Berenschot

RAPPORT

Evaluatie Baseline Informatie-beveiliging Overheid (BIO)

67874 – 17 november 2022

RAPPORT

Evaluatie Baseline Informatiebeveiliging Overheid (BIO)

Luuk Stadhouders MSc CISM
Rianne Zivali-de Kievit MSc CISA CIPP/e
Ir. Harro Spanninga MMC
Lars van Bladel MSc

67874 – 17 november 2022

Inhoudsopgave

HOOFDSTUK 1

Inleiding

1.1 Aanleiding

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (hierna: BZK) heeft de stelselverantwoordelijkheid voor de Baseline Informatiebeveiliging Overheid (hierna: BIO).
De BIO is in december 2018 vastgesteld door de Ministerraad voor de Rijksoverheid. Daarvoor was door de gemeenten, waterschappen en provincies reeds besloten tot invoering van de BIO. De overheidslagen zijn in januari 2019 gestart met de implementatie van de BIO ter vervanging van de baselines die voorheen per bestuurslaag vastgesteld waren.

In de kamerbrief 'hoofdlijnen beleid voor digitalisering'[1] van de staatssecretaris van Koninkrijksrelaties en Digitalisering uit maart 2022, heeft informatiebeveiliging een belangrijke rol bij de vormgeving van de digitale transitie in Nederland. Informatiebeveiliging is een onderdeel van het digitale fundament. Het versterken van dat fundament zal plaatsvinden door onder andere actief te normeren. Een geëvalueerde en geactualiseerde BIO heeft een belangrijke rol op het gebied van normeren van het fundament.

1 Kamerstuk 26643, nr. 842

De huidige BIO stelt het als volgt: “De BIO beoogt [...] de beveiliging van informatie(systemen) bij alle bestuurslagen en bestuursorganen van de overheid te bevorderen, zodat alle onderdelen erop kunnen vertrouwen dat onderling uitgewisselde gegevens, in lijn met wet- en regelgeving, passend beveiligd zijn.”[2]

De BIO is onder meer gebaseerd op de internationale standaard ISO 27002. Dit jaar is er een nieuwe versie van de ISO 27002 gepubliceerd door de NEN. Bij de vaststelling van de BIO is afgesproken dat de BIO in 2023 geëvalueerd zou worden. In opdracht van BZK is in 2022 onderzoek uitgevoerd naar de impact van de komende ISO 27002 op de huidige BIO. Mede op basis van deze uitgevoerde impactanalyse is besloten dat de BIO de nieuwe ISO 27002 blijft volgen.[3] Daarom is de evaluatie van de BIO naar voren gehaald. Hierdoor kan een BIO 2.0 zowel wijzigingen naar aanleiding van de evaluatie als aanpassingen naar aanleiding van de nieuwe ISO 27002 bevatten. Het Directoraat-generaal Digitalisering en Overheidsorganisatie van BZK (hierna: DGDOO/BZK) heeft Berenschot gevraagd de evaluatie uit te voeren.

1.2 Vraagstelling

De gehele evaluatie van de BIO is opgesplitst in enerzijds een onderdeel over de ontwerpprincipes van de BIO (onderliggende evaluatie bestaande uit twee delen) en anderzijds een onderdeel over de inhoud van de overheidsmaatregelen (een derde onderdeel van de evaluatie). De eerste twee delen vallen binnen de reikwijdte van de evaluatieopdracht. De uitkomsten hiervan worden gebruikt voor het derde deel gericht op de verbeteringen voor de overheidsmaatregelen uit de BIO. De twee delen van onderliggende evaluatie zijn:

1. Het toetsen van de bestaansreden van de BIO bij bestuurders en hoogambtelijke vertegenwoordigers.
2. Evalueren welke verbeteringen op het instrument BIO mogelijk zijn in de ogen van de functionarissen die betrokken zijn bij de uitvoering c.q. implementatie.

We hebben hierbij gekeken naar de doelmatigheid van het instrument, oftewel zijn met de inzet van het instrument BIO de beoogde (beleids)doelen behaald, en is gekeken naar het doelbereik oftewel in hoeverre die doelen zijn bereikt en welke (neven)effecten zijn behaald.

De vragen die in de verschillende delen van de evaluatie aan de orde dienen te komen, zijn voorafgaand aan de opdracht door de opdrachtgever aan ons verstrekt. Deze vragen zijn vastgesteld in de werkgroep-BIO[4] en opgenomen in bijlage 1. Tevens heeft BZK voorafgaand aan de opdracht aangegeven welke stakeholders ten minste betrokken moeten worden in de evaluatie.

1.3 Doel van dit document

Het doel van dit eindrapport is een antwoord te geven op de vragen die aan ons zijn gesteld. De vragen worden beantwoord per onderdeel van de evaluatie. Ons rapport biedt inzicht in de wijze waarop wij tot deze antwoorden zijn gekomen. Ons rapport plaatst deze resultaten in de relevante context van de opgave voor BZK bij de vormgeving van de digitale transitie in Nederland.

1.4 Onderzoeksopzet

In bijlage 2 is de gehanteerde onderzoeksopzet en aanpak beschreven in de wijze waarop wij in nauwe samenwerking met de opdrachtgever en betrokken medeoverheden tot de resultaten zijn gekomen.

1.5 Leeswijzer

Het eindrapport is als volgt opgebouwd: in hoofdstuk 2 en 3 beschrijven we de twee onderdelen van de evaluatie. In hoofdstuk 2 wordt de bestaansreden van de BIO getoetst bij de bestuurders en hoogambtelijke vertegenwoordigers van de vier bestuurslagen. Op basis van de vastgestelde kaders en beoogde richting uit dit deel van de evaluatie is vervolgens in hoofdstuk 3 antwoord gegeven op welke verbeteringen op het instrument BIO mogelijk zijn. In hoofdstuk 2 en 3 beschrijven we telkens de synthese middels een analyse van de bevindingen. In hoofdstuk 4 geven we tot slot de conclusies en aanbevelingen.

2 Uit de BIO-versie 1.04zv
3 Zie https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/informatieveiligheid/kaders-voor-informatieveiligheid/baseline-informatiebeveiliging-overheid/

4 De interbestuurlijke werkgroep-BIO draagt zorg voor het onderhoud op de BIO. Onder het voorzitterschap van BZK zijn in de werkgroep-BIO de vier overheidskoepels vertegenwoordigd: CIO Rijk, Vereniging Nederlandse Gemeenten (VNG), InterProvinciaal Overleg (IPO) en Unie van Waterschappen (UvW). Verder bestaat de werkgroep uit een aantal grote uitvoeringsorganisaties: het Forum Standaardisatie, het Nationaal Cybersecurity Centrum en het Centrum voor Informatiebeveiliging & Privacybescherming.

HOOFDSTUK 2

Analyse deel 1

In deel 1 van de evaluatie is met bestuurders en hoogambtelijke vertegenwoordigers van alle bestuurslagen gekeken naar de bestaansreden van de BIO. In twee werksessies is op basis van een aantal vragen deze hoofdvraag beantwoord. De bevindingen uit dit eerste deel hebben na het eerste deel de evaluatie geleid tot het besluit[5] om door te gaan met het tweede deel van de evaluatie. In dit hoofdstuk worden de bevindingen en onze analyse en conclusies van deel 1 van de evaluatie beschreven.

5 Dit besluit is genomen door de opdrachtgever in samenwerking met de vier overheidslagen in het kern-IBO d.d. 9 september 2022.

2.1 Beleidsdoelen

Bij het opstellen van de BIO zijn vier hoofddoelen, ook wel beleidsdoelen genoemd, vastgesteld. Deze zijn als volgt geformuleerd en overgenomen uit de beschrijving van de opdracht voor de evaluatie:

- Het management in staat stellen om op basis van expliciete risicoafweging informatiebeveiligingsmaatregelen te kiezen, implementeren en uit te dragen.
- Voldoen aan specifieke wet- en regelgeving op het gebied van informatiebeveiliging.
- Veilige ketensamenwerking mogelijk maken met interne en externe partners.
- Fundamenteel beheer bieden.

In deze paragraaf worden de bevindingen beschreven in hoeverre de BIO bijdraagt aan deze beleidsdoelen en of deze beleidsdoelen nog relevant zijn.

2.1.1 Bijdrage aan huidige beleidsdoelen

Per huidig beleidsdoel wordt beschreven welke bevindingen de evaluatie heeft opgeleverd en welke conclusies we hieruit trekken.

2.1.1.1 Het management in staat stellen om op basis van expliciete risicoafweging informatie-beveiligingsmaatregelen te kiezen, te implementeren en uit te dragen.

In algemene zin geldt dat de deelnemers de BIO zien als een sterke overheidsbrede basis, die bijdraagt aan de digitalisering van Nederland en het vertrouwen in overheidsdienstverlening. De BIO heeft daarbij, zo wordt gesteld, een doorwerkend effect naar accountability tussen (keten)partners. Ook draagt de BIO bij aan het vertrouwen van de samenleving in de informatiebeveiliging binnen de overheid. Met andere woorden: door actief te normeren op basis van een overheidsbrede baseline draagt de BIO bij aan het versterken van het digitale fundament van de overheid.

Naast het vergroten van het vertrouwen heeft de BIO ook een sterke bijdrage geleverd aan het op de politieke agenda krijgen van informatiebeveiliging binnen individuele organisaties en tussen de organisaties. Door de komst van de BIO is informatiebeveiliging zowel bij de ambtelijke top als op de bestuurlijke tafel meer onderwerp van gesprek geworden. Informatiebeveiliging wordt meer en meer in ogenschouw genomen bij nieuwe ontwikkelingen.

Ook draagt de BIO door de doorwerking binnen een organisatie bij aan het gesprek over welke beveiligingsmaatregelen gekozen en geïmplementeerd moeten worden.

Tegelijkertijd moet echter geconstateerd worden dat de BIO 'slechts' een goede basis vormt. Indien organisaties daadwerkelijk invulling aan de BIO geven middels adequaat en reeds ingebed risicomanagement, wordt de BIO pas meer dan een basis. Momenteel ziet men vooral dat de BIO te vaak compliancy-gedreven wordt geïmplementeerd en toegepast binnen publieke organisaties. Het hanteren als een 'afvinklijst' uit zich in het feit dat op basis van de basisbeveiligingsniveaus (hierna: BBN's) 'zonder nadenken' risico's vastgesteld worden en de bijbehorende maatregelen worden geïmplementeerd. Het ontbreekt aan de afweging wat nodig is voor de feitelijke 'echte' informatieveiligheid[6]. Men gaat daarmee voorbij aan het definiëren van benodigde aanvullende maatregelen bij de controls. Hoewel risicomanagement in de BIO dus de facto wordt benoemd, komt het beleidsdoel risicomanagement, zo is het gedeelde beeld van de deelnemers, onvoldoende naar voren in de BIO. Dit leidt er toe dat het management in onvoldoende mate de risico's afweegt en op basis van het pas-toe-of-leg-uit-principe informatiebeveiligingsmaatregelen kiest, implementeert en uitdraagt. Met andere woorden: in veel publieke organisaties wordt het gesprek over risicobeheersing onvoldoende gevoerd en toegepast. De BIO verwijst slechts en is hierin onvoldoende voorschrijvend. Dit kan volgens de deelnemers actiever gefaciliteerd worden door bijvoorbeeld een (organisatiebrede, strategische) risicomanagement framework toe te voegen. Ook vraagt een aantal deelnemers zich af of het op sommige plekken in de BIO 'dichttimmeren van controls met maatregelen' geen averechts effect heeft op het toepassen van risicomanagement.

6 Bij 'feitelijke' informatieveiligheid gaat het om de daadwerkelijk, objectief aantoonbare status van de informatieveiligheid van een (keten van) organisatie(s) op basis van bijvoorbeeld een penetratietest, vulnerability assessment of (IT-)audit.

Analyse en geïdentificeerde verbetermogelijkheden Berenschot

- De BIO draagt bij aan het bereiken van versterken van het digitale fundament, maar biedt soms ook onterecht de verwachting bij bestuurders dat voldoen aan de BIO betekent dat de feitelijke informatieveiligheid van de organisatie op orde is. Met andere woorden: voor bestuurders is in de beeldvorming rondom de BIO onvoldoende duidelijk dat feitelijke informatieveiligheid verder gaat dan het afvinken van BIO-maatregelen. De opgave ligt deels in de beeldvorming, waarbij de BIO wordt gezien als 'afvinklijst'. Een kanteling van dit beeld vraagt meer dan een inhoudelijke wijziging van het normenkader en ligt voornamelijk in het begrijpen wat er in de volledige breedte (en dus breder dan de BIO) nodig is om goed invulling te geven aan informatiebeveiliging, inclusief de rol en betekenis van een normenkader daarbinnen.
- Hoewel risicomanagement als cruciale basis wordt benoemd in de BIO, is 'organisatiebreed' risicomanagement (dus breder dan op het gebied van informatiebeveiliging) bij veel organisaties niet of onvoldoende ingericht. Hierdoor worden bij specifieke risico's op informatiebeveiliging onvoldoende of niet altijd op de juiste wijze maatregelen genomen of wordt onvoldoende invulling gegeven aan eigenaarschap en verantwoordelijkheden.
- Het management krijgt vanuit het instrument BIO onvoldoende handvatten mee om een expliciete risicoafweging te doen en dit daadwerkelijk te implementeren in een bredere context van (strategisch) risicomanagement. Onderliggende vraag is of het inrichten van organisatiebreed risicomanagement 'slechts' randvoorwaardelijk is voor het adequaat toepassen van de BIO of dat de BIO zou moeten ondersteunen bij het neerzetten van organisatiebreed risicomanagement. De BIO is dan een normenkader met geïntegreerd risicomanagement framework. Het eerste heeft onze voorkeur, waarbij wel rule-based voorschriften kunnen worden opgenomen. Zie ook de conclusies en aanbevelingen in hoofdstuk 4. Een expliciete beleidskeuze (en uitwerking van die keuze), is noodzakelijk bij het bereiken van dit beoogde beleidsdoel.
- Het is van belang om de BIO praktisch toepasbaar te houden. Dit betekent dat er meer aandacht voor uitwerking van de controls in de BIO mag zijn ('wat'), maar vervolgens beperkter voorgeschreven hoeft te worden 'hoe' voldaan moet worden aan de controls. Wat kan helpen als alternatief voor het 'dichttimmeren van controls met maatregelen' is werken met en blijven uitdragen van handreikingen en best practices voor de praktische implementatie van de betreffende controls. Maak hierbij gebruik van een verwijzing van de BIO naar vertegenwoordigende organisaties waar best practices te vinden zijn.

2.1.1.2 Voldoen aan specifieke wet- en regelgeving op het gebied van informatiebeveiliging

Hoewel de BIO primair een baseline is in generieke zin voor informatiebeveiliging, draagt het ook bij aan het voldoen van meer specifieke wetgeving. De deelnemers aan de evaluatie geven aan dat de BIO bijdraagt aan overzicht hebben van relevante wet- en regelgeving en het een goede opstap biedt om te voldoen aan die wet- en regelgeving.

Hier ligt echter ook een valkuil volgens de deelnemers. De BIO levert slechts een bijdrage aan het in- en overzicht. Ten onrechte ontstaat hierdoor ook het beeld dat het voldoen aan de BIO ook betekent dat een organisatie voldoet aan alle relevante wet- en regelgeving, waarbij zelfs in een enkel geval het beeld ontstaat dat incidenten uitgesloten zijn als organisaties voldoen aan de BIO.

In meer algemene zin concluderen de deelnemers dat het onvoldoende gelukt is om (de ontwikkeling van) aparte normen vanuit de Rijksoverheid te beperken. Het gevolg daarvan is dat dit leidt tot onwenselijke en nodeloos complexe situaties voor de verschillende overheidslagen. Er bestaan veel verschillende stelsels inclusief sectorale wetgeving op het gebied van informatiebeveiliging.

Departementen houden vaak vast aan eisen en normen die niet in de BIO zijn opgenomen of weer net afwijken van hetgeen gesteld in de BIO, of zelfs conflicterend zijn.

Analyse en geïdentificeerde verbetermogelijkheden Berenschot

- De BIO draagt als kapstok bij aan het beleidsdoel 'het voldoen aan wet- en regelgeving' en maakt deels inzichtelijk voor bestuurders en het hoger management welke normen gelden.
- Mede dankzij de BIO is reductie van het aantal toe te passen normen gerealiseerd, met name via ENSIA voor gemeenten. Echter blijft het terugdringen van het aantal (elkaar conflicterende) normen een belangrijke opgave voor bestuurders en hoger management. Het wettelijk verankeren van de BIO zal hierbij een belangrijke verbetering teweegbrengen, aangezien vanuit ieder stelsel hiermee rekening gehouden dient te worden.

2.1.1.3 Veilige ketensamenwerking mogelijk maken met interne en externe partners

Mede door een grote diversiteit binnen de verschillende overheidslagen is dé digitale overheid momenteel erg gefragmenteerd en versnipperd. Daarbij is het moeilijk om daar grip op te krijgen. Standaarden en normenkaders helpen bij het verkrijgen van grip op de digitale overheid, mits goed gehanteerd en gehandhaafd. Een instrument als de BIO helpt niet alleen in het spreken van dezelfde taal binnen de digitale overheid, maar biedt daarmee ook de mogelijkheid om gemakkelijk eenduidige eisen binnen een keten te stellen.

Doordat de BIO een 'gezamenlijke taal' creëert, is het een goed instrument om in dienstverleningsketens gezamenlijk de informatiebeveiliging te verbeteren. Een goed voorbeeld hiervan zijn de cyberoefeningen die waterschap Noorderzijlvest met de Veiligheidsregio heeft gedaan. Hier kwam naar voren dat informatiebeveiliging rondom bijvoorbeeld waterzuiveringsinstallaties gezamenlijk gedaan moet worden, omdat de gesimuleerde cyberaanval zich in de keten uitbreidde via gekoppelde systemen. De BIO biedt dan een basis om gezamenlijk de informatiebeveiliging in die keten te verbeteren.

Toch geeft men ook aan dat 'vertrouwen op de BIO' niet volstaat. Hiervoor worden twee belangrijke argumenten aangedragen door de deelnemers. Ten eerste betekent het stellen van eisen of normen niet dat de ketenpartner het ook daadwerkelijk goed ingericht heeft. Het adagium 'vertrouwen is goed, controle is beter' wordt hierbij aangehaald. Bestuurders en hoogambtelijke vertegenwoordigers ervaren dit ook in de eigen organisatie. Zo benoemen zij dat ze vaak een positief verhaal horen van de CISO's wanneer ze vragen naar de implementatie van de BIO. Wanneer ze dan vragen of er ook getoetst is op de daadwerkelijke implementatie en de effecten ('werking') ervan, dan is dat vaak niet gedaan. Ten tweede, in lijn met de bevindingen rondom risicomanagement, wordt te gemakkelijk op 'maatregelniveau' gekeken. Hierbij wordt slechts vanuit compliancy gekeken naar datgene wat er in de BIO gesteld wordt. Een expliciete risicoafweging voor aanvullende maatregelen wordt veelal overgeslagen.

Daarnaast wordt aangegeven dat het geregeld gebeurt dat de gehele BIO opgelegd wordt binnen ketens en in aanbestedingen. Waar dit bij ketenpartners binnen de overheid niet direct tot een probleem zou moeten leiden omdat de BIO immers toch van toepassing is, kan gesteld worden dat op deze manier voorbij gegaan wordt aan het beleidsdoel van (feitelijke) veilige samenwerking. In aanbestedingen past een dergelijke verplichting nog minder, omdat zaken die niet relevant zijn voor de specifieke dienstverlening toch opgelegd worden. In een context met internationale ketenpartners is een dergelijke verplichting van de BIO daadwerkelijk een belemmering. De BIO is immers een Nederlandse overheidsnorm. In zulke gevallen wordt de ISO 27001 geprefereerd.

In meer algemene zin zijn er deelnemers die pleiten voor een nadrukkelijker gebruik van of zelfs vervanging van de BIO door de ISO 27001- en ISO 27002-normen en de daarbij behorende mogelijkheden van certificering. De gedachte van certificering, zo geven zij aan, is belangrijk: de BIO kan als te vrijblijvend worden ervaren. De ISO-normen worden daarnaast vaker geëvalueerd en zijn inwisselbaar met andere ketenpartners buiten de overheid. Het kan veilige ketensamenwerking gemakkelijker maken wanneer wordt aangesloten op de ISO-normen, met een addendum voor zaken voor de overheid die niet in de ISO zitten.

Analyse en geïdentificeerde verbetermogelijkheden Berenschot

- De BIO biedt een goede basis en gezamenlijke taal voor het beleidsdoel samenwerking op het gebied van informatiebeveiliging in ketens (tussen overheidspartijen).
- Een normenkader dat enkel van toepassing is op overheidspartijen is echter niet ideaal in de ketensamenwerking met organisaties buiten de overheid of in een internationale context. Voorgaande moet tevens bezien worden in de context van de eerder beschreven beperkingen die de BIO kent op het gebied van risicomanagement. Expliciteer de maatregelen uit hoofdstuk 4 van de BIO met betrekking tot externe dienstenleveranciers om vast te stellen of deze voldoen aan de BIO ('statement of compliancy').

2.1.1.4 Fundamenteel beheer bieden

Van de vier beleidsdoelen werd het beleidsdoel 'fundamenteel beheer bieden' het minst herkend door de deelnemers. Deelnemers zien dat fundamenteel beheer, als organisatiebreed en regulier goed ingericht hebben van informatiemanagement en databeheer, verweven zit in een deel van de gestelde controls. Door de deelnemers wordt dit beleidsdoel in een bredere context geplaatst dan uitsluitend informatiebeveiliging. In die context constateert men dat de BIO in ieder geval bijdraagt.

Analyse en geïdentificeerde verbetermogelijkheden Berenschot

- De BIO draagt bij aan het bieden van fundamenteel beheer vanuit een bredere benadering van dit onderwerp.
- Van alle beleidsdoelen wordt fundamenteel beheer het minst herkend en meer beschouwd als een gegeven dat er een verband is tussen fundamenteel beheer en informatiebeveiliging. Het doelbereik is beperkt, maar dit is ons inziens ook passend bij de aard van het beleidsdoel. Behoud dit beleidsdoel bij de BIO 2.0.

2.1.2 Relevantie beleidsdoelen in huidige en toekomstige context

De BIO als instrument heeft toegevoegde waarde voor de bestuurlijke en hoogambtelijke deelnemers. Dit is een belangrijke basis om een uitspraak te doen over de bijbehorende beleidsdoelen. Op dit punt is er eensgezindheid onder de deelnemers. De deelnemers vinden de beleidsdoelen nog altijd relevant en zijn van mening dat deze ook in de toekomst standhouden. Men heeft geen directe aanvullingen voor de beleidsdoelen.

Indirect maken we echter gedurende de sessies en niet specifiek bij de vraag op dit onderdeel, op uit de door de deelnemers gedeelde beelden dat er behoefte is aan meer verbinding met de feitelijke informatieveiligheid dan nu ervaren wordt binnen de BIO. Vanuit de deelnemers wordt aangegeven graag meer focus te willen leggen op het verhogen van de volwassenheid van de organisaties op het gebied van informatiebeveiliging. Het gaat daarbij ook om vanuit dat perspectief daarover het gesprek te voeren. De BIO leidt te vaak en wellicht onbewust tot een focus op compliancy, zo geeft men aan. Dit staat in contrast met het beoogde uiteindelijke doel om informatiebeveiliging als vanzelfsprekend onderdeel te zien van wat er gebeurt binnen een organisatie. Het 'sturen op volwassenheid' kan helpen om te voorkomen dat informatiebeveiliging een eenmalige inspanning of het aflopen van een afvinklijst is. Een hogere volwassenheid helpt om informatiebeveiliging daadwerkelijk onderdeel te laten zijn van de PDCA-cyclus en draagt daarmee bij aan feitelijke informatieveiligheid.

Bovendien geven de deelnemers aan dat het gebruik van een dergelijk geambieerd volwassenheidsniveau meer handelingsperspectief geeft voor organisaties in de doorontwikkeling naar dat geambieerde niveau.

Analyse en geïdentificeerde verbetermogelijkheden Berenschot

- De BIO als instrument (met de huidige beleidsdoelen) heeft toegevoegde waarde voor bestuurders en draagt in algemene zin bij aan (het bereiken van) de beoogde beleidsdoelen.
- Het beleidsdoel *'sturen op volwassenheid van organisaties'* opnemen als aanvullend beleidsdoel en hier in de BIO 2.0 meer uitwerking aan geven, draagt bij aan de wens van bestuurders om meer sturing te kunnen geven aan informatiebeveiliging.

2.2 Opzet van het instrument BIO

2.2.1 Rule-based en principle-based

In de BIO wordt een mix gehanteerd van voorschrijvende maatregelen (rule-based) en meer open controls met uitgangspunten die naar eigen invulling van organisaties ingevuld dienen te worden (principle-based). Aan de deelnemers van de sessies is gevraagd of deze gehanteerde mix een juiste is.

De BIO heeft in de huidige vorm een grote bijdrage geleverd aan het bestuurders bewust maken van het belang en de urgentie van informatiebeveiliging. Uitgangspunt voor de inrichting van het instrument moet volgens de deelnemers dan ook zijn dat het maximaal bijdraagt aan deze bewustwording. Ook moet het bijdragen aan het feit dat bestuurders over de gehele linie betrokken moeten worden bij informatiebeveiliging en niet pas wanneer het verkeerd gaat of dreigt te gaan.

De deelnemers in de sessies geven echter aan dat er soms behoorlijk geworsteld wordt met wanneer en hoe je een control toepast. Veelal is men daarom op zoek naar aanvullende richtlijnen en niet per se naar voorschrijvende maatregelen. Wat in elk geval onderschreven wordt, is dat het nuttig is dat de BIO voorschrijvend is wanneer risico's hiertoe aanleiding geven. Of de huidige mix dan de juiste is, vinden ze echter lastig te beantwoorden. Zo wordt het voorbeeld aangehaald van de maatregel over wachtwoordbeleid (control 9.4.3.1) waarin gesteld wordt dat een wachtwoord minimaal acht tekens moet hebben. Dit is een achterhaalde maatregel en leidt zelfs tot onveilige situaties.

In zo'n geval kun je beter géén voorschrijvende maatregelen hebben, zo constateren de deelnemers. De BIO is, met andere woorden, op dit punt té voorschrijvend geweest. Op andere punten van de BIO had men meer rule-based echter juist wel passend had gevonden. Bijvoorbeeld omdat de principle-based controls daar tot onduidelijkheid in implementatie kunnen leiden die vervolgens in ketensamenwerking weer tot misverstanden of onbegrip over en weer leiden.

Het beginsel principle-based zou het uitgangspunt moeten zijn, totdat blijkt dat op een specifiek aspect rule-based noodzakelijk is voor het uniform mitigeren van risico's overheidsbreed. Als randvoorwaarde voor principle-based ziet men adequate toetsing op de implementatie en 'werking'. Men constateert dat bij een meer principle-based inrichting ook meer hulpmiddelen voor praktische implementatie welkom zijn.

Als aanvulling op de rule-based controls concluderen de deelnemers nog dat een voorspelbaar onderhoudsregime randvoorwaardelijk is. Alleen wanneer de maatregelen ook daadwerkelijk up to date zijn, dragen ze bij aan feitelijke informatieveiligheid. Deze voorspelbaarheid helpt organisaties in het kunnen anticiperen op wijzigingen.

Analyse en geïdentificeerde verbetermogelijkheden Berenschot

- De BIO is een passende mix bestaande uit principle-based en rule-based controls. Slechts daar waar het vanuit expliciete risico's noodzakelijk is om voorschrijvend te zijn, is rule-based zinvol.
- Zorg bij rule-based dat de mate van voorschrijving past bij de dreigingsontwikkelingen en dat de maatregelen zoveel mogelijk onafhankelijk zijn van de techniek.
- Zorg waar mogelijk, als aanvulling op de BIO, voor praktische richtlijnen en handreikingen voor concretisering van controls.
- Zorg bij controls zonder expliciete maatregelen voor adequate toetsing.
- Zorg voor een voorspelbaar onderhoudsregime, waarbij bij wijzigingen duidelijk is op welk moment aan welke gewijzigde maatregelen moet worden voldaan.

2.2.2 Samenhang met ISO en andere normen

De BIO is gebaseerd op de internationaal geaccepteerde standaarden ISO 27001 en de ISO 27002. De gedachte hierbij is dat het hanteren van deze internationaal geaccepteerde standaarden de afstemming van de informatiebeveiligingsbehoefte met externe leveranciers vergemakkelijkt.

De deelnemers aan de sessies herkennen dat het hanteren van deze normen inderdaad het gesprek met leveranciers over informatiebeveiligingsbehoeften eenvoudiger heeft gemaakt. Dit is tweeledig: het geeft meer richting aan wat je zelf hoort te vragen vanuit een organisatie waardoor het eenvoudiger is om hierop te toetsen en zorgt er voor leveranciers voor dat er geen wirwar aan regels ontstaat bij elke aanbesteding. Ondanks dat het gesprek met leveranciers eenvoudiger is, geven sommige organisaties aan juist onduidelijkheid te ervaren of dat in een concreet geval de BIO of de ISO 27001 (in zijn geheel) of slechts een subset van één van beide zou moeten gelden voor leveranciers.

De deelnemers merken ook op dat ze soms enig ongemak ervaren wanneer aan leveranciers een ISO-certificering als verplichting gevraagd wordt en overheidsorganisaties zichzelf dit dan weer niet opleggen als verplichting. Ook hier wordt, net als eerder, het punt naar voren gebracht dat wellicht een ISO-certificering met een BIO als addendum met aanvullende maatregelen wellicht passender is. Dit heeft als bijkomend voordeel dat het onderhoud van de BIO lichter en eenvoudiger wordt, omdat organisaties zich nu eenmaal moet aanpassen aan vernieuwingen van de ISO-standaard bij certificering.

Analyse en geïdentificeerde verbetermogelijkheden Berenschot

- Het hebben van de ISO 27001 en ISO 27002 als basis voor de BIO wordt breed onderschreven.
- De algemene tendens in de bestuurlijke sessies is dat overheden zelf meer moeten aansluiten op de ISO-standaarden en alleen afwijken waar dat nuttig of noodzakelijk is. Een deel van de deelnemers stelt voorstander te zijn van certificering op de ISO 27001 aangevuld met BIO-normen in een addendum. Hierover is echter geen consensus onder de deelnemers.

2.3 Wijze van verplichting

2.3.1 Zelfregulering

De BIO wordt binnen de overheid toegepast op basis van verplichtende zelfregulering. Er is vooralsnog geen wettelijke verankering voor de BIO. De vraag die leeft, is dan ook of hiermee de BIO voldoende zekerheid biedt. De deelnemers stellen dat het verplichtende karakter van de zelfregulering heeft bijdragen aan het op de kaart zetten van informatiebeveiliging binnen overheidsorganisaties. In het verlengde daarvan hebben overheidsorganisaties meer verantwoordelijkheid genomen ten aanzien van hun informatiebeveiliging. In de huidige opzet behoudt de BIO echter een bepaalde mate van vrijblijvendheid. Met andere woorden: de deelnemers ervaren de BIO lang niet altijd als een verplicht normenkader. Gezien de consensus dat de vrijblijvendheid in de huidige context niet meer passend is, is er brede steun voor een meer verplichtend karakter dan nu het geval is. Minder ruimte voor vrijheid en heldere consequenties bij het niet-voldoen, zou een verbetering zijn, aldus de deelnemers. Een dergelijk meer verplichtend of dwingend karakter kan liggen in een wettelijke verankering, maar ook in scherper toezicht op de BIO.

Informatiebeveiliging is een hygiënefactor en noodzakelijk voor een organisatie om invulling te geven aan informatieveiligheid. Als een organisatie hieraan onvoldoende doet, is de basis niet op orde. De keerzijde van hygiënefactoren binnen organisaties is echter dat ze de neiging hebben het onderspit te delven wanneer andere belangrijke of meer urgente problemen of opgaven op de bestuurlijke agenda komen. Het voldoen aan wet- en regelgeving staat hoger op de agenda dan iets wat niet (wettelijk) verplicht is. Daarnaast verschaft een meer verplichtend karakter ook een sterkere positie aan de informatiebeveiligingsorganisatie om maatregelen daadwerkelijk door te voeren.

Ook merken deelnemers op dat juist een hogere mate van verplichting kan leiden tot lastenverlichting. Wanneer er één duidelijk geldend kader is voor iedereen, dan is er minder ruimte voor aparte stelsels om eigen eisen te stellen op het gebied van informatiebeveiliging. Hierbij delen de gemeentelijke deelnemers hun ervaringen met ENSIA waarin stelselhouders van eigen normen zijn afgestapt en deze hebben geplot op de BIO, en zo een minder divers geheel aan normen ontstond. Dit zou men graag nog breder toegepast willen zien, zodat de regels op het gebied van informatiebeveiliging overzichtelijker worden en de auditlast wordt verminderd.

Analyse en geïdentificeerde verbetermogelijkheden Berenschot

- De huidige zelfregulering heeft organisaties veel gebracht en heeft ervoor gezorgd dat overheidslagen hun verantwoordelijkheid hebben gepakt waardoor aan de beoogde (beleids-) doelen van de BIO is bijgedragen.
- De ervaren vrijblijvendheid is echter niet meer passend in het huidige stelsel en het bereiken van het beoogd effect. In elk geval moeten er adequate waarborgen komen om de ervaren vrijblijvendheid weg te nemen. Dit kan zowel door meer autoriteit en toezicht in te stellen op het gebied van informatiebeveiliging als door een wettelijke verankering (zoals reeds beoogd in de Wet Digitale Overheid).

2.4 Toetsing en verantwoording

Eén van de gedachten achter de BIO is dat de BIO bijdraagt aan de interne transparantie en helpt bij het toe bewegen naar single audit voor stelselhouders. In die situatie is de BIO een uniform sturingsmiddel die overheidsbreed een gewenst niveau bepaalt. Hier valt volgens deelnemers nog veel winst te behalen. Met name het reeds genoemde feit dat stelselhouders nog te vaak en teveel aanvullende eisen opleggen naast de BIO komt hier duidelijk naar voren. Waar deelnemers uit gemeenten zien dat voor bijvoorbeeld SUWI, BRP en Reisdocumenten nu getoetst wordt langs normen van de BIO, houden andere stelselhouders vast aan hun eigen normen die weer net anders zijn dan de BIO. Hierdoor is de auditlast hoger dan gewenst en hoger dan noodzakelijk volgens de deelnemers. Zo werd als voorbeeld de DigiD-audit besproken. Hierin zitten een heel aantal technische normen die duidelijk aanvullend zijn op de BIO en hier ook niet in vervat zouden moeten worden. Er zitten echter ook meer beleidsmatige en procesmatige normen in die weldegelijk ook in de BIO zitten. Doordat deze normen echter net anders gesteld zijn en apart getoetst worden, brengt dit een dubbele auditlast met zich mee.

In de gewenste situatie is de BIO de standaard, de baseline, waarop aanvullingen gedefinieerd worden. En niet, zoals nu, een normenkader naast allerlei andere normenkaders binnen diverse stelsels. Deze kaders vanuit stelsels leiden niet alleen tot lastenverhoging, maar zijn ook vaak onduidelijk of zelfs conflicterend met de BIO. De BIO moet niet té complex of allesomvattend worden, maar wel gelden als basis voor het geheel. Aan stelselhouders is dan de vraag om informatiebeveiligingsnormen te definiëren die - op basis van dreigingen en risico's - nodig zijn aanvullend op de BIO.

Een dergelijke definiëring draagt bij aan de vereenvoudiging van de regels en aan het verlagen van de auditlast.

Een ander uitgebreid besproken onderwerp is de vraag in hoeverre overheidsorganisaties elkaar moeten controleren. Een voorbeeld wat in één van de sessies uitgebreid besproken werd, is het onderzoek van de Algemene Rekenkamer naar de Corona Check-app. In het onderzoek 'Staat van de Rijksverantwoording 2021[7]' staat te lezen: *"Na een incident met een van de commerciële testaanbieders scherpte de minister van VWS de vereisten voor aansluiting en de controles op informatiebeveiliging en autorisatiebeheer aan. Uit ons onderzoek blijkt dat de controles bij organisaties als de GGD en het RIVM veel minder intensief zijn. De minister van VWS gaat ervan uit dat deze overheidsorganisaties voldoen aan de regels hiervoor. Wij bevelen de minister aan dit voortaan zelf vast te stellen."*

De deelnemers stellen dat het vanuit de BIO niet duidelijk is wanneer extra controle plaats zou moeten vinden en vinden de conclusie van de Algemene Rekenkamer weliswaar begrijpelijk gezien de aard van de verwerking, maar vragen zich af wanneer het gerechtvaardigd is om de administratieve lasten van overheidsorganisaties, gefinancierd door gemeenschapsgeld, te rechtvaardigen. Moet de samenleving er niet van op aan kunnen dat andere overheidsorganisaties gewoon voldoen aan de BIO, zo wordt in de sessies gesteld? Vanuit de financiële sector wordt door de toezichthouder precies beschreven wat je bij andere organisaties dient te checken. Wellicht is dat, aldus de deelnemers, de situatie waar je met de BIO ook naartoe moet bewegen.

Analyse en geïdentificeerde verbetermogelijkheden Berenschot

- De huidige situatie waarin de BIO en andere regels deels overlappend en soms ook conflicterend zijn, is onwenselijk. In een ideale situatie geldt de BIO als basis voor informatiebeveiliging bij de overheid en wordt slechts op basis van risico's vanuit stelsels gesteld welke aanvullende eisen aan de BIO noodzakelijk zijn voor de beveiliging van de data of systemen.
- We onderschrijven het belang van waar mogelijk uitgaan van single information, single audit. Ook vanuit dit principe heb je als opdrachtgever, ons inziens, wel de verplichting na te gaan of de andere partij daadwerkelijk voldoet. Zeker wanneer de belangen groot zijn. Je hoeft dan alleen geen extra audit uit te voeren, maar doet dit op basis van een generieke audit. Waar nodig met de hierboven genoemde extra eisen als aanvulling. De financiële sector biedt hiervoor een lonkend perspectief.

2.5 Conclusie evaluatie deel 1

Uit dit eerste deel van de evaluatie met bestuurders en hoogambtelijke vertegenwoordigers blijkt er steun te zijn voor de BIO als middel om de informatieveiligheid te verhogen. Deze steun is op voorwaarde dat de BIO moet blijven bijdragen aan het verhogen van de feitelijke informatieveiligheid. Dientengevolge dient de BIO dus voldoende actueel te blijven.

Wij concluderen dat de deelnemers op bestuurlijk en hoogambtelijk niveau meerwaarde zien in het feit dat met de BIO op uniforme wijze voldaan kan worden aan het gestelde minimumniveau. De bijdrage die wordt geleverd aan de beoogde beleidsdoelen kan worden onderschreven en de bestaansreden van de BIO wordt door de bestuurlijke en hoogambtelijke vertegenwoordigers bevestigd. De geïdentificeerde verbetermogelijkheden van de BIO zijn: de wijze waarop risicomanagement al dan niet onderdeel is van de BIO, 'feitelijke informatieveiligheid' wordt gemist, een uitbreiding van de beleidsdoelen, er wordt niet op getoetst en de ervaren vrijblijvendheid dient te worden weggenomen. De bevestigde bestaansreden en deze aspecten vormen de vastgestelde kaders voor deel twee van de evaluatie.

7 Zie 'Staat van de rijksverantwoording 2021 (Algemene Rekenkamer, 2022) Geraadpleegd via https://www.rekenkamer.nl/binaries/rekenkamer/documenten/rapporten/2022/05/18/staat-van-de-rijksverantwoording-2021/SRV+220517+WR.pdf

HOOFDSTUK 3

Analyse deel 2

Met deel twee van de evaluatie is gestart, nadat de conclusie uit deel één was dat de BIO bestaansrecht heeft.[8] In dit deel is gekeken naar verbetermogelijkheden voor het instrument BIO aansluitend op de uitkomsten van en binnen de kaders uit het eerste deel van de evaluatie.

8 Dit besluit is genomen door de opdrachtgever in samenwerking met de vier overheidslagen in het kern-IBO d.d. 9 september 2022.

3.1 Beleidsdoelen

3.1.1 Bijdrage aan huidige beleidsdoelen

Evenals in deel één van de evaluatie is gestart met het toetsen of de huidige beleidsdoelen van de BIO herkend worden en (nog) volstaan. Per beleidsdoel is een uitwerking hiervan gemaakt.

Het management in staat stellen om op basis van expliciete risicoafweging informatiebeveiligingsmaatregelen te kiezen, te implementeren en uit te dragen

Evenals de bestuurders en hoogambtelijke vertegenwoordigers stellen de uitvoerende functionarissen in de vragenlijst dat er beperkt gestuurd wordt op informatiebeveiliging op basis van risico's. De deelnemers vinden dat risicomanagement een te beperkt onderdeel is van de BIO en nadrukkelijker aandacht zou moeten krijgen. De BIO draagt bij aan het op orde krijgen van het digitale fundament van organisaties. Informatiebeveiliging is zogezegd geen *"broodje speciaal"* meer en de BIO wordt door sommigen zelfs gezien als cruciaal voor het op orde krijgen en houden van informatiebeveiliging, mits goed toegepast. Zo biedt de BIO een concreet en gedeeld beeld binnen de overheid waar aan gewerkt moet worden, en kan men op basis daarvan - in opzet - risico's mitigeren.

Ook net als bij de deelnemers van deel 1 van de evaluatie, halen de deelnemers aan dat de neiging bestaat de BIO als 'afvinklijstje' te beschouwen. Aan CISO's wordt bijvoorbeeld gevraagd 'hoeveel procent van de maatregelen geïmplementeerd is', in plaats van welke risico's de organisatie (nog) loopt. De CISO's missen hier dan ook dat de verantwoordelijken van de primaire bedrijfs- of uitvoeringsprocessen zelf actief aan de slag gaan met risicomanagement. Hier wordt overigens tevens opgemerkt door deelnemers dat het volwassenheidsniveau van de organisatie zelf ook weer een samenhang heeft met in hoeverre men in staat is om invulling te geven aan de BIO en dan meer specifiek voor dit onderdeel het benodigd risicomanagement.

Men voelt weinig voor de suggestie van het voorschrijven van de risicomethodiek ofwel een herhaalbare en controleerbare aanpak. De gehanteerde methodiek moet immers aansluiten bij de organisatie. Meer handvatten van hoe je invulling geeft aan risicomanagement zouden wel positief ontvangen worden. De BIO is op dit moment, zo wordt gesteld, te weinig ondersteunend op het gebied van risicomanagement. De risico-benadering komt volgens de gesprekspartners enkel terug in de introductietekst van de BIO. Men zou bijvoorbeeld graag een verwijzing willen vanuit ISO 27001 en ISO 27002 op risicomanagement en inrichting van controls voor ISMS. Dit leidt tot een betere uitwerking van risicomanagement en beter zicht op hoe het principe 'pas-toe-of-leg-uit' toegepast kan worden.

Daarnaast wordt gesteld dat het werken met de BBN's in de huidige opzet de mogelijkheden om risicogebaseerd te werken beperkt. Men mist de flexibiliteit om op basis van een risicoafweging te kiezen of je een maatregel die bij een zeker BBN-niveau past wel of niet toepast. De beperking uit zich er in dat bij externe audits geen 'compliance wordt afgegeven' wanneer men niet letterlijk voldoet aan wat er in de betreffende maatregel staat. Daarmee kunnen we stellen dat het principe 'pas-toe-of-leg-uit in de praktijk niet werkt, want 'leg-uit' heeft de facto niet dezelfde waarde als 'pas-toe'.

De huidige BBN-niveaus worden daarnaast gezien als een belemmering in het nader diversifiëren in een risicogebaseerde aanpak. De BBN-niveaus zijn gericht op impact op een organisatie in plaats van op risico's. Bovendien zijn de BBN-niveaus enkel ingestoken vanuit het aspect vertrouwelijkheid. Risico's bestaan echter uit meerdere componenten, zoals beschikbaarheid en integriteit van informatie.

Analyse en geïdentificeerde verbetermogelijkheden Berenschot

- In lijn met en binnen de kaders uit deel 1 van de evaluatie is de conclusie dat de BIO bijdraagt aan het beleidsdoel. Binnen dit kader werden verschillende verbetermogelijkheden geïdentificeerd.
- Besteed in de eerste hoofdstukken van de BIO nadrukkelijk aandacht aan hóe risicomanagement gehanteerd moet worden bij de implementatie van de BIO om zodoende invulling te geven aan het beleidsdoel. De huidige tekst is daarvoor te beperkt (toepasbaar). Verwijs hiervoor naar handreikingen. De aandacht zou moeten liggen op het procesmatig inrichten van informatiebeveiliging met meer aandacht voor het Information Security Management System (ISMS), met andere woorden: het kwaliteitsmanagementsysteem voor informatiebeveiliging, naar analogie van de ISO 27001. Tevens kan ter versterking en doorwerking van risicomanagement per control geduid worden op welke wijze maatregelen bijdragen aan de reductie van een dreiging en daarmee het mitigeren van een risico.
- Zorg voor minder vrijblijvendheid vanuit de BIO richting het management om zo het beoogde effect van feitelijke informatieveiligheid te bevorderen. Dit kan zowel voor wetgeving als door toezicht.
- CISO's van meer volwassen organisaties op het vlak van informatiebeveiliging stellen dat zij een apart framework (inclusief risk-appetite scaling) voor risicomanagement hebben ontwikkeld, aanvullend op de BIO. In lijn met de wens vanuit bestuurders en hoger management is het aan te raden een maatregel voor het hanteren van een risicomanagement framework op te nemen in de BIO of op andere wijze praktische handvatten of ondersteuning mee te geven aan overheidsorganisaties hoe partijen kunnen komen tot risicogebaseerde maatregelen.
- Een dergelijk framework kan minder volwassen organisaties op het gebied van risicomanagement vooruit helpen in het toepassen zoals de BIO bedoeld is: op basis van adequaat risicomanagement.
- Meer mogelijkheden om te diversifiëren in BBN-niveaus kunnen bijdragen aan een beter risicomanagement. Veel organisaties blijven nu steken op BBN2 wat hen, zo stellen zij, beperkt in het uitvoeren van risicomanagement. Daarnaast zou de scope van de BBN-niveaus verbreed kunnen worden met aspecten zoals beschikbaarheid en integriteit van informatie.
- Om risicomanagement meer kans te geven in de praktische uitwerking van de BIO zou nadrukkelijker naar voren mogen komen dat een goede 'leg-uit' evenveel waard is als een 'pas-toe'. De BIO is nu nog teveel compliancy-gedreven, aldus de deelnemers.

3.1.1.2 Voldoen aan specifieke wet- en regelgeving op het gebied van informatiebeveiliging

De huidige set aan wet- en regelgeving in de bijlage 1 van de BIO is niet volledig. In de vragenlijst en nadere toelichting geven vrijwel alle deelnemers aan dat relevante wet- en regelgeving ontbreekt. Het gaat dan zowel om Nederlandse als Europese wet- en regelgeving.

Het feit dat de deelnemers wet- en regelgeving missen, ontstaat vanuit de behoefte dat de opgenomen set aan wet- en regelgeving in de bijlage inzichtelijk en overzichtelijk maakt aan welke wet- en regelgeving de BIO mede bijdraagt. Dit helpt om de BIO en daarmee informatiebeveiliging hoger op de politieke agenda te krijgen. In die zin draagt de BIO dan ook daadwerkelijk bij aan dit beleidsdoel.

Door een aantal gemeentelijke deelnemers wordt hierop aangevuld dat zij voor wet- en regelgeving nog wel een mogelijkheid tot aanscherping zien. Zo wordt binnen de ENSIA-tool gekoppeld aan normen aangegeven welke wet- en regelgeving hier aan gelinkt is. Ze achten het relevant om ook in de BIO aan te geven aan welke specifieke artikelen van een wet een bepaalde control invulling geeft. Dan wordt het beleidsdoel nog nadrukkelijker ingevuld en kan het direct(er) worden gekoppeld aan de primaire processen.

Tegelijkertijd is ook de constatering dat deelnemers aangeven dat het zo volledig in beeld hebben van wet- en regelgeving in relatie tot de BIO een utopie is. Het is onmogelijk om volledig te zijn, want er zal altijd een delta zitten tussen de laatste versie van de BIO en de geldende wet- en regelgeving die erbij komt in de periode tot een nieuwe versie van de BIO. Een potentieel risico is dat je tracht te vervallen in een onderhoudscyclus voor de BIO die tot onrust leidt door continue veranderingen. Bovendien vergroten te veel onderlinge verbindingen tussen normen enerzijds en wetgeving anderzijds de complexiteit aanzienlijk. Tenslotte bestaat er ook veel sectorale wetgeving die niet relevant is voor alle bestuurslagen of onderdelen binnen het openbaar bestuur. Ook dit is een argument om juist de wet- en regelgeving buiten de BIO te laten. Op basis van die argumenten spreekt dan ook een groot deel van de deelnemers tijdens de sessies zich uit tegen bijlage 1.

Analyse en geïdentificeerde verbetermogelijkheden Berenschot

- Hoewel er behoefte is aan een in- en overzicht om te voldoen aan wet- en regelgeving op het gebied van informatiebeveiliging is de BIO daarvoor niet de meest aangewezen plaats en kan worden geschrapt als bijlage.
- Het is bovendien een utopie om alle vormen van wet- en regelgeving op te nemen in de BIO. De BIO is, als het gaat om praktische toepasbaarheid, niet gebaat bij een stevigere verbinding met wet- en regelgeving.
- Eventueel kan een goed onderhouden ondersteunings-product als 'een continu actueel in- en overzicht' voor control 18.1.1 "Vaststellen van toepasselijke wetgeving en contractuele eisen" bijdragen aan meer inzicht in aan-palende wet- en regelgeving.

3.1.1.3 Veilige ketensamenwerking mogelijk maken met interne en externe partners

De BIO draagt bij aan het vertrouwen tussen overheden om samen te kunnen werken door het stellen van een gelijke norm van alle partijen. Belangrijkste reden hiervoor is het feit dat de BIO zorgt voor een gezamenlijke taal. In aanvulling op dat wat in deel één van de evaluatie naar voren kwam, zien de uitvoerende deelnemers bovendien een groot voordeel van de BIO als het gaat om advisering richting management en operationele uitvoering. De BIO is een breed geaccepteerde en gemeenschappelijke norm. Daar waar samengewerkt wordt met andere partijen, hoeft noch het management noch de operationeel medewerker overtuigd te worden van het feit dat de BIO gehanteerd wordt waardoor het samenwerken vergemakkelijkt.

Waar het echter aan ontbreekt momenteel, is toezicht op de toepassing van de BIO. Ondanks dat de BIO het vertrouwen tussen overheden heeft versterkt, ervaren de geraadpleegde deelnemers toezicht op de toepassing van de BIO als noodzakelijk voor ketensamenwerking tussen overheden. Informatiebeveiliging is namelijk niet 'wel' of 'niet veilig' en bovenal niet permanent. Daarnaast haalt toezicht de vrijblijvendheid van het onderwerp af en stimuleert het de volwassenheid van organisaties. De bij de evaluatie betrokken toezichthouders beamen dat toezicht kan bijdragen, maar geven aan dat daar niet de enige oplossing ligt. Sommige bevindingen blijven, zo wordt gesteld, jarenlang terugkomen en worden niet opgelost. Met toezicht kun je met andere woorden zaken inzichtelijk maken en op de kaart zetten, maar als in de stappen voor het toezicht niet de juiste mensen of capaciteit beschikbaar zijn of adequaat wordt opgepakt, kun je met toezicht niets oplossen.

Wanneer het gaat om samenwerken met partijen buiten te overheid of het gemakkelijker maken van de inkoop van producten en diensten, zijn de deelnemers minder enthousiast. Het grootste deel van de deelnemers vindt dat de BIO hier niet of onvoldoende aan bijdraagt. Wat betreft de samenwerking met partijen buiten de overheid dient allereerst gesteld te worden dat het nooit de bedoeling is geweest om leveranciers te verplichten aan de BIO te voldoen. Leveranciers zouden in lijn met control 15.1.1 moeten voldoen aan eisen die worden gesteld in het informatiebeveiligingsbeleid voor leveranciers. Overheidsorganisaties kunnen in dit kader van leveranciers eisen dat zij de beschikken over een ISO-certificering en bijvoorbeeld aanvullende eisen concretiseren in verwerkersovereenkomsten en contracten. In de praktijk ziet men echter dat overheidspartijen worstelen met het stellen van aanvullende eisen. Het opstellen van aanvullende eisen wordt als complex en tijdrovend ervaren door de geraadpleegde uitvoerende medewerkers. Bij projecten en aanbestedingen dienen BIO en ISO-normen telkens opnieuw naast elkaar gelegd dienen te worden hetgeen aanbestedingen soms onnodig complex en duur maakt. Het gevolg is dat overheidspartijen de gehele BIO opleggen aan ketenpartners en leveranciers, waardoor externe partijen zich weer terugtrekken. Vanuit leverancierssperspectief leidt dit namelijk ertoe dat zij met een meer dan wenselijke diversiteit aan normen dienen te werken. Leveranciers geven hier bovendien aan dat overheidspartijen vaak niet in staat zijn in de, veelal zeer tijdrovende, nota's van inlichtingen aan te geven waarom bijvoorbeeld de ISO 27001 niet volstaat of wat er nu precies extra of meer geëist wordt door de BIO op te leggen.

Analyse en geïdentificeerde verbetermogelijkheden Berenschot

- De BIO draagt bij aan veilige ketensamenwerking en biedt de meeste meerwaarde binnen en tussen overheden.
- Een verbetermogelijkheid ligt in meer toezicht in te richten op de BIO. Zowel voor samenwerkingen binnen als buiten de overheid. Geef ook handvatten voor hoe een organisatie toezicht moet houden op leveranciers.
- In algemene zin wordt echter wel onderschreven dat het hebben van ondersteuningsproducten voor het vaststellen van de juiste inkoopeisen op het gebied van informatiebeveiliging nuttig is. Los van de ICO is hierop de belangrijkste bevinding: standaardiseer de benodigde (sub)set(s) aan maatregelen die opgelegd dienen te wor-den zoveel mogelijk.

3.1.1.4 Fundamenteel beheer bieden

De deelnemers aan de sessies zien vooral de processen incidentmanagement, continuïteitsmanagement en configuratiemanagement als zeer belangrijk voor informatiebeveiliging op het gebied van fundamentele beheerprocessen. Sowieso ondersteunen de deelnemers in algemene zin het feit dat de BIO op het gebied van fundamenteel beheer waarborgen moet meenemen. De discussie gaat er dan wel over in hoeverre is het vooral van belang om te realiseren dat een goede informatiebeveiliging steunt op een goede inrichting van fundamentele beheerprocessen bij de IT-afdeling en in hoeverre de BIO daadwerkelijk iets moet voorschrijven op dit gebied. Vanuit informatiebeveiliging steun je immers op de processen, maar dat maakt het niet opeens integraal onderdeel ervan. Informatiebeveiliging is breder dan IT, ITIL-processen zijn weer breder dan informatiebeveiliging en wordt er vanuit ITIL al het nodige voorgeschreven. Het in control brengen van de ITIL-beheerprocessen is niet nodig vanuit de BIO, aldus de deelnemers. Ze vragen zich vervolgens af wat dan de toegevoegde waarde is van sommige voorschrijvende maatregelen op dit vlak. De mate van detaillering op sommige vlakken legt de maatregelen uit de BIO namelijk dwingend op en laat weinig ruimte voor risicomanagement. Men stelt dat dit leidt tot een 'schijndiscussie' over de uitvoering van maatregelen in plaats van het goed uitwerken van de controls in de organisatie. De stevige focus op de uitvoering van maatregelen leidt af van het uiteindelijke doel 'fundamenteel beheer'.

Analyse en geïdentificeerde verbetermogelijkheden Berenschot

- Het belang van een goede inrichting van fundamentele beheersprocessen voor informatiebeveiliging is groot. Dergelijke processen zijn echter breder dan informatie-beveiliging en informatiebeveiliging omvat meer dan IT. De huidige controls zijn passend en toereikend en dragen voldoende bij aan fundamenteel beheer.
- Er dient wel een expliciete afweging te komen wanneer uitwerking in voorschrijvende maatregelen bijdraagt aan het beoogde (beleids-)doel of effecten op informatie-veiligheid.

3.1.2 Relevantie beleidsdoelen in huidige en toekomstige context

Daar waar de bestuurders in aanvullingen op de huidige beleidsdoelen focussen op het inzichtelijk maken van de volwassenheid van de organisatie, focussen de uitvoerende medewerkers meer op ISMS, OT/SCADA en fysieke beveiliging als bijdrage aan de feitelijke informatieveiligheid. Ten aanzien van het ISMS merkt men op dat het kan bijdragen aan risicomanagement als er meer focus ligt op een kwaliteitssysteem. Nadenken over en toepassen van zaken als risicoacceptatie en restrisico's blijft achter door de wijze waarop de BIO nu wordt ingestoken. Een dergelijke insteek helpt ook om de BIO uit de IT-hoek te trekken en meer van de primaire bedrijfs- of uitvoeringsprocessen te maken, aldus de deelnemers.

Met het oog op het toenemende belang en rol van de overheid in het waarborgen van 'cyberveiligheid in de stad' zien sommige deelnemers noodzaak om deze onderwerpen meer centraal te zetten in de BIO. Dit kan door gerelateerde controls uit hoofdstuk 11 op te nemen in een nieuw hoofdstuk en waar nodig aanvullende controls op te nemen.

Analyse en geïdentificeerde verbetermogelijkheden Berenschot

- In aanvulling op de bestuurders ligt de nadruk in dit deel van de evaluatie op andere aspecten. Hoewel OT/SCADA/procesautomatisering en fysieke beveiliging van enkele deelnemers meer naar voren mogen komen in de BIO, onderschrijven wij dit niet. Wij vinden de huidige werkwijze waarin de BIO de ISO volgt en de breed toepasbare normen stelt voor elke organisatie meer passend. In het kader van een doelgericht toepassingsgebied en hanteerbaar beheer en onderhoud vinden wij het verstandiger OT/SCADA/procesautomatisering vooral in de speciaal daarvoor opgestelde normenkaders te laten. Tevens zijn we van mening dat de BIO fysieke beveiliging vanuit informatiebeveiligingsperspectief voldoende afdekt en ook voor fysieke beveiliging als onderwerp op zichzelf andere normen en expertise nodig zijn. We onderschrijven dat risicomanagement randvoorwaardelijk is voor adequate informatiebeveiliging. Zie ook onder meer paragraaf 2.1.1.1. In die context draagt een ISMS bij aan informatieveiligheid binnen organisatiebreed risicomanagement.
- Zet het ISMS meer centraal in de BIO en benadruk de bredere context. Zorg dat de bestuurders hun verantwoordelijkheid pakken voor het organisatiebrede risicomanagement. Hoewel dit risicomanagement 'buiten de BIO' valt, helpt meer nadruk op het randvoorwaardelijke karakter van risicomanagement, aansluitend op ISMS om zodoende het beleidsdoel te bereiken. Een framework als de Three Lines of Defense sluit hierbij goed aan en geeft organisaties richting in de interne controle en verantwoordelijkheden op orde te brengen. Zie ook de conclusies en aanbeveling in hoofdstuk 4.

3.2 Opzet van het instrument BIO

3.2.1 Samenhang met ISO en andere normen

Net zoals de bestuurders en hoogambtelijke vertegenwoordigers stellen de uitvoerende medewerkers dat de ISO-normen de te volgen normen zijn en dat deze bovendien een prominentere plek moeten krijgen in de BIO. In de update van de ISO 270002 van februari 2022 is een mapping ten opzichte van andere normen, zoals de NIS, gemaakt. Deelnemers zien er voordeel van om deze mapping door te laten werken in de BIO. Als dat goed gebeurt, is de nieuwe BIO vrijwel allesomvattend, aldus de deelnemers. Nu is dat niet het geval. Er mist bijvoorbeeld veel op het gebied van de cloud.

De geraadpleegde deelnemers missen wel de vrijheid die je bij ISO 27001 wel hebt in het kiezen of je wel of niet een maatregel toepast op basis van risicomanagement. Vanuit dat perspectief bezien zou ISO 27001 dus juist een prominentere plek in 'deel 2' van de BIO moeten krijgen, zodat de uitwerking van ISO 27001 in deel 2 van de BIO meer in lijn is met de beschrijving in deel 1 van de BIO. Een groot deel van de deelnemers stelt, net zoals bij de bestuurlijke sessie, voorstander te zijn van het opleggen van de ISO-standaarden via verplichtende zelfregulering aangevuld met BIO-normen in een addendum. Eén van de deelnemers vatte dit kernachtig samen: *'Uitgaande dat ISO dé norm is, zou je de BIO moeten aanvullen met slechts die hele specifieke aspecten voor de overheid'*. Certificering op basis van ISO 27001 is daarbij vervolgens een reële mogelijkheid.

Tevens wordt wederom gesteld dat een stevigere koppeling met risicomanagement een verrijking is voor de BIO. De organisaties verschillen en hebben dan ook een ander risicoprofiel. De te nemen maatregelen zouden genomen moeten worden op basis van dat specifieke risicoprofiel.

Analyse en geïdentificeerde verbetermogelijkheden Berenschot

- In lijn met de bevindingen uit deel één van de evaluatie zijn de ISO 27x de te volgen normen.
- Als verbetering wordt gezien te zorgen voor blijvende aansluiting op de ISO-standaarden en slechts af te wijken waar dat nuttig (voor praktische toepassing) of noodzakelijk (voor specifieke risico's) is.
- Onderzoek of (verplichte) ISO-certificering haalbaar en wenselijk is en stel dan in de BIO alleen nog eisen die aanvullend op een dergelijke ISO-certificering zijn.

3.3 Uitwerking huidig instrument

3.3.1 Basisbeveiligingsniveaus (BBN)

De BIO kent momenteel drie basisbeveiligingsniveaus die een indeling geven - op basis van een beperkte risicoafweging - wat de minimale set aan normen en maatregelen is die verwacht mag worden op basis van het risicoprofiel. Het feit dat de BIO werkt met een classificatie wordt als positief ervaren door veel deelnemers en geeft enige houvast voor de juiste basis. Tegelijkertijd zijn er weinig deelnemers die aangeven goed uit de voeten te kunnen met de huidige set van BBN's. Op basis van de huidige set aan BBN's komen ze eigenlijk voor alles uit op BBN2, zo geeft men aan. BBN3 zegt immers alleen iets over vertrouwelijkheid en betreft vooral beveiliging tegen statelijke actoren. Hierdoor is het ook geen vervolg op niveau 2, maar eigenlijk een niveau ernaast. Bovendien blijft wat je kunt doen bij een hogere beschikbaarheid of integriteit buiten beschouwing in de huidige BIO.

Enkele organisaties, zoals betrokken waterschappen en gemeenten, geven aan te werken met een BBN2+ niveau en dit in de praktijk zeer goed toepasbaar te vinden. Echter, doordat het afwijkt van de BIO in de huidige vorm is het de facto een kunstgreep en beperk je hiermee de voordelen op het gebied van ketensamenwerking door het feit dat er meer ongecontroleerde differentiatie ontstaat.

Enkele anderen zijn stelliger. Zo zegt één deelnemer: *"Ik kan niks met BBN's. We doen standaard BBN2 en op basis van risicoanalyse doen we aanvullende maatregelen. BBN kan eruit"*. Een andere deelnemer zegt: *"BBN stuurt erg op het gebruik van een afvinklijst. Het is juist de bedoeling om een risicobenadering te hebben, daar heb je de BBN's niet voor nodig"*. En daar vult iemand op aan: *"BBN moet je afschaffen. Ze helpen je niet. Het dwingt je in een keurslijf dat niet passend is. Het geeft schijnveiligheid"*. De constatering die volgt in de hierop volgende discussie is dat het idee van ISO is dat organisaties zelf een risk appetite hebben. Met BBN ga je dat onnodig voorschrijven en werkt je het beoogde risicomanagement van de BIO de facto zelfs tegen. Er zou, zo wordt gesteld, dus gewerkt moeten worden aan een gemeenschappelijk kader voor classificatie door organisaties in plaats van het voorschrijven van BBN's.

De vraag of meer of minder niveaus dan de oplossing zouden kunnen brengen, wordt wisselend beantwoord. Degenen die zich hebben uitgesproken voor afschaffing van BBN's zien hierin geen oplossing. Degenen die voorstander zijn van BBN2+ zijn veelal ook voorstander van meer niveaus toevoegen. Tegelijkertijd blijkt ook hier dat de huidige BBN1 afgeschaft kan worden en je dus BBN2, BBN2+ en eventueel de huidige BBN3 als nieuwe niveaus zou kunnen hanteren.

Tot slot wordt door enkele deelnemers opgemerkt dat het concept van BBN's lastig lijkt te zijn voor het management. Zij verwarren het meer dan eens met rubricering van informatie. Daarom adviseren de deelnemers om, wanneer BBN's gehandhaafd blijven in de nieuwe BIO, hier meer duiding en uitleg aan te geven. Bovendien stelt men dat gemeenschappelijke rubriceringsregelingen over alle bestuurslagen heen meerwaarde kunnen hebben bijvoorbeeld in het kader van nationale belangen[9].

Analyse en geïdentificeerde verbetermogelijkheden Berenschot

- Het feit dat de BIO werkt met een classificatie is positief en biedt houvast om de basis op orde te hebben. In de praktijk kunnen organisaties echter beperkt uit de voeten met de huidige set van BBN's. Het expliciet uitwerken van een baseline toets zou hieraan kunnen bijdragen.
- Zorg voor een passende indeling in BBN-niveaus die recht doen aan een goede risicoclassificatie op basis van vertrouwelijkheid, beschikbaarheid en integriteit van informatie. En geef hier meer duiding en uitleg aan.
- Heroverweeg de BBN-structuur. Laat de huidige BBN1 vervallen (of stel deze bij) en hanteer in de BIO slechts een hoogste BBN, de huidige BBN3, wanneer hier ook daadwerkelijk de kaders/invulling voor wordt gegeven.
- Zorg voor een overheidsbrede basis voor het rubriceren van informatie (buiten de BIO). Zorg voor goede duiding, uitleg en communicatie hierover. Heb hierbij oog voor het verschil tussen rubriceren en classificeren, waarbij het belangrijkste aspect bij rubricering is dat gekeken wordt naar mogelijke schade voor de organisatie of samenleving.

9 Zie ook 'Digitaal als Nationaal Belang' (Noordbeek, 2022). Geraadpleegd via https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2022/04/02/onderzoek-afwegingskader-informatieveiligheidseisen-nationaal-belang/digitaal-als-nationaal-belang.pdf

3.3.2 Schadescenario's

In de BIO staan voor de classificering van beschikbaarheid, integriteit en vertrouwelijkheid schadescenario's gedefinieerd. Deze helpen bij het bepalen of een informatiesysteem als laag, midden of hoog op deze drie aspecten ingedeeld dient te worden. Een aantal deelnemers is onbekend met de schadescenario's.

Deelnemers die bekend zijn met de scenario's geven aan dat de schadescenario's helpen bij het hebben van een gedeelde taal binnen en tussen de overheden en daarmee bijdragen aan een uniforme toepassing van de BIO. Zo wordt gesteld dat het in de praktijk alleen niet altijd goed toe te passen is op de eigen organisatie.

In algemene zin wordt het hanteren van de schadescenario's ondersteund door de deelnemers en merken we dat ongeveer de helft van de deelnemers de schadescenario's ook echt hanteren. Sommige deelnemers stellen dat schadescenario's gekoppeld horen te zijn aan de risk appetite van een organisatie. Dit maakt dat de ene overheidsorganisatie een andere indeling gebruikt dan een andere overheidsorganisatie. Hiervan wordt direct door anderen opgemerkt dat dit niet strookt met de uniforme toepassing van de BIO en ook niet passend is in wat de burger mag verwachten van overheidsorganisaties in meer algemene zin.

Analyse en geïdentificeerde verbetermogelijkheden Berenschot

- Schadescenario's ondersteunen organisaties bij een uniforme aanpak van informatiebeveiliging.
- Actualiseer de schadescenario's en werk deze meer uit in lijn met alle bestuurslagen, zodat ze herkenbaar en toepasbaar worden voor iedereen. Zorg voor goede duiding, uitleg en communicatie hierover.

3.4 Toepassing en onderhoud instrument

3.4.1 Reikwijdte

Over de huidige reikwijdte van de BIO, de vier bestuurslagen, zijn de deelnemers eensgezind; deze is passend en hier hoeft geen verandering in aangebracht te worden. Het is juist fijn om overheidsbreed eenzelfde baseline te hanteren en toepassing buiten de overheid is niet logisch.

Wel wordt opgemerkt vanuit een deelnemer van een ZBO dat er onduidelijkheid is over of ZBO's nu wel of niet de BIO dienen te hanteren. Hierop geven enkele andere deelnemers aan dat in artikel 41 van de Kaderwet ZBO's expliciet is opgenomen dat de voor de rijksdienst geldende voorschriften op het gebied van gegevensbeveiliging ook van toepassing zijn op ZBO's.

Analyse en geïdentificeerde verbetermogelijkheden Berenschot

- De huidige reikwijdte van de BIO op de vier overheidslagen is voldoende passend.
- Indien onduidelijkheid bestaat bij ZBO's over of de BIO van toepassing is, kan het nuttig zijn hier helderheid over te verschaffen. Mogelijk speelt dit ook bij andere (type) organisaties. Dit verbeterpunt staat echter los van het instrument BIO.

3.4.2 Beloning

Ook ten aanzien van de vraag of organisaties beloond moeten worden voor het bereiken van een bepaalde volwassenheid of omdat ze een langere periode voldoen aan de BIO, bestaat veel eensgezindheid. Informatiebeveiliging en voldoen aan de BIO is basishygiëne van een organisatie en dus niet beloningswaardig, maar simpelweg een must. Overheidsorganisaties zijn dit verplicht aan burgers en ondernemers. Meer positief verwoord zegt een deelnemer dat het groeien in volwassenheid en bijvoorbeeld het behalen van een ISO 27001-certificering een beloning op zichzelf zijn.

Analyse en geïdentificeerde verbetermogelijkheden Berenschot

- Het op orde hebben van informatiebeveiliging is een basishygiëne, waarbij het groeien in volwassenheid voldoende is. Hoewel beloning is niet direct passend is, is te overwegen of minder intensief toezicht passend is.

3.4.3 Ondersteuning

In meer algemene zin wordt de gedachte van een prepared-by-client lijst[10] of een toetsingskader ondersteund. Wel wordt wisselend gedacht over in hoeverre ze dit echt zouden hanteren. Meer volwassen organisaties ondersteunen sneller een toetsingskader, omdat ze het zien als een middel om verder te groeien. Met andere woorden, men kijkt dan naar een toetsingskader meer als een volwassenheidsmodel.

De gedachte van meer toetsing en meer toezicht wordt ondersteund door de meeste deelnemers. Dan helpt het hebben van meer handvatten over wat er nodig is om te voldoen. Wat men vervolgens nog wel mist, is ook sturing op opvolging van verbeterpunten.

Analyse en geïdentificeerde verbetermogelijkheden Berenschot

- In de context van (praktische) ondersteuning wordt vooral meer toetsing en meer toezicht breed ondersteund. Het gebruik van handvatten als een prepared-by-client lijst of toetsingskader kan helpen bij het behalen van doelen en beoogde effecten.
- Op basis van de signalen van de deelnemers denken we dat een handreiking in de vorm van een ondersteunend volwassenheidsmodel, waarbij toetsing op volwassenheidsniveaus inzichtelijk wordt gemaakt, bijdraagt in het ondersteunen van groei van overheidsorganisaties op het gebied van volwassenheid. Een dergelijk volwassenheidsmodel met toetsingskader kan naast de BIO gehanteerd worden.

3.4.4 Periodieke actualisatie en onderhoudsregime

Er is brede consensus dat de huidige beheercyclus van de BIO niet volstaat. De maatregelen zijn in enkele gevallen verouderd (denk hierbij aan het eerder genoemde wachtwoordbeleid) en de aansluiting op vernieuwingen van de ISO volgt laat.

Men merkt op dat niemand zit te wachten op een continu wijzigend normenkader, maar dat actualiteit tegelijkertijd wel geborgd moet worden. Daarin moet een juiste balans gevonden worden. Bij voorkeur van de deelnemers gebeurt dit zoveel mogelijk door het stellen van maatregelen die niet aan veel onderhoud onderhevig zijn. Sluit dus aan op een expertorganisatie die hier adviezen over geeft in de maatregel, of stel geen maatregel.

Niet alleen voor overheidsorganisaties zelf is dit belangrijk, maar ook voor leveranciers die gehouden worden aan BIO-maatregelen. Check in elk geval jaarlijks of de maatregelen een update nodig hebben, aldus de deelnemers. Vanuit het perspectief en achterliggende doel van feitelijke informatieveiligheid leidt te laat wijzigen per definitie tot onnodige zorgen.

Qua normen wordt aangegeven graag up to date te blijven met het onderliggend normenkader van de ISO. Ook in deze context wordt daarom benadrukt dat het verplicht stellen van de ISO gemakkelijker is qua onderhoud, dan alles over te nemen naar de BIO. Met een dergelijke opzet is er slechts een beperkte set aan specifieke overheidsmaatregelen te onderhouden. Tot slot merken deelnemers op dat uitlegbaarheid van wijzigingen van groot belang is - onder meer richting bestuurders en management, waarbij duidelijk gemaakt wordt wat er wijzigt en waarom.

Analyse en geïdentificeerde verbetermogelijkheden Berenschot

- Een vaste periodieke actualisatie en helder onderhoudsregime is belangrijk voor de voorspelbaarheid en draagvlak van het instrument.
- Zorg ervoor dat in die lijn de normen in de BIO met de wijzigingen van de ISO veranderen.
- Zorg voor een jaarlijkse (check op) bijstelling van onderliggende overheidsmaatregelen en maak duidelijk wanneer deze maatregel actief wordt. Zorg ervoor dat organisaties voldoende tijd (bijvoorbeeld één jaar) hebben om de maatregelen te implementeren.
- Zorg ervoor dat overheidsmaatregelen zo geformuleerd worden dat bijstelling minimaal nodig zal blijken. Expliciteer daar waar mogelijk bij onderhoudsgevoelige normen dat herziening vaker mogelijk is. Zorg voor goede duiding, uitleg en communicatie hierover.

10 Een prepared-by-client lijst is een lijst met documenten voor een auditor die aangeleverd wordt door een organisatie bij een audit.

3.5 Vooruitblik

In het tweede deel van de evaluatie heeft de BIO van de deelnemers een cijfer gekregen en is telkens vooruitgekeken. De BIO scoort gemiddeld een voldoende bij alle deelnemers. Dit betekent echter niet dat iedereen unaniem en volledig positief is over de BIO. Het achterliggende nut en de noodzaak van de BIO wordt daarentegen breed ondersteund. In dit laatste deel van de evaluatie zijn verbetervoorstellen geformuleerd die maken dat de BIO in lijn met de bestuurlijke sessies en bevindingen in de aanvullende sessies beter bijdraagt aan de beoogde doelen en beter in de praktijk toepasbaar wordt voor de organisaties. Tegelijkertijd zullen deze wijzigingen de meest uitgesproken voor- of tegenstanders onvoldoende tevreden stellen. Belangrijke verbeteringen als meer de focus te leggen op risicomanagement vanuit de gedachte bij te dragen aan feitelijke informatieveiligheid en het 'wegnemen van de ervaren vrijblijvendheid' worden echter breed onderschreven.

Eén van de deelnemers vatte de vrij algemeen gedeelde blik op de BIO mooi samen:

"De BIO is een van de grootste goeden die we als overheid moeten koesteren. Het is een leidraad voor de gesprekken in de samenwerkingsverbanden en cruciaal voor informatiebeveiliging, mits goed toegepast. Dat zit in voorlichting en handelingsperspectief voor mensen die er mee om moeten gaan. Zoals met iedere norm heb je altijd discussie over iets meer naar links of rechts en wat er precies bedoeld wordt. Daarnaast is er vaak discussie over het juiste niveau - te abstract of te gedetailleerd. Of met de vraag waarom we de ISO niet gebruiken. De BIO zit echter op het juiste niveau tussen abstractie en detaillering in. Security is geen broodje speciaal meer en draagt daarom bij aan het waarborgen van fundamenteel beheer."

HOOFDSTUK 4

Conclusies en aanbevelingen

In het volgende hoofdstuk geven we onze algemene conclusies en aanbevelingen voor verbeteringen. De nadruk ligt hierbij op de ontwerpprincipes en omvatten aanbevelingen voor de BIO en in een enkel geval voor de bredere context. Daar waar relevant wordt dit onderscheid benadrukt. In hoofdstuk 2 hebben we reeds op specifieke onderdelen onze analyse en verbetermogelijkheden gegeven. In hoofdstuk 3 zijn daarnaast per onderdeel meer concrete verbetervoorstellen opgenomen.

1. De BIO is een breed geaccepteerd en gemeenschappelijk normenkader binnen de overheid en heeft in opzet alom een erkende bestaansreden. De BIO legt een overheidsbrede basis voor optimalisering van informatiebeveiliging binnen de gehele overheid en helpt individuele organisaties, mits goed toegepast, passende maatregelen te nemen. Ook draagt de BIO bij aan een gemeenschappelijke taal, waarmee veilige samenwerking in ketens binnen de overheid wordt versterkt. Het afdwingen van een norm of minimumniveau over de gehele overheid (BIO) binnen een internationale standaard (ISO) draagt bij aan feitelijke informatieveiligheid, werkt uniformerend en zorgt voor impliciet vertrouwen binnen en tussen overheden. Tevens heeft de BIO de potentie bij te dragen aan informatiebeveiliging in de samenwerking met ketenpartners en leveranciers. De BIO vergemakkelijkt de samenwerking met die externe ketenpartners echter niet altijd. De huidige beleidsdoelen worden in belangrijke mate bereikt.
   Aanbeveling: Blijf als overheid een norm of minimum-beveiligingsniveau hanteren om informatieveiligheid te waarborgen bij de vormgeving van de digitale transitie in Nederland. Informatieveiligheid is een onderdeel van dat digitale fundament. Een belangrijk instrument hierbij is communicatie. In de praktische communicatie en eventuele nadere ondersteuning aan medeoverheden over de BIO 2.0 dient helder te zijn dat een BIO de facto en de jure de internationale standaard ISO is, aangevuld met een minimumbeveiligingsniveau bestaande uit specifieke overheidsmaatregelen.

2. Hoewel de BIO gebaseerd is op en gestructureerd is volgens de NEN-ISO/IEC 27001:2017, bijlage A en NEN-ISO/IEC 27002:2017, aangevuld met specifieke overheidsmaatregelen, is de conclusie dat de BIO niet als zodanig wordt ervaren, maar als eigen, op zichzelf staand normenkader. De expliciete zinsnede in de BIO dat *'dit betekent dat de overheid deze normen [van de ISO] toepast tenzij er expliciet geformuleerde redenen zijn om dat niet te doen'* en dat *'die documenten [...] dus de details [geven] voor de toepassing, die niet in de BIO zijn beschreven en die nodig blijven voor een goede implementatie van de BIO'*[11] wordt deze basis en structurering gezien het betoog om 'de ISO' te hanteren niet als zodanig ervaren door medeoverheden.
   Aanbeveling: Versterk in de tekst van de BIO 2.0 dat de ISO-standaard als basis wordt gehanteerd (vanuit de lijst met 'verplichte standaarden' van het Forum Standaardisatie[12]) en dat de aanvullingen vanuit de BIO 'slechts' de norm en de specifieke overheidsmaatregelen zijn. De doelmatigheid van het instrument en het doelbereik wordt hiermee versterkt. Ter illustratie: de overheid hanteert dan dus niet 'de BIO op basis van de ISO', maar 'de ISO aangevuld met een minimumbeveiligingsniveau bestaande uit specifieke overheidsmaatregelen'. Een dergelijke kanteling in met name de opzet, vorm en beeldvorming kan ook de kennis uit de markt vergroten en een ISO 27001-certificering vergemakkelijken, waardoor de samenwerking met ketenpartners en leveranciers eenvoudiger wordt. Bijkomend effect is dat met een dergelijke opzet de samenhang met andere ISO-standaarden gemakkelijker gelegd kan worden, de samenhang versterkt in de bredere context van GRC en dat strategisch risicomanagement meer herkenbaar wordt.

3. De BIO expliciteert de essentiële randvoorwaarde van risicomanagement *'om tot de juiste beveiliging van informatie en informatiesystemen te komen binnen de context van de bedrijfsdoelstellingen'*[13]. *Daarbij wordt gesteld dat 'de overheidslagen [...] als basis voor deze procesmatige inrichting van risicomanagement en het inrichten van de PDCA-cyclus voor de NEN/ISO 27001:2017of NEN/ISO 31000-aanpak [kiezen]'.* De BIO omvat vanuit dat perspectief dan ook beheersdoelstellingen waarvoor passende maatregelen moeten worden gekozen gecombineerd met een verplichte set aan basis- of overheidsmaatregelen. De BIO is met andere woorden slechts toepasbaar in een enigszins 'in risicomanagement volwassen' organisatie. Risicomanagement als basis van de BIO wordt echter niet als zodanig ervaren. Dit komt (i) door de wijze waarop de BIO op dit moment in de praktijk wordt gehanteerd en (ii) vanuit de keuze in de BIO om risicomanagement hanteerbaar en efficiënt te houden door het gestelde minimumniveau en drie basisbeveiligingsniveaus (BBN's). De uitwerking van risicomanagement langs de lijnen van BBN's kan helpen bij het bereiken van de beleidsdoelen, maar heeft op dit moment tot effect dat het voor overheidsorganisaties beperkend en in praktijk lastig toepasbaar is. Zo wordt BBN1 niet gebruikt. En hoewel de in de praktijk voor gemeenten ontwikkelde differentiatie BBN2+ een handreiking is om de juiste maatregelen te nemen in het geval van 'vertrouwelijkheid hoog', staat dit in contrast met de beoogde opzet van de BIO, zoals uniformiteit. Meer differentiatie naar zowel beschikbaarheid, integriteit en vertrouwelijkheid is gewenst.

11 Zie BIO verzie 104zv def, pagina 2
12 Zie https://www.forumstandaardisatie.nl/open-standaarden/verplicht
13 Zie BIO verzie 104zv def, pagina 9

Aanbeveling: Zet 'ingebed organisatiebreed risicomanagement' meer centraal in de BIO als cruciale randvoorwaarde binnen een organisatie in zowel de context van een 'enterprise risicomanagement framework' als tussen organisaties ('vendor security management'[14]). Biedt hiervoor via vertegenwoordigende organisaties aan medeoverheden praktische handreikingen en best practices aan op welke wijze de implementatie van risicomanagement dient te worden toegepast.[15] Organisatiebreed strategisch risicomanagement zou als een rule-based voorschrift kunnen worden opgenomen in de BIO, waarbij bijvoorbeeld de doelstelling van hoofdstuk 5 wordt uitgebreid met de vereisten om 'de informatiebeveiligingsfunctie in overeenstemming te laten zijn met organisatiebreed risicomanagement en inrichtingsprincipes' en daarbij verwijzen naar een best practice. Hierbij kan dan tevens een link worden gelegd met control 18.2.2.1 in hoofdstuk 18 'Naleving', waarbij de informatiebeveiligingsfunctie nadrukkelijker wordt ingebed in de governance van de organisaties.

Aanbeveling: Informatiebeveiliging is onderdeel van breder (strategisch) risicomanagement[16], waarbij in lijn met de Three Ljnes of Defense[17] duidelijk onderscheid wordt gemaakt in taken, bevoegdheden en verantwoordelijkheden. De waarde van het Three Lines of Defense model wordt binnen en buiten de overheid breed gedeeld. Het nadrukkelijk uitdragen en toepassen van dit model - gericht op expliciete implementatie bij onder meer medeoverheden als kwalitatieve versterking van de interne governance zal, hoewel buiten scope van de BIO, als basis bijdragen om de beoogde (beleids)doelen te behalen. Vertegenwoordigende organisaties, zoals de VNG kunnen, indien zij een dergelijke inrichting willen uitdragen, dergelijke organisatieprincipes zichzelf opleggen ('verplichtende zelfregulering') vergelijkbaar met de huidige BIO.

Aanbeveling: Organisaties dienen zelf hun risicoanalyses uit te voeren. Overweeg overheidsbrede standaardisatie in rubricering en hanteer hierbij kwaliteitseisen of schadescenario's (bijlage 2 uit de BIO). Differentieer in de wijze waarop organisaties dit moeten doen, maar hanteer een minimumniveau waarop organisaties zelfstandig een adequate risicoanalyse dienen te doen (of te wel 'wat er minimaal moet gebeuren' van strategische risk appetite tot operationele toepassing). Dit is afhankelijk van de kennis en kunde van de (medewerkers van de) organisaties. Ter illustratie: 'Ongeacht de risicomethodiek dient data met kenmerken x, y en z te leiden tot classificatie 1, 2 of 3 op beschikbaarheid, integriteit of vertrouwelijkheid'. Toezicht op de juiste toepassing is daarbij wenselijk.

4. De BIO verwijst nadrukkelijk naar het ISMS en bijhorende eisen[18] uit de NEN-ISO/IEC 27001:2017. Een ISMS is onmisbaar voor risicomanagement en dus adequate informatiebeveiliging. Dit aspect is onderbelicht en wordt in lijn met voorgaande door de wijze waarop de BIO wordt gehanteerd niet als onderdeel van adequate informatiebeveiliging (in de context van de te nemen maatregelen uit de BIO) gezien.
   Aanbeveling: Draag zorg dat organisaties een ISMS hebben, waardoor organisaties deels invulling geven aan de aanbevelingen onder 3.
   De BIO biedt meerwaarde voor zowel compliance als feitelijke informatieveiligheid. Het voldoen aan BIO betekent echter niet dat een organisatie daadwerkelijk veilig is, niet kwetsbaar is of incidenten kan ervaren en/of volledige compliant is aan alle wet- en regelgeving op het gebied van informatiebeveiliging. De initiële hoofddoelen van de BIO zijn voldoende passend, maar zouden aangevuld kunnen worden met meer focus op 'feitelijk beveiligen', ofwel de basis op orde, in plaats van 'administratief beveiligen'[19]. In de huidige opzet wordt door overheidsorganisaties echter veelal gefocust op de te nemen maatregelen en 'het vinkje behalen'.

14 Met 'vendor security management' wordt het deel van leveranciersmanagement verstaan dat zich richt op het identificeren, analyseren, monitoren en mitigeren van risico's van leveranciers die mogelijk van invloed zijn op de informatiebeveiliging of compliance van een organisatie
15 Zie tevens het concluderende hoofdstuk in het adviesrapport 'Sturing op informatieveiligheid' voor aanbevelingen in de bredere context van de BIO (Berenschot, 2022)
16 Zie bevindingen uit het adviesrapport 'Sturing op informatieveiligheid' (Berenschot, 2022)
17 Het Three Lines of Defense model wordt wereldwijd als de standaard gezien voor risicomanagement. Met dit model wordt onderscheid gemaakt in de business (eerste lijn) die eindverantwoordelijk is voor de eigen processen en de risico's kent en beheerst. Daarnaast is er een functie die de eerste lijn ondersteunt, adviseert en coördineert (tweede lijn). Deze functie is verantwoordelijk voor het proces van risicomanagement en beheersing ter ondersteuning van de business. Tot slot is er een interne audit (derde lijn) die nagaat of de eerste en tweede lijn goed functioneert en hierover objectief en onafhankelijk een oordeel velt. Het model is inmiddels aangepast naar de 'Three Lines Model' (zie https://www.iia.nl/actualiteit/nieuws/belangrijke-update-three-lines-model) In deze rapportage hanteren we 'Three Lines of Defense' vanuit verwijzingen gedurende de evaluatie en de bredere herkenbaarheid.
18 Zie BIO verzie 104zv def, pagina 2
19 Kamerstuk 26643, nr. 917

Aanbeveling: Voeg *'sturen op volwassenheid van organisaties'* toe als beleidsdoel. Er moet meer nadruk komen op die feitelijke informatieveiligheid in de bredere context van cybersecurity. Toetsing en testen van organisaties in de vorm van onder meer penetratietesten in de bredere context van toezicht en handhaving op basis van een wettelijk kader biedt hiervoor aangrijpingspunten, vergelijkbaar met de rol van De Nederlandse Bank en *Threat Intelligence Based Ethical Red-teaming* (TIBER)[20].
Hierbij is het wel van belang dat er een enigszins volwassen informatiebeveiligingsorganisatie staat.
De huidige 'verplichtende zelfregulering' van de BIO zijn niet-vrijblijvende, bindende afspraken, waaraan overheidsorganisaties zichzelf committeren. Een dergelijke opzet wordt inmiddels als te vrijblijvend ervaren. Deze vrijblijvendheid ondermijnt de initiële beleidsdoelen en is niet langer passend in het huidige dreigingslandschap en verwachtingen en vereisten vanuit de samenleving. Bovendien ontstaat hierdoor de situatie dat vanuit verschillende stelsels verschillende eisen worden gesteld die zorgt voor onnodige onduidelijkheid in de uitvoering, beperkend is voor de doelmatigheid, niet bijdraagt aan de beoogde beleidsdoelen en effecten en tot slot een dubbele auditlast met zich meebrengt.

Aanbeveling: Werk toe naar een situatie met minder vrijblijvendheid. Dit punt is onderkend[21], waarbij aan de Tweede Kamer reeds is gemeld dat het streven is om informatiebeveiliging bij de overheid een wettelijke basis te geven in de Wet Digitale Overheid. Wij onderschrijven dit en benadrukken dat met het wettelijk verplichten van de BIO de vrijblijvendheid ingeperkt wordt en op die wijze eenduidig regels voor informatiebeveiliging bij de overheid worden gesteld.

5. Naast wettelijke verankering zal in lijn met andere stelsels[22], moeten worden toegezien op informatiebeveiliging bij overheden en een passend stelsel van toezicht en handhaving moeten wordt ingericht. Dergelijk toezicht en handhaving in samenhang met verantwoording vindt dan plaats per overheidslaag in de reguliere planning-and-control. Bij dit alles geldt, zo wordt in de Kamerbrief[23] gesteld *'dat vakministers, gemeenten, provincies en waterschappen zelf verantwoordelijk zijn en blijven voor hun informatieveiligheid'*. ENSIA biedt mogelijkheden voor stevigere verantwoording.
Aanbeveling: Richt duidelijker toezicht in op de BIO. In de kamerbrief is reeds onderkend dat toezien op informatiebeveiliging bij de overheid, niet alleen op de naleving van algemene regels, zoals de BIO, maar ook op specifieke regels die vanuit vakdepartementen aanvullend op de BIO worden gesteld, noodzakelijk is. Belangrijk aspect hierbij is de verantwoording van iedere individuele organisatie en de rol van het eigen controlerende orgaan, zoals een rekenkamer. Een juiste en uniforme normering en toetsing op basis van een te ontwikkelen toetsingskader draagt aan de feitelijke informatieveiligheid van de overheid en efficiënte vergelijkbare interbestuurlijke verantwoording. Ook op dit aspect is het belang van de juiste communicatie cruciaal.

Tot slot

Hoewel bovenstaande conclusies en aanbevelingen, inclusief de verbetervoorstellen in hoofdstuk 3, zullen bijdragen aan het versterken van de informatiebeveiliging bij de overheid, is het belangrijk om in ogenschouw te nemen dat dergelijke wijzigingen slechts tot verbeteringen zullen leiden, indien er ook aandacht is voor een aantal randvoorwaardelijke zaken, zoals ingebed risicomanagement.

Tot slot is het ook van belang dat individuele organisaties zich bewust zijn van het belang van informatiebeveiliging en dit ook onderdeel is van een veiligheid- of risicocultuur. Een dergelijke cultuur moet door de (ambtelijke) top worden uitgedragen en daarmee doorwerken naar de rest van de organisatie. Een functionele en gezonde risicocultuur is daarbij zowel een randvoorwaarde (voor een volwassen en weerbare organisatie op informatiebeveiliging), een gevolg (van het zetten van stappen in volwassenheid en weerbaarheid), als een doel (om na te streven). Immers een functionele risicocultuur draagt op zijn beurt weer bij aan een weerbare organisatie.

20 Zie https://www.dnb.nl/voor-de-sector/betalingsverkeer/tiber-nl/
21 Kamerstuk 26643, nr. 917
22 Bijvoorbeeld in de financiële sector
23 Kamerstuk 26643, nr. 917

BIJLAGE 1

Vragenlijst

Bij de opdrachtverstrekking heeft de opdrachtgever een set evaluatievragen gedeeld. Deze lijst is integraal opgenomen. De vragen hebben als basis gediend voor onderliggende evaluatie.

Deel 1 Onderwerpen op bestuurlijk niveau

1. Heeft de BIO bijgedragen aan de 4 beleidsdoelen op gebied van de informatieveiligheid van de overheid?
    1. Het management in staat stellen om op basis van expliciete risicoafweging informatiebeveiligingsmaatregelen te kiezen, implementeren en uitdragen.
    2. Voldoen aan specifieke wet- en regelgeving op het gebied van informatiebeveiliging.
    3. Veilige ketensamenwerking mogelijk maken met interne en externe partners.>
    4. Fundamenteel beheer bieden.
2. Zijn de beleidsdoelen van de BIO nog relevant?
    1. Zijn er minder of aanvullende doelen nodig, bijv. op het gebied van volwassenheid, Europese regelgeving of cybersecurity?
    2. Moeten de beleidsdoelen worden aangepast?
3. Is de mix van rule-based & principle-based aanpak die de BIO voorschrijft optimaal?
4. Is de verplichtende zelfregulering voldoende basis om de informatieveiligheid binnen uw organisaties langs de lijn van de BIO te organiseren?
    1. Levert dit voldoende zekerheid op over de feitelijke informatieveiligheid van uw partners?
5. De BIO is gebaseerd op de internationaal geaccepteerde standaarden ISO27001 en -2. In hoeverre heeft het toepassen van deze standaarden het afstemmen van de informatiebeveiligingsbehoefte met externe leveranciers beïnvloed?
6. In hoeverre draagt de BIO bij een aan invullen van het toezicht (interne transparantie) op de informatieveiligheid middels ‘single audit’ voor stelselhouders?
    1. Kan de BIO als uniform stuurmiddel worden gezien om de informatieveiligheid binnen overheidsorganisaties op het gewenste niveau te houden.

Deel 2 BIO als instrument

Binnen de context van de beantwoorde bestuurlijke vragen moet de evaluatie duidelijk maken of en zo ja welke verbeteringen nodig zijn om met de BIO in lijn te houden met de beoogde doelen op informatieveiligheid binnen de overheid. De BIO is een tactisch normenkader met deels operationele maatregelen. De verbetervraag zal op tactisch/operationeel niveau beantwoord moeten worden.

7. Heeft u de BIO geïmplementeerd?
    1. Welke plek heeft risicomanagement binnen uw organisatie?
    2. Heeft u de overheidsmaatregelen geïmplementeerd?
8. Ervaringen t.a.v. de ontwerpprincipes van de BIO?
    1. Beleidsdoel risicomanagement
        1. Is het uitgangspunt van risicomanagement voldoende duidelijk?
        2. Het topmanagement stuurt op risico’s?
        3. Is risicomanagement bepalend bij de beoordeling van controls uit de BIO?
        4. Biedt de BIO met z’n overheidsmaatregelen voldoende ruimte voor risicomanagement?
        5. Moet de BIO de te hanteren risicomethodiek voorschrijven en zo ja, welke methode is dat?
    2. De overige drie beleidsdoelen:
        1. Voldoen aan specifieke wet- en regelgeving
            1. Is de set wet- en regelgeving uit bijlage 1 van de BIO nog de juiste?
            2. Moet Europese wet- en regelgeving toegevoegd worden?
        2. Ketensamenwerking mogelijk maken?
            1. In welke mate draagt de BIO bij aan het elkaar vertrouwen om binnen de overheid samen te kunnen werken op basis van een gemeenschappelijke norm?
            2. Welke rol speelt het toezicht daarbij?
            3. Wat is er behalve de BIO als tactische normenkader en het toezicht nog meer nodig om in vertrouwen te kunnen samenwerken?

    4. Maakt de BIO het makkelijker veilig samen te werken met partijen buiten de overheid en bij inkoop van producten en diensten?
  3. Fundamenteel beheer waarborgen
    1. Welke ITIL-processen vormen het fundament?
    2. Dekken de overheidsmaatregelen dit fundament voldoende af?
  4. Zijn de 3 pijlers voldoende of moeten er andere pijlers toegevoegd worden?
3. ISO 27001 en ISO 27002 als kapstok:
  1. Zijn de ISO 27001 en ISO 27002 nog de te volgen normen?
    1. Zo nee: welke andere normen zouden daarvoor in de plaats kunnen komen?
    2. Zo nee: de BIO volgt de ISO27001 en 27002 o.a. omdat deze op de pas-toe-of-leg-uit lijst staan van het Forum. Als er geen directe relatie meer is naar deze normen, hoe denkt u dan te kunnen voldoen aan de eisen die het Forum stelt?
    3. Zo ja: Zou de ISO 27001 aanpak een prominentere plek moeten krijgen in deel 1 van de BIO?
  2. Zijn er andere (operationele/tactische) normen die de BIO kunnen verrijken?
    1. Welke normen? (operationele-/tactische normen, aanbrengen focusgebieden)
    2. En voor welke doelen en situaties?
4. Beveiligingsniveaus:
  1. Is er meer of minder differentiatie nodig binnen de BIO?
  2. Dekken de geselecteerde controls het basis-beveiligingsniveau van BBN1 en 2 voldoende af?
5. Schadescenario's passend?
  1. Zijn de schadescenario's eenduidig genoeg?
  2. Zijn de schadescenario's passend bij het respectievelijke BBN?
6. De BIO is van toepassing op de 4 overheidslagen. Is de reikwijdte van de BIO voldoende (breder/smaller)?
7. Zou u beloond moeten worden voor het bereiken van een bepaalde volwassenheid of omdat u een langere periode voldoet aan de BIO? Bij welk volwassenheidsniveau en welke periode is een beloning op z'n plaats? Wat zou die beloning kunnen zijn?
8. Heeft u behoefte aan een prepared by client-lijst en eventueel een toetsingskader/toetsingscriteria?
9. Is voldoende helder hoe de beleidsdoelen/pijlers moeten worden ingepast in bestaande processen?
9. Nieuwe dreigingen op cybergebied volgen elkaar snel op. Actuele beveiligingsmaatregelen kunnen dit mitigeren. Welk onderhoudsregiem past bij de BIO?
10. Wat vindt u van de digitale toegankelijkheid van de BIO?
11. Hoe waardeert u de BIO?
  1. Welk cijfer geeft u de BIO (schaal 1-10) en waarom?
  2. Heeft u problemen ervaren bij het implementeren van de BIO. Zo ja:
    1. Welke oplossing ziet u voor deze problemen;
    2. Waarom denkt u dat daarmee het probleem is opgelost?
  3. Welke voordeel heeft u ervaren van de implementatie van de BIO?

BIJLAGE 2

Onderzoeks-opzet

Inleiding

Om tot een volledige en adequate beantwoording van de vragen uit de twee delen van de evaluatie en onderliggende onderwerpen te komen, is onderstaande onderzoeksopzet gehanteerd.

Aanpak van het onderzoek

Het onderzoek is gestart in april en afgerond in oktober 2022 en werd begeleid door een medewerker van DGDOO/BZK in samenwerking met vertegenwoordigers van de medeoverheden uit het kern-IBO[24] en de interbestuurlijke werkgroep-BIO.

Fases

Het gehele onderzoek bestond uit twee onderdelen met een viertal fases en bijhorende inspanningen en resultaten, zoals weergegeven in onderstaand overzicht:

Fase	Inspanningen	Resultaat
Voorbereiding	Kick-off	Afgestemd plan van aanpak met de opdrachtgever en vertegenwoordigers van de medeoverheden uit het kern-IBO
		Afgestemde lijst met deelnemende (vertegenwoordigers van de) organisaties
	Voorbereiding evaluatie	Documentstudie
		Uitgewerkte en voorbereide evaluatiesessies
Uitvoering deel 1	Uitvoering bestuurlijke c.q. hoogambtelijke sessies	Interactieve sessies
	Verdiepend onderzoek	Aanvullende documentatie verzameld en meegenomen in de documentstudie
	Uitwerken (tussen)resultaten	Concept bevindingen
		Gevalideerde go/no go vanuit de opdrachtgever en vertegenwoordigers van de medeoverheden uit het kern-IBO
Uitvoering deel 2	Aanvullende voorbereiding: vragenlijst uitwerken	Aanvullende input verzameld voor de inhoudelijke sessies
	Uitvoering inhoudelijke sessies	Interactieve sessies
	Verdiepend onderzoek	Aanvullende documentatie verzameld en meegenomen in de documentstudie
Afronding	Afstemmen conceptrapportage	Conceptrapportage afgestemd met opdrachtgever en vertegenwoordigers van de medeoverheden uit het kern-IBO en verbetervoorstellen verwerkt
	Definitieve rapportage	Definitieve rapportage opgeleverd
	Afronding rapportage	Presentatie resultaten

24 Zie https://www.bio-overheid.nl/category/bio-wijzigingen/

Gedurende de uitvoering van de evaluatie is als referentie gebruik gemaakt van bevindingen gericht op of in de bredere context van de BIO uit het onderzoek 'Sturing op informatieveiligheid' in opdracht van BZK uitgevoerd door Berenschot (2022). In dit onderzoek is gekeken naar de wijze waarop bij grote (semi) commerciële organisaties in verschillende sectoren sturing wordt gegeven aan informatieveiligheid en welke lessen BZK hieruit kan trekken.

Een evaluatie in twee delen

Opzet deel 1

Het eerste deel van de evaluatie beantwoordde de vraag over de bestaansreden van de BIO in een tweetal gecombineerde interactieve werksessies met de bestuurders c.q. hoogambtelijke vertegenwoordigers. De werksessies bestonden telkens uit twee onderdelen, waarbij in het eerste gedeelte een eerste inventarisatie werd opgehaald en in het tweede deel de opgehaalde beelden nader werden uitgediept. Deze digitale groepssessies vonden plaats met een representatieve vertegenwoordiging vanuit de vier overheidslagen.

In de opzet van de sessies is gekozen voor een werkvorm die aansluit bij het beoogde doel om gezamenlijk te reflecteren. Hierbij zijn mogelijke verbeterpunten ten aanzien van de ontwerpprincipes in kaart gebracht en is gereflecteerd en vooruit gekeken. De vooraf gedeelde onderzoeksvragen werden als stellingen geponeerd. De werkvorm faciliteerde hierbij een transparante en open discussie met de verschillende vertegenwoordigers, bracht de partijen bij elkaar en bood eenieder de gelegenheid om zijn of haar input te leveren. In de discussie die daarop volgde, verdiepten we de evaluatievragen met de deelnemers en werd besproken hoe informatiebeveiliging en daarmee ook de BIO binnen de overheid verbeterd kan worden. De uitkomst van deel 1 van de evaluatie - een bevestiging van de bestaansreden van de BIO - was bepalend voor het al dan niet starten van het tweede deel van de evaluatie.

Opzet deel 2

Het tweede deel van de evaluatie beantwoordde de vragen welke verbeteringen op het instrument BIO mogelijk zijn. Dit deel van de evaluatie bouwde nadrukkelijk voort op de uitkomsten van en binnen de kaders van deel 1. Het tweede deel van de evaluatie levert verbetervoorstellen op voor het instrument BIO. De vragen van het tweede deel van de evaluatie werden beantwoord middels enkele interactieve werksessies. De opzet van deze sessies in dit tweede deel waren vergelijkbaar in vorm en inhoud als de bestuurlijke sessies.

In een drietal gecombineerde interactieve digitale werksessies werden de vooraf gestelde onderwerpen en vragen beantwoord. Voorafgaand aan de sessies hebben de deelnemers een vragenlijst toegestuurd gekregen. Deze vragenlijst is grotendeels gebaseerd op de aangeleverde vragenlijst door de opdrachtgever (bijlage 1). De uitkomsten van die vragenlijsten zijn gebruikt om enerzijds een eerste beeld op te halen en anderzijds de discussie te richten op de opvallende zaken en de bevindingen nader te verdiepen. Bijvoorbeeld wanneer de uitkomst van de deelnemers van een sessie afweek van die van de andere sessies, of wanneer er uiteenlopende antwoorden gegeven werden, was er aanleiding om wat langer bij een onderwerp stil te staan in de betreffende sessie. Gedurende de sessies zijn deze beelden nader uitgediept. Op deze wijze zijn effectief en tijdsefficiënt organisaties bij elkaar gebracht en ontstond een platform waar transparant is gesproken over mogelijke verbeteringen. Ook deze digitale groepssessies vonden plaats met een representatieve vertegenwoordiging.

Bij de uitvoering van de evaluatie zijn in beide delen telkens nadrukkelijk de gehanteerde begrippen geïntroduceerd en afgebakend en, indien nodig, gedurende de evaluatie op bijgestuurd, zodat de bevindingen daadwerkelijk op het besproken aspect van toepassing zijn.

Opdrachtgeverschap en begeleiding

De opdracht voor de evaluatie is gegeven door DGDOO/ BZK in nauwe samenwerking met de vier overheidslagen. De vier overheidslagen hebben zich middels verplichtende zelfregulering opgelegd de BIO te volgen en waren derhalve belangrijke stakeholders in dit traject. Hoewel BZK formeel de opdrachtgever is, is over voortgang van de evaluatie verantwoording afgelegd aan de vier overheidslagen die vertegenwoordigd zijn in het kern-IBO. Het kern-IBO wordt geadviseerd door de werkgroep-BIO. De werkgroep-BIO fungeerde als klankbordgroep tijdens de evaluatie.

Reikwijdte en vertegenwoordiging van de evaluatie

De reikwijdte van de opdracht is afgebakend tot een evaluatie van de ontwerpprincipes van de BIO. De impact van de nieuwe ISO 27002, aanvullingen op of aanscherping van de inhoud van de overheidsmaatregelen ('deel drie van de evaluatie') of specifieke (tekstuele) verbeteringen op het niveau van de controls vallen buiten scope van de opdracht.

Gedurende de voorbereidende fase is door de vertegenwoordigers van de overheden in het kern-IBO een representatieve lijst met deelnemers voor beide onderdelen van de evaluatie aangeleverd. Hoewel het in eerste instantie lastig was tijdig de juiste en voldoende deelnemers aan te laten sluiten, ontstond door deze opzet een gedragen, brede en representatieve vertegenwoordiging van betrokken overheidslagen. De aangeleverde vertegenwoordigers vormen naar inzicht van de kern-IBO leden dan ook een representatieve vertegenwoordiging van de overheidslagen op de verschillende niveaus en zorgen op deze wijze voor gedragen inbreng in de evaluatie vanuit de overheidslagen.

De deelnemers in het eerste deel van de evaluatie waren onder meer CIO's, (programma)managers en directeuren afkomstig uit (vertegenwoordigende organisaties van) gemeenten, provinciën, waterschappen en de rijksoverheid (vanuit diverse departementen). Ook hebben enkele burgemeesters, CISO's en een deelnemer van de Auditdienst Rijk deelgenomen. De deelnemers in het tweede deel van de evaluatie bestonden veelal uit CISO's of informatiebeveiligingsadviseurs uit alle bestuurslagen, deelnemers uit vertegenwoordigende of samenwerkende organisaties, zoals VNG, IPO en de UvW, een aantal grote uitvoeringsorganisaties (zoals UWV en SVB), de 'hofleveranciers' van producten op vlak van informatiebeveiliging en privacybescherming zoals het Centrum Informatiebeveiliging en Privacybescherming (CIP), Informatiebeveiligingsdienst (IBD), het Nationaal Cybersecurity Centrum (hierna: NCSC) en Forum Standaardisatie en enkele grote leveranciers, zoals Microsoft, ADP en Centric en andere organisaties zoals NOREA.

Berenschot

‘WIJ ZIJN BERENSCHOT, GRONDLEGGER VAN VOORUITGANG’

Nederland is continu in ontwikkeling. Maatschappelijk, economisch en organisatorisch verandert er veel. Al meer dan tachtig jaar volgen wij als adviesbureau deze ontwikkelingen op de voet en werken we aan een vooruitstrevende samenleving. De behoefte om iets fundamenteels te betekenen voor mens en maatschappij zit in onze genen. Met onze adviezen en oplossingen hebben we dan ook actief meegebouwd aan het Nederland van vandaag. Altijd op zoek naar duurzame vooruitgang.

Alles wat we doen is onderzocht, onderbouwd en vanuit meerdere invalshoeken bekeken. Zo komen we tot gefundeerde adviezen en slimme oplossingen. Die zijn op het eerste gezicht misschien niet altijd de meest voor de hand liggende. Juist deze eigenzinnigheid maakt ons uniek. Daarbij zijn we niet van symptoombestrijding. En gaan pas naar huis als het is opgelost.

Berenschot Groep B.V.

Van Deventerlaan 31-51, 3528 AG Utrecht

Postbus 8039, 3503 RA Utrecht

030 2 916 916

www.berenschot.nl