseline Informatiebeveiliging Overheid. De BIO is gebaseerd op de internationale NEN-ISO/IEC 27001:2017 en NEN-ISO/IEC 27002:2017 (hierna: ISO 27001 en 27002) . De opdracht is helder voor het Rijk, Gemeenten, Waterschappen en Provincies: de BIO moet worden gehanteerd als basis voor informatiebeveiliging (bio-overheid.nl).

De BIO is een invulling van ISO 27001 en 27002 toegespitst op overheden en bevat tevens aanvullingen die zichtbaar zijn gemaakt in groen en blauw gekleurde normen. De blauwe normen betreffen de ISO-normen, de aanvullende verplichte overheidsmaatregelen zijn groen gekleurd. Zie hiervoor het onderstaande voorbeeld uit hoofdstuk twaalf over ‘Bescherming tegen malware’. In dit voorbeeld is zichtbaar dat de aanvullende verplichte overheidsmaatregelen met betrekking tot bescherming tegen malware meer gedetailleerd zijn dan de ISO-norm.

[1] NB: Er is een nieuwe ISO 27002 gepubliceerd in 2022. De ‘vertaling’ van deze norm naar de BIO moet nog plaatsvinden. Alhoewel qua structuur grote wijzigingen hebben plaatsgevonden, blijven de meeste normen hetzelfde onder ISO 27002. Wel zijn er enkele nieuwe normen, bijvoorbeeld op het gebied van threat intelligence, data masking en secure coding.

12.2 Bescherming tegen malware

Doelstelling:
Waarborgen dat informatie en informatie verwerkende faciliteiten beschermd zijn tegen malware.

12.2.1	**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.	Secretaris/algemeen directeur Dienstenleverancier
12.2.1.1	1	Het downloaden van bestanden is beheerst en beperkt op basis van risico en need-of-use.	
12.2.1.2	1	Gebruikers zijn voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende links.	
12.2.1.3	1	De gebruikte antimalwaresoftware en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.	
12.2.1.4	1	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.	
12.2.1.5	1	De malwarescan wordt op verschillende omgevingen uitgevoerd, bijvoorbeeld op mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie.	

(Bron: p. 48 BIO v. 1.04vz)

Van overheidsorganisaties wordt verwacht dat zij jaarlijks een In Control Verklaring (hierna: ICV) publiceren over de geïmplementeerde én niet geïmplementeerde BIO-normen. Hierin verschilt de ICV van de ISO-certificering (aangezien de ICV een intern opgestelde verklaring betreft, in tegenstelling tot de ISO-certificering die door een extern geaccrediteerde organisatie wordt afgegeven).

De opdracht voor overheidsorganisaties is helder: voldoen aan de BIO om de informatiebeveiliging te waarborgen en daarover jaarlijks rapporteren. De implementatie is echter geen 'straight forward' traject. De route om uiteindelijk tot implementatie van de BIO en een ICV te komen is sterk afhankelijk van keuzes die voor, tijdens én na de implementatie worden gemaakt. Juist ook na de implementatie van de BIO-normen, omdat het borgen van informatiebeveiliging een continu verbeterproces is.

Route naar de BIO-implementatie

Er zijn diverse routes voor implementatie van de BIO mogelijk. Voor elk van deze routes is het raadzaam om te starten met de tone-at-the-top. Over het belang van de BIO moet een duidelijk signaal en commitment vanuit het management worden afgegeven, waarin voor alle stakeholders duidelijk wordt waarom de BIO-implementatie prioriteit heeft. Voorbeelden hiervan betreffen kick-offsessies met het management, waarin draagvlak wordt gecreëerd voor het afleggen van de BIO-route. Vanuit het draagvlak op managementniveau worden bijvoorbeeld via interne communicaties andere lagen in de organisatie geïnformeerd over de implementatie. Om te bepalen hoe uitdagend de route naar de BIO-implementatie wordt, is het raadzaam om als organisatie voorafgaand aan de start een aantal vragen te beantwoorden. Allereerst is het raadzaam om de security governance in kaart

te brengen. Een intern gedragen overzicht wie welke rollen, verantwoordelijkheden en bevoegdheden heeft. Dit zorgt voor duidelijkheid vooraf. Hoe ziet de RACI (Responsible, Accountable, Consulted en Informed)-matrix eruit als het gaat om informatiebeveiligingsbeleid en implementaties? Is deze al beschreven en helder belegd, of is dit onderdeel van de BIO-implementatie? Mocht dit laatste onderdeel zijn van de implementatie zelf, dan betreft dit een van de eerste actiepunten.

In het verlengde hiervan is het belangrijk om de vraag te stellen of er al andere (security) baselines zijn geïmplementeerd. Denk hierbij bijvoorbeeld aan ISO 27001 en 27002, BIR, NIST security control baseline, COBIT of hardening baselines. De reden hiervoor is dat ervaring met de implementatie van andere baselines en de potentiële aansluiting daarop de implementatie van de BIO kan bevorderen én versnellen. Het Centrum Informatiebeveiliging en Privacybescherming (CIP) heeft een aantal handige producten online gepubliceerd die de implementatie kan ondersteunen, waaronder tools om een 'BIO Self Assessment' uit te voeren (Producten - bio-overheid). Deze tools kunnen een analyse van de volwassenheid van de huidige security governance ondersteunen.

Een andere relevante vraag om voorafgaand aan de implementatie te beantwoorden, is of er binnen de organisatie reeds security dan wel risk officers werkzaam zijn. Denk hierbij aan Business Security Officers (BSO's) en IB&P-coördinatoren. Zij beschikken veelal over kennis van de huidige status van beheersmaatregelen en (resterende) kwetsbaarheden binnen de organisatie. Zodoende kunnen zij de implementatie van de BIO begeleiden en de scope van de BIO-implementatie bepalen door middel van een risicogebaseerde aanpak.

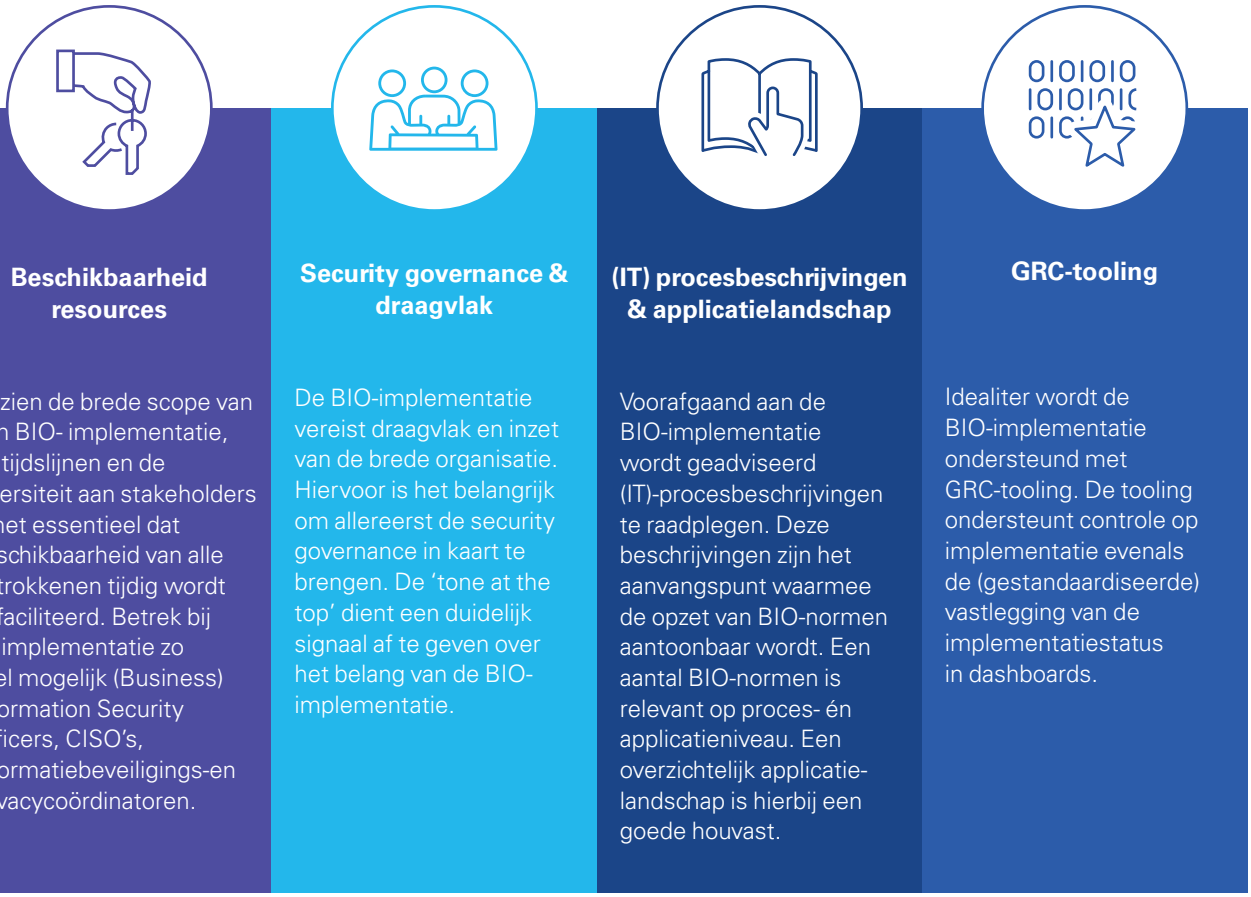
Voorafgaand aan de BIO-implementatie is het relevant om te beoordelen in hoeverre (IT-)processen zijn beschreven. Deze IT-processen kunnen het aanvangspunt zijn waarmee de opzet van BIO-normen aantoonbaar wordt gemaakt. Het is daarmee een stevig fundament voor verdere implementatie. Daarnaast bieden procesbeschrijvingen een basis voor het scherp krijgen van verantwoordelijkheden en daarmee welke afdeling of welk team verantwoordelijk is voor de implementatie van een set aan BIO-normen.

Naast de 'papieren basis' van (IT-)processen is het tevens relevant om te bepalen in hoeverre het applicatielandschap inzichtelijk is. Een aantal BIO-normen is relevant op proces- én applicatieniveau. Om een beeld te krijgen van de mate waarin BIO-normen op applicatieniveau kunnen worden geïmplementeerd, is een inzichtelijk applicatielandschap een goede houvast (om onder andere de omvang en diversiteit van het applicatielandschap en de toepasselijke BIO-normen te bepalen). Idealiter wordt een set aan BIO-normen toegepast op meerdere applicaties.

Behalve de aanwezigheid van eventuele andere security baselines, ervaring van het personeel, beschreven IT-processen en het applicatielandschap, is het tevens raadzaam om het gebruik van GRC-tooling te overwegen. Met meer dan honderd BIO-normen die al dan niet worden geïmplementeerd, is het verzamelen van bewijsmateriaal en het opvolgen van (potentiële) verbeteracties een omvangrijk proces. Dit proces wordt idealiter ondersteund met GRC-tooling, waarbij BIO-normen worden gekoppeld aan verantwoordelijke medewerkers. In de tooling kan controle op de implementatie worden uitgevraagd en de reacties daarop worden vastgelegd. De status hiervan wordt zichtbaar in diverse dashboards die de tooling mogelijk maakt. Een kanttekening bij het gebruik van GRC-tooling is dat de betrokken medewerkers – voorafgaand aan het gebruik – training ontvangen. Tevens is het raadzaam om één werkwijze te hanteren voor het invullen van de tooling, zodat deze door iedereen op dezelfde manier wordt ingevuld.

Tot slot is het raadzaam om vooraf te peilen of voldoende medewerkers beschikbaar zijn voor de implementatie. De implementatie van de BIO is – uiteraard mede afhankelijk van de scope – een omvangrijke opdracht. De ervaring leert dat het voor organisaties belangrijk is om medewerkers hiervoor (van bovenaf) tijdig te informeren, te trainen, en voldoende beschikbaar te maken. Een kwalitatief goede implementatie vraagt de nodige tijd, kennis en coördinatie van diverse medewerkers. Het is belangrijk om de benodigde tijd vooraf gedetailleerd in te schatten.

De volgende kritieke factoren zijn belangrijk om een BIO-implementatie binnen de gestelde tijd, het budget en de kwaliteitscriteria af te ronden:



Beschikbaarheid resources

Gezien de brede scope van een BIO- implementatie, de tijdslijnen en de diversiteit aan stakeholders is het essentieel dat beschikbaarheid van alle betrokkenen tijdig wordt gefaciliteerd. Betrek bij de implementatie zo veel mogelijk (Business) Information Security Officers, CISO's, Informatiebeveiligings-en privacycoördinatoren.

Security governance & draagvlak

De BIO-implementatie vereist draagvlak en inzet van de brede organisatie. Hiervoor is het belangrijk om allereerst de security governance in kaart te brengen. De 'tone at the top' dient een duidelijk signaal af te geven over het belang van de BIO-implementatie.

(IT) procesbeschrijvingen & applicatielandschap

Voorafgaand aan de BIO-implementatie wordt geadviseerd (IT)-procesbeschrijvingen te raadplegen. Deze beschrijvingen zijn het aanvangspunt waarmee de opzet van BIO-normen aantoonbaar wordt. Een aantal BIO-normen is relevant op proces- én applicatieniveau. Een overzichtelijk applicatie-landschap is hierbij een goede houvast.

GRC-tooling

Idealiter wordt de BIO-implementatie ondersteund met GRC-tooling. De tooling ondersteunt controle op implementatie evenals de (gestandaardiseerde) vastlegging van de implementatiestatus in dashboards.

Invulling van de route naar BIO-implementatie

In de voorgaande paragraaf zijn verschillende overwegingen toegelicht die relevant zijn voorafgaand aan de BIO-implementatie. Daarmee is het een typisch voorbeeld van 'bezint eer gij begint'. Als het gaat om de daadwerkelijke implementatie, zijn er opnieuw een aantal relevante keuzes te maken. De belangrijkste keuzes worden hieronder toegelicht.

- **Wat wordt de scope van de BIO-implementatie?** Hier zijn vele afwegingen in te maken (bij voorkeur risicogebaseerd), zoals de focus op kernprocessen of belangrijkste applicaties. Anderzijds kan ook gekozen worden om de focus eerst te richten op specifieke organisatieonderdelen (afdelingen/teams). Een suggestie is om niet met een te brede scope van start te gaan. Dit maakt het gemakkelijker om de scope in een later stadium gefaseerd uit te breiden.
- **Wat is het BBN-niveau?** De BIO onderscheidt drie basisbeveiligingsniveaus (BBN) op basis van generieke schades en bedreigingen. Een hoger BBN betekent een hogere potentiële impact van het risico. Aan elk BBN is een verplichte set aan maatregelen gekoppeld. Alle overheidssystemen moeten minimaal voldoen aan BBN 1. BBN2 gaat om het principe 'valt de maatregel onder goed huisvader-schap; toont deze beveiliging de betrouwbare overheid?' BBN3 is van toepassing op gerubriceerde informatie die Departementaal Vertrouwelijk dan wel vergelijkbaar is met vertrouwelijk op andere overheidslagen, waar weerstand tegen statelijke actoren of vergelijkbare dreigingsbronnen benodigd is. Het BBN-niveau is te vinden in de tweede kolom van links bij iedere control en maatregel (zie de afbeelding op pagina 2 over 'bescherming tegen malware'). Om te ondersteunen bij het bepalen van het BBN is er de BBN-toets (zie BBN-toets in Deel 2 van de BIO).

- **Waar zijn potentiële BIO-normen belegd binnen de organisatie?** Deze activiteit ligt dicht bij de kern van de implementatie zelf, namelijk het bepalen welke BIO-normen relevant zijn voor de organisatie. Hiervoor is het belangrijk om te weten waar zowel de uitvoering evenals de verantwoordelijkheid voor de BIO-normen is belegd. Een suggestie hierbij is om de hoofdstukken van de BIO hiervoor te hanteren (zoals 'Naleving' en 'Informatiebeveiligingsbeleid'). Het is onwaarschijnlijk dat alle hoofdstukken van de BIO binnen één afdeling zijn belegd. Sterker nog, hoe groter de organisatie, hoe waarschijnlijker het is dat de verantwoordelijkheden zijn verspreid. Uiteraard zijn er verschillende mogelijkheden om scherp te krijgen waar welk BIO-hoofdstuk is belegd: via interviews, workshops of een enquête. De keuze van de methode hangt af van de beschikbare tijd, de grootte van de organisatie, de mate van decentralisatie en de omvang van de scope.

- **Opzet, bestaan en werking tegelijkertijd toetsen?** Om de implementatie van BIO-normen aan te tonen, wordt doorgaans onderscheid gemaakt in de mate van implementatie: opzet, bestaan en (uiteindelijk) werking van beheersmaatregelen. Mede afhankelijk van de vragen bij de paragraaf 'Routeopties op weg naar de BIO-implementatie', is het raadzaam om te starten met opzet en bestaan. Zodra opzet en bestaan zijn aangetoond, kan de werking worden getoetst.

Opzet

De opzet van BIO-maatregelen staat voor het ontwerp, zoals beleid en procedures.

Bestaan

Het bestaan van BIO-maatregelen staat voor de Implementatie en daadwerkelijk toepassing.

Werking

De werking van BIO-maatregelen duidt op de effectiviteit ervan.

- **Wie valideert de implementatie?** Voor een objectieve beoordeling van de mate waarin BIO-normen zijn geïmplementeerd, kunnen diverse interne teams worden samengesteld. Denk daarbij aan een tweede- of derdelijnscontrolefunctie (zoals Compliance, Risicomanagement of Internal Audit). Hoewel de ICV geen geaccrediteerde externe organisatie vereist, is het raadzaam om een objectieve partij binnen de organisatie aan te stellen voor de controle op de implementatie.

- **Inrichting (half)jaarlijkse Plan-Do-Check-Act (PDCA)-cyclus?** De BIO-implementatie is geen eenmalige activiteit, maar leidt idealiter tot de inrichting van een PDCA-cyclus waarmee de borging van de implementatie wordt bewaakt. Het is belangrijk om de BIO-normen duurzaam in de organisatie te beleggen. Daarmee is de BIO meer dan enkel het behalen van de jaarlijkse ICV.

De BIO is meer dan de In Control Verklaring

Hoewel een BIO-implementatie jaarlijks wordt vertaald in een ICV, is dit niet hét jaarlijkse einddoel. Allereerst omdat de BIO in complexe organisaties duidelijkheid schept over de uitvoering van informatiebeveiliging en eenieders verantwoordelijkheden daarin. Met name in grote organisaties zijn de verantwoordelijkheden als het gaat om informatiebeveiliging veelal verspreid. De BIO verplicht Nederlandse overheidsorganisaties om per BIO-norm helder te hebben wie waarvoor verantwoordelijk is en hoe de invulling van de norm plaatsvindt.

Daarnaast biedt de BIO de mogelijkheid om normen af te stemmen op de organisatie, de organisatiecultuur en de gewenste wijze waarop informatiebeveiliging binnen de organisatie dient te opereren. De BIO biedt hierin veel flexibiliteit. Het is een raamwerk dat om de organisatie heen gebouwd kan worden. Het is geen stug stramien, maar een kneedbaar middel om het bewustzijn en de digitale weerbaarheid van de organisatie te vergroten. Echter, hiervoor is het belangrijk om veelvuldig te communiceren over de gekozen BIO-route en de praktische invulling ervan. Denk hierbij aan regelmatige interne communicatie, video's, werksessies, statusupdates, etc. Dit begeleidt de verandering die de BIO in werking stelt om informatiebeveiliging naar een hoger niveau te tillen.

De BIO vraagt om een jaarlijkse evaluatie van de implementatie en drijft daarmee continue verbetering op alle relevante BIO-normen. Dit heeft te maken met de wijze waarop de implementatie dient te worden aangetoond. Elk jaar wordt een review gedaan op de mate waarin wordt voldaan aan opzet, bestaan en werking van de BIO-normen (resulterend in een ICV). Hetgeen dit jaar voldeed aan opzet, maar niet aan bestaan, zal met de benodigde inspanning volgend jaar wel voldoen aan opzet én bestaan. De jaarlijkse rapportage hierover en de uitvoering van verbeteracties drijven continue verbetering als het gaat om het digitaal weerbaar(der) maken van de organisatie.

Daarnaast biedt de BIO een handvat voor de prioritering van verbeterinitiatieven. Op het gebied van informatiebeveiliging zijn vaak veel verbeteringen mogelijk. De BIO geeft hierbij richting door te focussen op de hoofdstukken die nog niet volledig zijn ingericht (bijvoorbeeld de hoofdstukken die niet voldoen aan opzet). Doordat verbeterinitiatieven jaarlijks worden gerapporteerd in de vorm van een ICV, blijft het onderwerp op de agenda.

Tot slot

De opdracht is helder: hanteer de BIO als basis voor de implementatie van informatiebeveiliging (Home NL - bio-overheid). De wijze waarop de implementatie plaatsvindt kent vele mogelijkheden en afwegingen. Een organisatie moet eerst inzicht krijgen in het reeds bestaande niveau van security governance. Dit betreft onder meer de beschreven securityprocessen, de capaciteit en ervaring van medewerkers, het applicatielandschap en eventuele GRC-tooling. Daarna is het belangrijk om allereerst te starten met de scope van de BIO-implementatie evenals de invulling daarvan, afhankelijk van de prioriteiten van de organisatie. Het is belangrijk om tijdens de implementatie de borging op lange termijn in het vizier te houden. Dit zorgt ervoor dat elk jaar wordt gestuurd op de continue verbetering van de cyberweerbaarheid. Mocht u ondersteuning wensen bij het opzetten van de BIO- implementatie, of vragen hebben over de BIO, kunt u contact opnemen met Annemarie Zielstra en/of Fleur Boor-Zeeman.

De twee volgende artikelen richten zich op verandermanagement en risicomanagement in het kader van BIO-implementatie.

Contact

Annemarie Zielstra
Partner | Cyber Strategy & Risk
Zielstra.Annemarie@kpmg.nl
T +316 12992883

Fleur Boor-Zeeman
Manager | Cyber Strategy & Risk
BoorZeeman.Fleur@kpmg.nl
T +316 19296294

KPMG.nl

home.kpmg/socialmedia