



Ministerie van Financiën

Rapport

Onderzoek Beheer Verwijzingsportaal Bankgegevens Justid 2025

Definitief

Colofon

Titel	Onderzoek Beheer Verwijzingsportaal Bankgegevens Justid 2025
Uitgebracht aan	DG-Ondermijning van het ministerie van Justitie en Veiligheid
Datum	6 oktober 2025
Kenmerk	2025-0000475742
Referentienummer	2025-J&V-011

Inlichtingen
Auditdienst Rijk

Inhoud

Aanleiding opdracht—5

—7

(Management)samenvatting—7

Context—11

Leeswijzer—12

- 1 Bevindingen en aanbevelingen onderzoeksvraag 1 - “Governance van privacy en Informatiebeveiliging”—13**
 - 1.1 Inleiding—13
 - 1.2 Bevindingen en aanbevelingen die betrekking hebben op beheersmaatregel 1.1—14
 - 1.3 Bevindingen die betrekking hebben op beheersmaatregel 1.2—15
 - 1.4 Bevindingen die betrekking hebben op beheersmaatregel 1.3—15
 - 1.5 Bevindingen die betrekking hebben op beheersmaatregel 1.4—16
 - 1.6 Bevinding en aanbeveling die betrekking hebben op beheersmaatregelen 1.1 tot en met 1.4—16
 - 1.7 Bevindingen en aanbevelingen die betrekking hebben op beheersmaatregel 1.5—17
- 2 Bevindingen en aanbevelingen onderzoeksvraag 2 - “Wijzigingenbeheer”—25**
 - 2.1 Bevindingen en aanbevelingen die betrekking hebben op beheersmaatregelen 5.1 en 5.3—26
 - 2.2 Bevindingen die betrekking hebben op beheersmaatregel 5.3—27
 - 2.3 Bevindingen en aanbeveling die betrekking hebben op beheersmaatregelen 5.2 en 5.3—27
 - 2.4 Bevindingen en aanbevelingen die betrekking hebben op beheersmaatregelen 5.1 tot en met 5.3—28
 - 2.5 Bevindingen en aanbeveling die betrekking hebben op beheersmaatregel 5.4—31
- 3 Bevindingen en aanbevelingen onderzoeksvraag 3 - “Logische Toegangsbeveiliging”—33**
 - 3.1 Bevindingen en aanbevelingen die betrekking hebben op beheersmaatregel 6.1—35
 - 3.2 Bevinding en aanbevelingen die betrekking hebben op beheersmaatregel 6.6—36
 - 3.3 Bevindingen en aanbevelingen die betrekking hebben op beheersmaatregelen 6.1 tot en met 6.8—37
 - 3.4 Bevindingen en aanbeveling die betrekking hebben op beheersmaatregelen 6.1 en 6.4—39
 - 3.5 Bevinding en aanbeveling die betrekking hebben op beheersmaatregelen 6.1, 6.4 en 6.8—40
- 4 Bevindingen en aanbevelingen onderzoeksvraag 4 - “Back-up, restore en uitwijk”—41**
 - 4.1 Bevindingen en aanbevelingen die betrekking hebben op beheersmaatregel 9.1 en 9.2—42
 - 4.2 Bevindingen en aanbeveling die betrekking hebben op beheersmaatregel 9.4—42

- 4.3 Bevindingen en aanbevelingen die betrekking hebben op beheersmaatregel 9.1 tot en met 9.4—43

5 Verantwoording onderzoek—47

- 5.1 Werkzaamheden en afbakening—47
- 5.2 Gehanteerde standaard en kwaliteitsborging—49
- 5.3 Verspreiding rapport—49

6 Ondertekening—50

Bijlage 1 Managementreactie Justid Opsporing—51

Aanleiding opdracht

Op grond van artikel 5 lid 4 van het Besluit verwijzingsportaal bankgegevens van 10 september 2020 heeft de Auditdienst Rijk (ADR) in de periode april tot en met juni 2025 een audit naar het uitgevoerde beheer van het Verwijzingsportaal Bankgegevens (VB) bij de Justitiële Informatiedienst onderdeel Opsporing (Justid, een agentschap van het ministerie van Justitie en Veiligheid, hierna Justid Opsporing) uitgevoerd. Het Besluit verwijzingsportaal bankgegevens bevat o.a. nadere regels over de gegevens die via het Verwijzingsportaal Bankgegevens worden ontsloten, de technische eisen waaraan het systeem en de aansluiting daarop moeten voldoen, de partijen die bevoegd zijn om het VB te gebruiken (1) en uit te voeren audits.

Om verdere invulling te geven aan de bepalingen in het Besluit verwijzingsportaal bankgegevens heeft Directoraat-Generaal Ondermijning van het ministerie Justitie en Veiligheid (JenV) aan de ADR gevraagd een onderzoek uit te voeren naar een aantal beheerprocessen van het VB bij Justid Opsporing.

Doel onderzoek en onderzoeksvragen

Het doel van dit onderzoek is het geven van bevindingen en aanbevelingen bij de opzet, het bestaan en de werking van de verbijzonderde controle op de naleving van de BIO-maatregelen voor het VB door Justid Opsporing voor de volgende processen:

1. Governance van privacy en informatiebeveiliging;
2. Wijzigingenbeheer;
3. Logische toegangsbeveiliging;
4. Back-up, restore en uitwijk.

Met dit rapport willen wij een antwoord geven op de volgende onderzoeksvragen:

1. Welke bevindingen en aanbevelingen heeft de ADR over de uitgevoerde verbijzonderde controle door Justid op het beheerproces "Governance van privacy en informatiebeveiliging" voor het VB?
2. Welke bevindingen en aanbevelingen heeft de ADR over de uitgevoerde verbijzonderde controle door Justid op het beheerproces "Wijzigingenbeheer" voor het VB?
3. Welke bevindingen en aanbevelingen heeft de ADR over de uitgevoerde verbijzonderde controle door Justid op het beheerproces "Logische toegangsbeveiliging" voor het VB?

¹ Nationale Politie, het openbaar ministerie, de Koninklijke Marechaussee, de Rijksrecherche, de Fiscale Inlichtingen- en Opsporingsdienst, de Inlichtingen- en Opsporingsdienst van de Nederlandse Voedsel- en Warenautoriteit, de directie Opsporing van de Inspectie Sociale Zaken en Werkgelegenheid, de Inlichtingen- en Opsporingsdienst van de Inspectie Leefomgeving en Transport, de officier van justitie, FIU-Nederland en de Belastingdienst (de inspecteur, de ontvanger en de Belastingdienst/Toeslagen)

4. Welke bevindingen aanbevelingen heeft de ADR over de uitgevoerde verbijzonderde controle door Justid op het beheerproces "Back-up, restore en uitwijk" voor het VB?

Peildatum onderzoek

De peildatum van ons onderzoek is 24 mei 2025. Op deze datum heeft hoor en wederhoor met Justid Opsporing plaatsgevonden. Alle aangereikte documentatie van Justid ten behoeve van ons onderzoek voorafgaand aan de peildatum is meegenomen.

(Management)samenvatting

In het Besluit verwijzingsportaal bankgegevens is bepaald dat jaarlijks een audit moet worden uitgevoerd naar de werking van het Verwijzingsportaal Bankgegevens (VB) en de kwaliteit van vorderingen, verzoeken en verstrekkingen van gegevens. Het directoraat-generaal Ondernijning van het ministerie van Justitie en Veiligheid, de opdrachtgever van het VB, heeft de Auditdienst Rijk (ADR) gevraagd een onderzoek bij Justid Opsporing te doen om daarmee invulling te geven aan de auditbepaling van het besluit.

Deze samenvatting bevat op hoofdlijnen de belangrijkste aandachtspunten van het onderzoek bij Justid Opsporing en geeft antwoord op de onderzoeksvraag: Welke bevindingen en aanbevelingen heeft de ADR voor het VB over de uitgevoerde verbijzonderde controle door Justid Opsporing over de periode 4^e kwartaal 2024 tot en met het 1^e kwartaal 2025 op de beheerprocessen "Governance van privacy en informatiebeveiliging", "Wijzigingsbeheer", "Logische Toegangsbeveiliging" en "Back-up, restore en uitwijk"?

In het vorige onderzoeksrapport "Follow-up ADR-bevindingen Verwijzingsportaal bankgegevens 2023 bij Justid Opsporing" van 8 juli 2024 (kenmerk 2024-0000375298) was vermeld dat vijf jaar na de vaststelling van de Baseline Informatiebeveiliging Overheid (BIO) (versie 1.04) van 4 november 2019 het opzetten en het inrichten van de BIO-maatregelen bij Justid Opsporing nog niet was afgerond. Justid Opsporing had bij de audit in 2024 aangegeven dat zij het belang van de BIO zeker onderkent en dat zij in 2024 ernaar streefde de specifieke BIO-maatregelen voor het VB ingericht te hebben. Om dit mede te kunnen realiseren had Justid Opsporing een deskundige ingehuurd. Deze deskundige was medio 2024 vertrokken. ADR heeft gezien dat Justid Opsporing veel werk heeft verzet aan de professionalisering van het proces rond de BIO-controles VB en de inrichting ervan.

Naar aanleiding van ons onderzoek rapporteren wij een aantal bevindingen en aanbevelingen. Met het opvolgen van de aanbevelingen kan een groei naar een hoger volwassenheidsniveau op het proces "Uitvoering van verbijzonderde BIO-controles" binnen Justid Opsporing worden bereikt. Hieronder zijn onze bevindingen opgenomen.

Procesbeschrijving uitvoering BIO-controles ontbreekt

Een procesbeschrijving over uitvoering BIO-controles vanuit Justid breed is niet aangetroffen, waarin minimaal het volgende is beschreven: verantwoordelijkheden binnen het controleproces, de wijze van plannen BIO-controles en de uitvoering ervan, op welke wijze de generieke en specifiek BIO-controles uitgevoerd moeten worden (consistente werkwijze binnen alle organisatieonderdelen van Justid), hoe opzet, bestaan en werking geïnterpreteerd dienen te worden voor consistente uitvoering van de controle en de wijze van het bespreken en rapporteren van de bevindingen binnen Justid en Justid Opsporing.

Aanbeveling (Justid en Justid Opsporing)

- Stel een procedure beschrijving op en vast die gericht is op de controle op de BIO-maatregelen en zorg voor de inrichting binnen Justid breed, zodat de uitvoering van de BIO-controles binnen Justid breed op een consistente wijze plaatsvindt.

De kwalitatieve vastlegging van de resultaten in de BIO-sjablonen/Topdeskregistraties is niet altijd toereikend

Voor een groot aantal controles op de BIO-maatregelen geldt dat het BIO-sjabloon en/of Topdeskregistratie in opzet, bestaan en werking niet is voorzien van een beschrijving (onderbouwing/toelichting) waarop de conclusies zijn gebaseerd. Bij sommige registraties wordt alleen verwezen naar onderliggende documentatie (audittrail). De Information Security Officer (ISO) beoordeelt de BIO-sjablonen (en/of Topdeskregistraties), maar zijn oordeelsvorming is niet zichtbaar op deze stukken vastgelegd.

Aanbevelingen (Justid Opsporing)

- Draag zorg voor de kwalitatieve vastlegging van de onderbouwde conclusie (incl. verwijzing naar beoordeelde documentatie en/of screenshots) in het BIO-sjabloon en/of de Topdeskregistratie voor opzet, bestaan en werking.
- Draag zorg dat het oordeel van de ISO zichtbaar in het BIO-sjabloon en/of de Topdeskregistratie wordt vastgelegd.

Vastlegging geplande/uitgevoerde BIO-controles in dashboard ISO Justid Opsporing heeft beperkingen

Op dit moment verzorgen de ISO's binnen Justid de realisatie van de generieke beheersmaatregelen door handmatige handelingen op basis van gesprekken met de verschillende afdelingen. Om inzicht te krijgen in de stand van zaken rondom de uitvoering van de BIO-controles VB wordt gebruik gemaakt van een dashboard van ISO Justid Opsporing. Dit dashboard geeft niet in alle gevallen de werkelijkheid (juistheid en volledigheid) weer van de stand van zaken over de kwantitatieve uitvoering van de BIO-controles VB (o.a. planning versus realisatie). Het gevolg hiervan is dat het compliancy-percentages een onjuiste waarde weergeeft. Daarnaast is het dashboard ISO alleen kwantitatief van aard en toont alleen numerieke waarden die overeenkomen met een compliancy-percentages. Kwalitatieve informatie

over de uitgevoerde BIO-controles waarop de conclusies zijn gebaseerd wordt niet meegenomen in het dashboard.

De GRC-tool "Key Control Dashboard (KCD)"² wordt binnen heel JenV ingezet, maar is niet bruikbaar voor de werkwijze binnen Justid. Daardoor ontbreekt een mechanisme om de algehele vastlegging van de geplande/uitgevoerde BIO-controles te waarborgen. Ook zijn er geen rapportagemogelijkheden om een kwantitatief en kwalitatief overzicht te creëren van de huidige stand van zaken met betrekking tot de generieke en specifieke beheersmaatregelen. Justid Opsporing heeft op 8 juli 2025 meegedeeld dat het nieuwe GRC-tool voor besluitvorming is voorgelegd aan het Directieteam Justid.

Aanbevelingen (Justid Opsporing)

- Draag zorg voor dat het dashboard ISO de juiste en volledige bestuurlijke informatie weergeeft over de kwantitatieve uitvoering van de BIO-controles voor VB (planning versus realisatie) en dat de gegeven conclusies voor opzet, bestaan en werking in het dashboard ISO ook overeenstemmen met de resultaten voortvloeiend uit de daadwerkelijk uitgevoerde BIO-controles VB.
- Draag zorg voor dat uit het dashboard de relatie blijkt tussen de uitkomsten van de uitgevoerde BIO-controles (opzet, bestaan en werking) met het betreffende BIO-sjabloon en/of Topdeskregistratie. Leg in het kort ook de kwalitatieve onderbouwing van de conclusies in het dashboard vast.
- Draag zorg voor dat in de nieuwe GRC-tool de kwantitatieve en kwalitatieve uitvoering van de BIO-controles op een consistente wijze worden vastgelegd en dat uit deze tool een BI-rapportage vervaardigd kan worden waaruit blijkt de stand van zaken omtrent uitvoering van de BIO-controles en de kwalitatieve onderbouwing van de conclusies voor opzet, bestaan en werking.

BIO-implementatie en controles niet op de agenda maandelijks BIO-overleg

Kwalitatieve beoordeling en vastlegging van de BIO-implementatie en de controle hierop wordt tijdens het maandelijks BIO-overleg en met het dashboard ISO niet expliciet behandeld en vastgelegd in notulen. Generieke BIO-controles uitgevoerd door het Cluster Beveiliging worden niet besproken tijdens het maandelijks BIO-overleg van Justid Opsporing. Het onderzoek was gebaseerd op BIO versie 1.04 van 4 november 2019. Inmiddels is de nieuwe Baseline Informatiebeveiliging Overheid 2 (BIO2) van 14 maart 2025 van kracht.

Aanbeveling (Justid Opsporing)

- Draag zorg voor dat tijdens het maandelijks overleg binnen Justid Opsporing niet alleen de kwantitatieve voortgang van de implementatie en de controle van de BIO-maatregelen worden besproken maar ook de resultaten voortvloeiend uit de uitgevoerde

² GRC-tool (Governance, Risk & Compliance) is software die organisaties helpt bij het beheren en controleren van hun governance, risico's en naleving van regelgeving.

BIO-controles. Leg datgene wat besproken is vast in een notulen, waarmee aangetoond kan worden dat het bespreken van de BIO-controles zijn aandacht krijgt binnen Justid Opsporing.

- Draag zorg voor tijdige implementatie van beheersmaatregelen gebaseerd op BIO2.

Geen rapportage Justid Opsporing aan Justid over uitvoering BIO-controles

De manager Justid Opsporing geeft aan dat er geen rapportage over de uitvoering van de BIO-controles VB binnen Justid Opsporing aan Justid breed (zoals CISO, Privacyfunctionaris, MT/DT Justid) plaatsvindt over de bevindingen en te ondernemen acties met betrekking tot (niet) uitgevoerde BIO-maatregelen VB.

Aanbeveling (Justid Opsporing)

- Draag zorg voor een kwalitatieve rapportage waaruit blijkt in hoeverre Justid Opsporing voldoet aan de beheersing van (beheer) activiteiten (BIO-controles en overige beheersingsmaatregelen) gericht op onder andere: Governance, Contractmanagement, Incidentbeheer, Wijzigingenbeheer, Logische Toegangsbeveiliging, Beveiliging van IT-infrastructuur en data, Back-up, restore en uitwijk en Opschonen en vernietigen van data.

Aantal BIO-controles niet onafhankelijk uitgevoerd.

De ADR heeft vastgesteld dat een aantal BIO-controles VB is uitgevoerd door een functionaris die zelf betrokken is in het proces. Er is geen sprake van een onafhankelijke controle. Het aantal functionarissen dat operationele werkzaamheden doet voor het VB is bij Justid Opsporing beperkt. Daarnaast is de ISO niet alleen betrokken voor het VB, maar ook voor andere informatiesystemen. De manager Justid Opsporing heeft aangegeven dat het wenselijk is om een Informatie Beveiligingsfunctionaris aan te trekken. Ondanks het verzoek van manager Justid Opsporing is er geen officiële rol voor Informatiebeveiligingsfunctionaris ingevuld bij Justid Opsporing. De ISO van Justid Opsporing doet naast de ISO-werkzaamheden ook een deel van de IBF-werkzaamheden, maar dit acht de manager Justid Opsporing niet toereikend genoeg voor alle taken die behoren tot de rol van IBF'er.

Aanbeveling

- Draag in eerste instantie zorg dat de uitvoering van de BIO-controles plaatsvindt door een functionaris die niet betrokken is bij het proces. Als blijkt dat dit gezien de organisatiegrootte voor het VB niet realiseerbaar is, bepaal aanvullende beheersingsmaatregelen. Hierbij kan gedacht worden aan de inhoudelijke beoordeling door de ISO op de uitgevoerde BIO-controles en dat deze functionaris zijn beoordeling vastlegt op het BIO-sjabloon of in de topdeskregistratie en dashboard ISO (later: in de nieuwe GRC-tool).

Context

Het Verwijzingsportaal Bankgegevens (VB)

Het VB is een digitale voorziening voor de geautomatiseerde verstrekking van gegevens die worden opgevraagd door de daartoe bevoegde overheidsdiensten in de strafrechtketen (o.a. Politie, KMAR, Nederlands Arbeidsinspectie en de Belastingdienst (bevragers)). Banken en andere betaaldienstverleners (verstrekkers) zijn wettelijk verplicht om aan dergelijke vorderingen of bevragingen door deze diensten te voldoen. Het beheer van het portaal VB is ondergebracht bij Justid en werkt als doorgeefluik tussen de verstrekkers en de afnemende organisaties.

Justid Opsporing voert voor het VB de volgende beheertaken uit:

- Applicatiebeheer: het proces om software en databases te onderhouden en aan te passen aan nieuwe omstandigheden. Hieronder vallen het incidentbeheer, het wijzigingsbeheer en het beheer van toegangsrechten;
- Technisch beheer: het operationeel houden, onderhouden en vernieuwen van de technische infrastructuur (netwerken, apparatuur). Hieronder vallen de monitoring van de infrastructuur en de koppelingen met alle banken, de beveiliging van de infrastructuur en het beheer van alle technische componenten.

In het Besluit verwijzingsportaal bankgegevens van 2020 is in artikel 5 lid 4 opgenomen dat de eerste vijf jaar na de inwerkingtreding van het besluit de audit jaarlijks zal worden gedaan. De audit bij Justid Opsporing vindt jaarlijks plaats. Een volledige audit zoals in 2022 is uitgevoerd wordt afgewisseld door een opvolgaudit met beperkte reikwijdte.

In de Tweede Kamer is door de minister van JenV de toezegging gedaan dat de audits tot en met 2027 jaarlijks zullen blijven plaatsvinden.

Leeswijzer

In hoofdstukken 1 tot en met 4 gaan wij in op de centrale onderzoeksvraag: Welke bevindingen en aanbevelingen heeft de ADR voor het VB over de uitgevoerde verbijzonderde controle door Justid op de beheerprocessen "Governance van privacy en informatiebeveiliging" (hoofdstuk 1), "Wijzigingsbeheer" (hoofdstuk 2), "Logische Toegangsbeveiliging" (hoofdstuk 3) en "Back-up, restore en uitwijk" (hoofdstuk 4)?

In hoofdstuk 5 geven wij een toelichting op het door ons uitgevoerde onderzoek.

In bijlage 1 is de managementreactie van Justid Opsporing op het rapport opgenomen.

Voor wie is dit rapport?

Dit rapport is opgesteld voor de opdrachtgever voor het onderzoek, de plaatsvervangend directeur-generaal van DGO. Met dit rapport wordt DGO in staat gesteld om de Tweede Kamer te informeren over de resultaten van de uitgevoerde audit.

Met dit rapport wordt geen zekerheid verschaft, omdat geen assurance-werkzaamheden zijn uitgevoerd. Het rapport bevat daarom geen samenvattende conclusie of eindoordeel.

1 Bevindingen en aanbevelingen

onderzoeksvraag 1 - "Governance van privacy en Informatiebeveiliging"

1.1 Inleiding

In dit hoofdstuk zijn de bevindingen en aanbevelingen opgenomen die betrekking hebben op de onderzoeksvraag: "Welke bevindingen en aanbevelingen heeft de ADR over de uitgevoerde verbijzonderde controle door Justid Opsporing op het beheerproces "Governance van privacy en informatiebeveiliging" voor het VB over de periode 4^e kwartaal 2024 tot en met het 1^e kwartaal 2025?

Voor de meest relevante bevindingen hebben wij een aanbeveling meegegeven.

Voor het beheerproces "Governance van privacy en informatiebeveiliging" is in de onderstaande tabel per norm aangegeven welke BIO-maatregelen van toepassing zijn. Deze BIO-maatregelen zijn afgeleid uit de Baseline Informatiebeveiliging Overheid (BIO) (versie 1.04) van 4 november 2019. Voor de uitvoering van de verbijzonderde controle op de BIO-maatregelen maakt Justid onderscheid tussen generieke BIO-maatregelen en specifieke BIO-maatregelen voor VB. De benoemde generieke BIO-maatregelen zijn ook relevant voor VB. Justid Opsporing heeft per BIO-maatregel aangegeven welke BIO maatregelen belegd zijn bij het Cluster Beveiliging van Justid (generiek) en Justid Opsporing (specifiek).

1 Governance van privacy en Informatiebeveiliging (scope onderzoek VB bij Justid 2025)			
Nr	Beheersmaatregel	Belegd bij Justid Cluster Beveiliging Generieke BIO-maatregelen	Belegd bij Justid Opsporing Specifiek BIO-maatregelen
1.1	<i>De verantwoordelijkheid voor het blijven voldoen aan geldende kaders voor informatiebeveiliging is belegd in de organisatie.</i>	5.1; 5.1.1.1 5.1.2.1	
1.2	<i>De verantwoordelijkheid voor het blijven voldoen aan geldende kaders op het gebied van privacy is belegd in de organisatie.</i>	18.1.4; 18.1.4.1	
1.3	<i>Periodiek wordt vastgesteld dat privacy en bescherming van persoonsgegevens worden gewaarborgd in overeenstemming met</i>	18.1.4; 18.1.4.2 < ook belegd Justid Privacy >	

	<i>relevante wet- en regelgeving (AVG, WPG, WJSG).</i>		
1.4	<i>Periodiek wordt VB beoordeeld op naleving van het beleid en de maatregelen voor informatiebeveiliging (BIO).</i>	18.2.3; 18.2.3.1	
1.5	<i>Periodiek wordt de manager Opsporing en de CISO op de hoogte gebracht van de uitgevoerde verbijzonderde controles op de generieke – en specifieke BIO-maatregelen VB</i>	ADR ³	

1.2 Bevindingen en aanbevelingen die betrekking hebben op beheersmaatregel 1.1

Cluster Beveiliging heeft op 18 maart 2025 het document “BIO controls ADR” d.d. 18 maart 2025 aangereikt en voor de BIO-maatregelen het volgende aangegeven:

- a) 5.1.1.1: “Integraal beveiligingsbeleid” is herzien en in november 2022 vastgesteld door Algemeen Directeur Justid”;
- b) 5.1.2.1: “Het IB beleid is beschikbaar voor medewerkers van Justid en wordt minimaal 1x in de 3 jaar herzien”.

Uit het overzicht “18032025 – BIO controls ADR – audit VB” is niet vast te stellen wanneer deze BIO-controles 5.1.1.1 en 5.1.2.1 daadwerkelijk zijn uitgevoerd en op basis waarvan de conclusie voor opzet, bestaan en werking zijn gebaseerd (inclusief onderbouwing/toelichting).

Er zijn voor de BIO-maatregelen 5.1.1.1 en 5.1.2.1 geen BIO-sjablonen aangereikt. (zie § 1.6 – en § 1.7 -BIO-sjablonen (Topdeskmeldingen) - 2^e bullet)

Herzien frequentie evaluatie Integraal beveiligingsbeleid is een aandachtspunt

Voor BIO-maatregel 5.1.2.1 is aangegeven dat het Integraal beveiligingsbeleid (IB-beleid) van Justid minimaal 1x in de drie jaar wordt herzien. ADR is van mening dat gezien de veranderingen in de nieuwe wetgevingen (o.a. Cyberbeveiligingswet, inclusief kader BIO 2.0) en externe spanningen (lokale en internationale cyberbedreiging) het IB-beleid (incl. risicoanalyse) ieder jaar dient te worden geëvalueerd in plaats van minimaal 1x per drie jaar. Het IB-beleid is herzien en vastgesteld in november 2022 door de Algemeen Directeur Justid. De CISO Justid heeft op 12 mei 2025 het volgende meegedeeld:

- a) Het Integraal beveiligingsbeleid v2.0 zal in 2025 ((laatst vastgesteld en akkoord 2022) worden herzien en vastgesteld;
- b) Terechte opmerking van ADR om de periodiciteit van de vaststelling van dit beleid aan te scherpen. De CISO Justid zal dit intern bespreekbaar maken.

³ Relevante beheersmaatregel, toegevoegd door de ADR, niet af te leiden van de BIO

Aanbeveling (Cluster Beveiliging en Justid Opsporing)

- Draag er zorg voor dat het Integraal Beveiligingsbeleid jaarlijks wordt herzien en vastgesteld.
- Draag er zorg voor dat de eerste lijn (o.a. Justid Opsporing) tijdig over het hernieuwd Integraal Beveiligingsbeleid wordt geïnformeerd, zodat de eerste lijn op basis van dit beleid zorg kan dragen voor aanpassingen van de inrichting van hun informatiesystemen (zoals Justid Opsporing voor het VB).

1.3 Bevindingen die betrekking hebben op beheersmaatregel 1.2

Cluster Beveiliging heeft op 18 maart 2025 het document "BIO controls ADR" d.d. 18 maart 2025 aangereikt en voor de BIO 18.1.4.1 het volgende meegedeeld: "Justid heeft een Privacy Officer die namens de FG van JenV het beleid t.a.v. Privacy uitrolt". Uit het overzicht "18032025 – BIO controls ADR – audit VB" is niet vast te stellen wanneer de controle daadwerkelijk is uitgevoerd en op basis waarvan de conclusies voor opzet, bestaan en werking zijn gebaseerd (inclusief onderbouwing/toelichting).

Het document "PROCESBESCHRIJVING Meldplicht Datalekken versie 1.0 definitief dd 180222 ondertekend" d.d. 18 februari 2022 is door de Teamleider VB op 7 april 2025 als onderliggende evidence aangereikt. In Bijlage 1 "Invultabel" van dat document staat op pagina 20 de naam van de aangestelde Privacy Officer vermeld. ADR heeft aan de hand van de Rijksadresgids vastgesteld dat de naam van de Privacy Officer overeenkomt met de naam in het aangereikte document.

Er is voor de BIO-maatregel 18.1.4.1 geen BIO-sjabloon aangereikt. (zie § 1.6 – en § 1.7 -BIO-sjablonen (Topdeskmeldingen) - 2^e bullet)

1.4 Bevindingen die betrekking hebben op beheersmaatregel 1.3

Cluster Beveiliging heeft op 18 maart 2025 het document "BIO controls ADR" d.d. 18 maart 2025 aangereikt en voor de BIO 18.1.4.2 het volgende meegedeeld: "Justid heeft een Privacy team met 5 Privacy medewerkers die voor relevante systemen een DPIA uitvoeren in samenwerking met de afdelingen waar de systemen in beheer zijn. Het Privacy team wordt betrokken bij datalekken, beveiligingsincidenten en nieuwe projecten om de AVG te handhaven binnen Justid". Uit het overzicht "18032025 – BIO controls ADR – audit VB" is niet vast te stellen wanneer de BIO-controle 18.1.4.2 daadwerkelijk is uitgevoerd en op basis waarvan de conclusie voor opzet, bestaan en werking zijn gebaseerd (inclusief onderbouwing/toelichting).

De BIO-maatregel betreft niet alleen hoe om te gaan met datalekken, maar het betreft ook het aantonen van de naleving op de geïmplementeerde privacywet- en regelgeving door het privacy-team van Justid (onder toezicht van de Privacy Officer). ADR heeft voor de toetsingsnorm 1.3 geen documentatie ontvangen van een periodiek toezicht (rapportages) door het privacy-team van Justid (onder

toezicht van de Privacy Officer) waaruit blijkt dat voor onder ander het VB-systeem de privacy en bescherming van persoonsgegevens worden gewaarborgd in overeenstemming met relevante wet- en regelgeving (AVG, WPG, WJSG).

Er is voor de BIO-maatregel 18.1.4.2 geen BIO-sjabloon aangereikt.
(zie § 1.6 – en § 1.7 -BIO-sjablonen (Topdeskmeldingen) - 2^e bullet)

1.5 Bevindingen die betrekking hebben op beheersmaatregel 1.4

Cluster Beveiliging heeft op 18 maart 2025 het document "BIO controls ADR" d.d. 18 maart 2025 aangereikt en voor de BIO 18.2.3.1 het volgende meegedeeld: "Kwetsbaarheidsanalyses gebeurt via Nessus in Den Haag. Daarnaast wordt code kwaliteit uitgevoerd door SIG. Pentesten worden periodiek uitgevoerd: bij nieuwe systemen, grote wijzigingen of 1x in de 3 jaar".

Uit het overzicht "18032025 – BIO controls ADR – audit VB" is niet vast te stellen wanneer de BIO-controle 18.1.4.2 daadwerkelijk is uitgevoerd en op basis waarvan de conclusie voor opzet, bestaan en werking zijn gebaseerd (inclusief onderbouwing/toelichting).

ADR heeft voor de generieke maatregel 18.2.3.1) geen documentatie en een BIO-sjabloon ontvangen van een uitgevoerd periodieke beoordeling op naleving van het beleid en de maatregelen voor informatiebeveiliging (BIO) voor het VB-systeem vanuit het Cluster Beveiliging of door ISO Justid Opsporing (namens de CISO).
(zie § 1.6 en § 1.7 -BIO-sjablonen (Topdeskmeldingen) - 2^e bullet)

1.6 Bevinding en aanbeveling die betrekking hebben op beheersmaatregelen 1.1 tot en met 1.4

Voor generieke BIO-maatregelen wordt geen gebruik gemaakt van BIO-sjablonen
Door CISO Justid is op 12 mei 2025 medegedeeld dat voor de generieke BIO-maatregelen 5.1.1.1, 5.1.2.1, 18.1.4.1, 18.1.4.2 en 18.2.3.1 er geen BIO-sjabloon wordt gehanteerd vanwege veranderingen door de komst van de BIO 2.0 en de lopende marktverkenning naar een nieuwe GRC-tool. De standaard BIO-sjablonen zijn door de CISO en zijn beveiligingsteam ontwikkeld voor de specifieke beheersmaatregelen om de werkzaamheden voor de Informatiebeveiligingsfunctionarissen (IBF'ers) te standaardiseren. De BIO-sjablonen zullen in de nieuwe GRC-tool worden geïntegreerd om de PDCA-cyclus te automatiseren voor de eerste lijn.

Aanbeveling (Cluster Beveiliging en Justid Opsporing)

Draag er zorg voor dat zowel voor de generiek- als voor de specifiek BIO-maatregelen gewerkt wordt met een consistente eenduidige vastlegging van de uit te voeren BIO-controles in de BIO-sjablonen en/of Topdeskregistratie (later in de nieuwe GRC-tool). Vastlegging heeft betrekking op: planning, realisatie, toelichting op opzet, bestaan en werking (inclusief de conclusies), te ondernemen acties voortvloeiend uit de controle.

Algemeen

In de Baseline Informatiebeveiliging Overheid (BIO) (versie 1.04) van 4 november 2019 staat beschreven dat de BIO alleen het WAT beschrijft (controles en maatregelen per beveiligingsdoelstelling) en niet het HOE (inrichting van beheersingsmaatregelen). De inrichting van de beheersingsmaatregelen is belegd bij het lijnmanagement. Het beveiligen van informatie is echter geen eenmalige zaak, maar een proces waarbij steeds de Plan-Do-Check-Act cyclus wordt doorlopen. Het doorlopen van dit proces is een verantwoordelijkheid van elk lijnmanagement. Het is van belang dat Justid Opsporing voor VB zelf aantoont of zij voor VB in control is of niet.

In deze paragraaf gaan wij nader in op de bevindingen voor het proces PCDA-cyclus bij Justid Opsporing voor het VB, te weten: verantwoordelijkheden, relatie Justid Opsporing met Justid, Overleg Justid Opsporing, Dashboard ISO, BIO-sjabloon (Topdeskmeldingen), rapportage en een aantal opzetdocumentatie.

Justid Opsporing heeft voor de beheersmaatregel 1.5 geen specifieke beheersingsmaatregel beschreven en ingericht. Dit betreft een door de ADR relevant geachte beheersingsmaatregel. Deze is niet uit de BIO (versie 1.04) af te leiden. De Teamleider VB en de Product Owner VB van Justid opsporing hebben tijdens de interviews meegedeeld dat zij voortdurend werken aan professionalisering van het proces rond de BIO-controles en dat de kwalitatieve invulling ervan nog de nodige aandacht behoeft.

Verantwoordelijkheden

De Manager van Justid Opsporing is met name verantwoordelijk voor de systeem specifieke BIO-maatregelen van Justid IBO voor een aantal informatiesystemen, waaronder het VB. Daarnaast draagt de manager een gedeelde verantwoordelijkheid voor de overige generieke BIO-maatregelen. De voornaamste bijdrage is het zorgdragen voor het consistent oppakken van de werkzaamheden door de verschillende teams (waaronder het VB) binnen Justid Opsporing.

Per controle wordt een verantwoordelijke functionaris aangewezen. Deze functionaris is ook verantwoordelijk voor de uitvoer van de controle op de geïmplementeerde BIO-maatregel. Justid Opsporing heeft meegedeeld dat het voorgaande niet altijd goed gaat. Vandaar dat Justid Opsporing gedeeltelijk is overgegaan op het gebruik van Topdesk, omdat hier terugkerende activiteiten kunnen worden aangemaakt, waardoor de terugkerende controles middels een toegekende activiteit door de functionaris moeten worden opgepakt. Alleen blijft de aangewezen functionaris wel verantwoordelijk voor het uitvoeren van de controle.

Ondanks het verzoek van manager Justid Opsporing is er geen officiële rol voor Informatiebeveiligingsfunctionaris ingevuld bij Justid Opsporing. De ISO van Justid Opsporing doet naast de ISO-werkzaamheden ook een deel van de IBF-werkzaamheden, maar dit acht de manager Justid Opsporing niet toereikend genoeg voor alle taken die behoren tot de rol van IBF'er.

Afstemming uitkomsten BIO-controles tussen Justid Opsporing en Justid

Manager Justid Opsporing is niet aangehaakt bij Justid breed overleg over de voortgang van de kwalitatieve en kwantitatieve controle op de BIO-maatregelen (waaronder ook voor VB). Generiek beleid m.b.t. invulling van de controle op generiek- en specifieke BIO-maatregelen niet bekend bij Manager Opsporing

Er ontbreekt in opzet, bestaan en voor de werking evidence waaruit blijkt dat periodiek de CISO op de hoogte wordt gebracht van de verbijzonderde controles die door Justid Opsporing worden uitgevoerd naar de systeem specifiek geïmplementeerde BIO-maatregelen VB.

Er is naar het idee van de manager Justid Opsporing geen generiek beleid over hoe om te gaan met de invulling van de generieke en specifieke BIO-maatregelen voor Justid breed en de diverse organisatieonderdelen binnen Justid (o.a. implementatie en controle). Vanuit de directie wordt aangegeven dat systemen compliant moeten zijn met de BIO-maatregelen. De PDCA-cyclus vanuit Justid breed is de manager Opsporing niet duidelijk.

De samenhang tussen het specifieke beleid van Justid Opsporing en het generieke Justid beleid is de manager niet duidelijk.

De manager Opsporing is niet aangehaakt bij Justid breed overleg over de voortgang van de kwalitatieve en kwantitatieve controle op de BIO-maatregelen VB. De manager Opsporing geeft aan dat er hier onvoldoende aansluiting over is tussen Justid en Justid Opsporing.

Naar aanleiding van een vraag over de invulling van de controle op de generieke BIO-maatregelen van een ander team binnen Justid Opsporing ligt er nu een verzoek tussen de ISO en het Cluster Beveiliging om meer inzicht te krijgen over de voortgang en controle op systeem generieke implementatie van de BIO-maatregelen.

De controle op de naleving van generieke en specifieke BIO-maatregelen vindt plaats door het Beveiligingsteam. De CISO en de Beveiligingscoördinator (BVC) hebben periodiek overleggen met de Managers en Informatiebeveiligingsfunctionarissen (IBF'ers) van alle afdelingen binnen Justid. Daarnaast komen alle beveiligingsincidenten volgens de CISO bij het

Beveiligingsteam samen, hierdoor houden zij controle op bijv. het onjuist uitvoeren van het beleid.

De GRC-tool "Key Control Dashboard (KCD)" wordt binnen heel JenV ingezet, maar is niet bruikbaar voor de werkwijze binnen Justid en daardoor ontbreekt er een goed mechanisme om de algehele vastlegging van de geplande/uitgevoerde BIO-controls te waarborgen. De GRC-tool (KCD) die wordt afgenomen als gemeenschappelijke dienst van het Ministerie van Justitie en Veiligheid leent zich niet tot rapportagemogelijkheden om een kwantitatief en kwalitatief overzicht te creëren van de huidige stand van zaken met betrekking tot de generieke en specifieke beheersmaatregelen. Justid is bezig met het voortraject van een aanbesteding van een nieuwe GRC-tool die deze inzichten geautomatiseerd kan geven. Op dit moment verzorgen de ISO's binnen Justid de realisatie van de generieke beheersmaatregelen door handmatige handelingen op basis van gesprekken met de verschillende afdelingen.

Aanbeveling (Cluster Beveiliging en Justid Opsporing)

- Draag zorg voor een beleid/procedures over hoe de controles op generieke- en specifieke BIO-maatregelen (inclusief het bespreken van uitkomsten van de BIO-controles binnen de organisatie) ingevuld dienen te worden door Justid breed en de diverse organisatieonderdelen binnen Justid.

Overleg binnen Justid Opsporing

Bespreken van kwalitatieve beoordeling en vastlegging van de BIO-implementatie en de controle hierop in maandelijkse BIO-overleg binnen Justid Opsporing is een aandachtspunt

In het document "Proces BIO-implementatie & controle" wordt aangegeven dat er iedere maand een overleg plaatsvindt waar de manager Justid Opsporing op de hoogte wordt gebracht over de BIO-implementatie en de controle.

Tijdens het maandelijks overleg van Justid Opsporing wordt het dashboard van de ISO gebruikt als weergave van de werkelijkheid, waarmee de kwantitatieve voortgang van de implementatie en de controle van de BIO-normen worden getoond. Dit dashboard is kwantitatief van aard en toont alleen numerieke waarden die overeenkomen met een compliancy-percentages. Kwalitatieve beoordeling en vastlegging van de BIO-implementatie en de controle hierop wordt tijdens dit overleg en met dit dashboard niet expliciet behandeld.

Als er bevindingen zijn worden die besproken tijdens het overleg, maar meestal worden die van tevoren besproken door de ISO Justid Opsporing met Product Owner VB en Teamleider VB.

Generieke BIO-controles uitgevoerd door het Cluster Beveiliging worden niet besproken tijdens het maandelijks BIO-overleg van Justid Opsporing.

Aanbeveling (Justid Opsporing)

- Draag er zorg voor dat tijdens het maandelijks overleg binnen Justid Opsporing niet alleen de kwantitatieve voortgang van de implementatie en de controle van de BIO-maatregelen worden besproken maar ook de resultaten voortvloeiend uit de uitgevoerde BIO-controles. Leg datgene wat besproken is vast in een notulen, waarbij aangetoond kan worden dat het bespreken van de BIO-controles zijn aandacht krijgt binnen Justid Opsporing.

Dashboard ISO (1 april 2025)

Dashboard ISO van 1 april 2025 geeft alleen kwantitatieve bestuurlijke informatie over BIO-controles weer, kwalitatieve informatie ontbreekt; kwantitatieve informatie geeft niet juiste beeld weer

Volgens de manager Justid Opsporing is de waarde van het dashboard ISO dat het voor alle betrokkenen in één keer zichtbaar is waar Justid Opsporing staat op het BIO-gebied. Dit betreft voornamelijk wat de voortgang is en waar er nog werk te doen is.

Dashboard ISO van 1 april 2025 geeft niet de werkelijkheid (juistheid en volledigheid) weer van de stand van zaken over de kwantitatieve uitvoering van de BIO-controles (o.a. planning versus realisatie, formulier ingevuld/aangereikt wel of niet).

(Zie § 2.4, § 3.3 en § 4.3 - Dashboard ISO Justid Opsporing (1 april 2025) toont niet de juiste werkelijkheid weer van geplande/uitgevoerde BIO-controles)

Uit het gesprek met de ISO is naar voren gekomen dat het gebruik op het dashboard nog niet volledig is. Op dit moment wordt eerst gestreefd naar een eerste controle op alle relevante BIO-maatregelen voor VB. Frequentie versus realisatie speelt op dit moment nog geen rol in de verbijzonderde uitgevoerde controle binnen Justid Opsporing (VB).

Het dashboard ISO is kwantitatief van aard en toont alleen numerieke waarden die overeenkomen met een compliancy-percentages. De ISO beoordeelt de sjablonen en de resultaten worden alleen op een kwantitatieve manier opgenomen in het dashboard van de ISO. De planning versus de realisatie valt niet uit het dashboard op te maken. Kwalitatieve beoordeling en vastlegging van de BIO-controle is niet zichtbaar in het dashboard.

Aanbevelingen (Cluster Beveiliging en Justid Opsporing)

- Draag er zorg voor dat het dashboard ISO de juiste en volledige bestuurlijke informatie weergeeft over de kwantitatieve uitvoering van de BIO-controles voor VB (planning versus realisatie) en dat de gegeven conclusies voor

opzet, bestaan en werking in het dashboard ISO ook overeenstemmen met de resultaten voortvloeiend uit de daadwerkelijk uitgevoerde BIO-controles VB.

- Draag er zorg voor dat uit het dashboard blijkt de relatie tussen de uitkomsten van de uitgevoerde BIO-controles (opzet, bestaan en werking) met het betreffende BIO-sjabloon en/of Topdeskregistratie. Leg in het kort ook de kwalitatieve onderbouwing van de conclusies vast.
- Draag er zorg voor dat bij de nieuwe GRC-tool de kwantitatieve en kwalitatieve uitvoering van de BIO-controles op een consistente wijze worden vastgelegd en dat uit deze tool een BI-rapportage vervaardigd kan worden waaruit blijkt de stand van zaken over de uitvoering van de BIO-controles en de kwalitatieve onderbouwing van de conclusies opzet, bestaan en werking.

BIO-sjablonen (Topdeskmeldingen)

Kwalitatieve vastlegging resultaten in BIO-sjablonen/Topdeskregistratie is een aandachtspunt

Het specifieke BIO-sjabloon voor VB wordt als leidend beschouwd. Dit BIO-sjabloon moet worden ingevuld om tot een oordeel te komen over de mate waarin de BIO-maatregel in control (compliant) is. Het ingevulde BIO-sjabloon met onderbouwing van opzet, bestaan en werking (inclusief conclusie) moet ook de basis voor het oordeel van de ISO vormen. Voor een groot aantal controles op de BIO-maatregelen geldt dat het BIO-sjabloon en/of Topdeskregistratie in opzet, bestaan en werking niet is voorzien van een beschrijving (onderbouwing/toelichting) waarop de conclusies zijn gebaseerd. Bij sommige registraties wordt alleen verwezen naar onderliggende documentatie (audittrail). De ISO beoordeelt de BIO-sjablonen (en/of Topdeskregistraties), maar zijn oordeelsvorming is niet zichtbaar op deze stukken vastgelegd.

Cluster Beveiliging van Justid heeft de standaard BIO-sjablonen ontwikkeld voor de specifieke beheersmaatregelen om de werkzaamheden voor de IBF'ers te standaardiseren. Voor de generieke beheersmaatregelen zijn geen BIO-sjablonen ontwikkeld vanwege de veranderingen door de komst van de BIO2 en de lopende marktverkenning naar een nieuwe GRC-tool. De BIO-sjablonen zullen in de nieuwe GRC-tool worden geïntegreerd om de PDCA-cyclus te automatiseren voor de eerste lijn.

Topdesk wordt voor VB voorlopig als Proof-of-concept-product gebruikt en vormt een overzichtelijke manier om documenten en handelingen vast te leggen, zodat een bepaalde vindbaarheid van de onderliggende stukken wordt gewaarborgd. Volgens manager Opsporing dient Topdesk te worden gebruikt om de uitgevoerde acties van de ISO en de controlerende functionaris zichtbaar vast te leggen, voor

wat betreft de uitvoering van de controle op een BIO-maatregel. Ten slotte vormt Topdesk een middel om terugkerende activiteiten aan te maken.

Over het algemeen geldt dat de kwalitatieve vastlegging van onderbouwing en toelichting binnen het BIO-sjabloon en/of Topdeskregistratie voor VB (opzet, bestaan, werking en conclusie) een aandachtspunt is. Op dit moment is een BIO-sjabloon en/of Topdeskregistratie binnen VB geen zelfstandig leesbaar document.

(Zie § 2.4, § 3.3 en § 4.3 - Kwalitatieve vastlegging BIO-sjablonen/topdeskregistratie is een aandachtspunt)

Aanbeveling (Justid Opsporing)

- Draag er zorg voor de kwalitatieve vastlegging van de onderbouwde conclusie (incl. verwijzing naar beoordeelde documentatie en/of screenshots) in het BIO-sjabloon en/of Topdeskregistratie voor opzet, bestaan en werking.
- Draag er zorg dat het oordeel van de ISO zichtbaar in het BIO-sjabloon en/of Topdeskregistratie wordt vastgelegd.

Rapportage

Geen rapportage over de uitkomsten van de BIO-controles (per proces)

De manager Justid Opsporing geeft aan dat er geen rapportage plaatsvindt over bevindingen en te ondernemen acties met betrekking tot (niet) uitgevoerde BIO-maatregelen. De manager Justid Opsporing geeft aan dat dit wenselijk geacht wordt.

De manager Justid Opsporing geeft aan dat er geen aparte rapportage over de BIO-implementatie binnen Justid Opsporing aan Justid breed (zoals CISO, Privacyfunctionaris, MT/DT Justid) wordt gedaan.

De ISO van Justid Opsporing rapporteert aan de CISO Justid en binnen het IBF-overleg alleen op een kwantitatieve manier.

Daarnaast maakt de ISO van Justid Opsporing elke twee maanden – voorheen maandelijks – een voortgangsrapportage voor de directie van IBO. Dit betreft een aantal slides in een PowerPointpresentatie waar een aantal grafieken worden getoond en een kleine duiding vanuit de ISO wordt geboden op de getoonde grafieken. De voortgangsrapportage is kwantitatief (cijfers) van aard. De ISO levert dit document alleen aan en het wordt verder niet met hem besproken.

Aanbevelingen (Justid Opsporing)

- Draag zorg voor een kwalitatieve rapportage waaruit blijkt in hoeverre Justid Opsporing voldoet aan de beheersing van (beheer) activiteiten (BIO-

controles en overige beheersingsmaatregelen) gericht op onder andere: Governance, Contractmanagement, Incidentbeheer, Wijzigingenbeheer, Logische Toegangsbeveiliging, Beveiliging van IT-infrastructuur en data, Back-up, restore en uitwijk en Opschonen en vernietigen van data.

- Draag er voor zorg dat de rapportage wordt voorgelegd aan de belanghebbenden binnen Justid (zoals CISO, Privacyfunctionaris, MT/DT Justid).

Opzet documentatie

Procesbeschrijving over uitvoering BIO-controles vanuit Justid breed niet aangetroffen

Uit het document "VB - Interne Controleprotocol 2025" (datum ontbreekt, lijkt opgesteld maart 2025; niet geformaliseerd) kan niet opgemaakt worden hoe Justid Opsporing opzet, bestaan en werking invult. Het is niet duidelijk hoe er vanuit Justid breed wordt geïnstrueerd op de kwalitatieve invulling van de diepgang (opzet, bestaan en werking) van de BIO-controle, waaronder ook de wijze van vastlegging van de BIO-sjablonen en Topdeskregistraties.

In het Interne Controleprotocol 2025 ontbreekt een procesbeschrijving waaruit o.a. duidelijk wordt: wie doet wat en wanneer (verantwoordelijkheden); planning versus realisatie; controle aanpak; de wijze van vastlegging van resultaten; bespreken van de resultaten; rapporteren van de resultaten; en de overlegvormen.

De ISO heeft op 24 mei 2025 medegedeeld dat hij aan de hand van de BIO-sjablonen en/of Topdeskmeldingen de uitgevoerde BIO-controle inhoudelijk beoordeelt. Daarbij zoekt deze functionaris de onderliggende aangeleverde documentatie (audittrail) op en let op de status van het document (definitief of concept) en de datum (recent of verouderd).

Op basis hiervan worden in het dashboard ISO de conclusies voor opzet, bestaan en werking meegegeven, die bepalend zijn voor de kwantitatieve informatie over uitgevoerde BIO-controles. In de opzetdocumentatie "VB - Interne Controleprotocol 2025" ontbreekt een beschrijving van de activiteiten door de ISO. Een zichtbare beoordeling door de ISO op de uitgevoerde BIO-controles is niet aangetroffen op het BIO-sjabloon en/of in de topdeskmelding.

Aanbeveling (Cluster Beveiliging en Justid Opsporing)

- Stel een procedure beschrijving op en vast (formeel) die gericht is op de controle op de BIO-maatregelen en zorg voor de inrichting binnen Justid breed, zodat de uitvoering van de BIO-controles binnen Justid breed op een consistente wijze plaatsvindt.⁴

⁴ Onder het beoordelen van de opzet wordt verstaan de formele organisatie-opzet, zoals vastgelegd in organisatieschema's, beleidsdocumentatie, procesbeschrijvingen,

- In de procedure dient minimaal het volgende te zijn beschreven: verantwoordelijkheden binnen het controleproces, de wijze van plannen BIO-controles en de uitvoering ervan, op welke wijze de BIO-controles uitgevoerd moet worden (consistente werkwijze binnen alle organisatieonderdelen van Justid), hoe opzet, bestaan en werking geïnterpreteerd dienen te worden voor consistent uitvoering van de controle, de wijze van het bespreken en rapporteren van de bevindingen binnen Justid breed en Justid Opsporing.

procedurebeschrijvingen en handboeken. Voor het vaststellen van het bestaan gaat het om de aanwezigheid van een proces of controle volgens de opzet (bestaansmoment). Voor het toetsen van de werking gaat het om de daadwerkelijk uitvoering van het proces of controle gedurende een periode.

2 Bevindingen en aanbevelingen onderzoeksvraag 2 - "Wijzigingenbeheer"

In dit hoofdstuk zijn de bevindingen en aanbevelingen opgenomen die betrekking hebben op de onderzoeksvraag: "Welke bevindingen en aanbevelingen heeft de ADR over de uitgevoerde verbijzonderde controle door Justid Opsporing op het beheerproces "Wijzigingenbeheer" voor het VB over de periode 4^e kwartaal 2024 tot en met het 1^e kwartaal 2025?"

Voor de meest relevante bevindingen hebben wij een aanbeveling meegegeven.

Voor het beheerproces "Wijzigingenbeheer" is in de onderstaande tabel per norm aangegeven welke BIO-maatregelen van toepassing zijn. Deze BIO-maatregelen zijn afgeleid uit de Baseline Informatiebeveiliging Overheid (BIO) (versie 1.04) van 4 november 2019. Voor de uitvoering van de verbijzonderde controle op de BIO-maatregelen maakt Justid onderscheid tussen generieke BIO-maatregelen en specifieke BIO-maatregelen voor VB. De benoemde generieke BIO-maatregelen zijn ook relevant voor VB. Justid Opsporing heeft per BIO-maatregel aangegeven welke BIO maatregelen belegd zijn bij het Cluster Beveiliging van Justid (generiek) en Justid Opsporing (specifiek).

5 Wijzigingenbeheer (scope onderzoek VB bij Justid 2025)			
Nr	Beheersmaatregel	Belegd bij Justid Cluster Beveiliging Generieke BIO-maatregelen	Belegd bij Justid Opsporing Specifiek BIO-maatregelen
5.1	<i>In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan: (a) het administreren van wijzigingen; (b) risicoafweging van mogelijke gevolgen van de wijzigingen; (c) goedkeuringsprocedure voor wijzigingen.</i>	<i>12.1.2.1 Referentieontwerp VB: paragraaf 3.2.6</i>	<i>Justid Opsporing/IBO</i>
5.2	<i>Wijzigingen worden getest in een andere omgeving dan de productieomgeving. Bij het testen is aandacht voor de belangrijkste functionaliteiten en beveiliging. Testen worden voorbereid middels een</i>		<i>12.1.4 (12.1.4.1; 12.1.4.2) 14.2.3, 14.2.9 (14.2.9.1; 14.2.9.2), 14.3.1</i>

	<i>testplan. Testresultaten en evaluatie worden vastgesteld.</i>		
5.3	<i>Wijzigingen worden door de systeemeigenaar of product owner goedgekeurd op basis van gedocumenteerde testresultaten en pas daarna doorgevoerd in de productieomgeving.</i>	<i>12.1.2.1, 14.2.2 (14.2.2.1),</i>	<i>14.2.9 (14.2.9.1; 14.2.9.2</i>
5.4	<i>Er vindt periodiek controle plaats op wijzigingen aan het systeem VB, zodanig dat ongeautoriseerde wijzigingen wordenesignaleerd.</i>		<i>ADR⁵</i> <i><NB: 5.2. en 5.3 heeft betrekking op elk wijziging; 5.4 heeft betrekking op onafhankelijke controle ></i>

2.1 Bevindingen en aanbevelingen die betrekking hebben op beheersmaatregelen 5.1 en 5.3

Generieke BIO-maatregelen 12.1.2.1 en 14.2.2 uitgevoerd als specifiek, uitkomsten controle niet opgenomen in dashboard ISO

In het document "BIO controls ADR - Audit VB" d.d. 18 maart 2025 heeft het Cluster Beveiliging aangegeven dat de procedure voor wijzigingenbeheer aan het VB-systeem belegd is bij Justid Opsporing. BIO-maatregel 12.1.2.1 is als generiek aangemerkt, maar uitgevoerd op 25 maart 2025 als specifieke BIO-maatregel.

Daarnaast is de BIO-maatregel 14.2.2 als een generieke maatregel aangemerkt. Deze maatregel is als specifiek door Justid Opsporing VB opgepakt.

In het dashboard ISO d.d. 1 april 2025 ontbreekt een registratie van de uitkomsten van de uitgevoerde BIO-maatregelen 12.1.2.1 en 14.2.2.

(zie paragraaf 2.4 - Dashboard ISO Justid Opsporing (1 april 2025) toont niet de juiste werkelijkheid weer van geplande/uitgevoerde BIO-controles).

Aanbevelingen (Justid Opsporing)

- Draag er zorg voor dat de BIO-maatregelen 12.1.2.1 en 14.2.2 aangemerkt worden als specifiek zijnde en dat de kwantitatieve en kwalitatieve uitvoering van deze controles belegd zijn bij Justid Opsporing.
- Draag er zorg voor dat de uitkomsten van de controle op BIO-maatregelen 12.1.2.1 en 14.2.2 meegenomen worden in het dashboard ISO.

⁵ Relevante beheersmaatregel, toegevoegd door de ADR, niet af te leiden van de BIO

2.2 Bevindingen die betrekking hebben op beheersmaatregel 5.3

BIO-maatregel 14.2.2.1 is als een generieke maatregel belegd bij het Cluster Beveiliging. Uit het overzicht "18032025 – BIO controls ADR – audit VB" is niet vast te stellen wanneer de BIO-controle 14.2.2.1 daadwerkelijk is uitgevoerd, op basis waarvan de conclusie voor opzet, bestaan en werking zijn gebaseerd (inclusief onderbouwing/toelichting). In het dashboard ISO van 1 april 2025 worden alleen de kwantitatieve cijfers van de uitgevoerde controles van de specifieke BIO-maatregelen opgenomen.

Door CISO Justid is op 12 mei 2025 meegedeeld dat voor de generieke beheersmaatregelen er geen BIO-sjablonen ontwikkeld zijn vanwege veranderingen door de komst van de BIO 2.0 en de lopende marktverkenning naar een nieuwe GRC-tool. De standaard BIO-sjablonen heeft het Cluster Beveiliging met het beveiligingsteam ontwikkeld voor de specifieke beheersmaatregelen om de werkzaamheden voor de IBF'ers te standaardiseren. De BIO-sjablonen zullen in de nieuwe GRC-tool worden geïntegreerd om de PDCA-cyclus te automatiseren voor de eerste lijn.

(zie § 1.5 - BIO-sjablonen (Topdeskmeldingen))

2.3 Bevindingen en aanbeveling die betrekking hebben op beheersmaatregelen 5.2 en 5.3

Werking over het gehele controlejaar niet getoetst voor BIO-maatregelen 12.1.2.1, 14.2.3.0 en 14.2.9.1

Het toetsen van de werking voor de BIO-maatregelen 12.1.2.1, 14.2.3.0 en 14.2.9.1 heeft niet op de juiste wijze plaatsgevonden. De controle op deze BIO-maatregelen betreft een jaarcontrole. Een beperkt aantal samples is gecontroleerd uit het eerste kwartaal 2025. De werking over het gehele controlejaar is niet getoetst.

Uit interviews met Justid Opsporing en de vastlegging van de BIO-maatregelen blijkt dat voor Justid Opsporing niet duidelijk is hoe het toetsen van de werking geïnterpreteerd dient te worden.

Voor de uitgevoerde BIO-maatregel 14.2.3.0 (jaar-IC) van 19 november 2024 heeft de controle plaatsgevonden op de sprints 129, 130 en 131 (Q1-2025). Uit de controle is niet op te maken of er over een jaarperiode meerdere wijzigingen gericht op besturingsplatform voor VB hebben plaatsgevonden.

Voor de uitgevoerde BIO-maatregel 14.2.9.1 (jaar-IC) van 25 september 2024 is alleen een bestaansmoment (sprint 123) vastgesteld. De werking is niet getoetst. Er zijn over de betreffende controleperiode niet meer samples getrokken.

Voor de uitgevoerde BIO-maatregel 12.1.2.1 (jaar-IC) van 25 maart 2025 heeft de controle plaatsgevonden op de sprint 130 (Q1-2025). Uit de controle is niet op te maken of er over een jaarperiode meerdere wijzigingen zijn geweest, waaruit o.a. blijkt of de goedkeuring door Product Owner VB op basis van een testverslag heeft plaatsgevonden.

Product Owner heeft op 1 april 2024 meegedeeld dat er voor VB elke drie weken (sprint) wijzigingen hebben plaatsgevonden. Voor de controles op wijzigingenbeheer heeft de Product Owner aangegeven dat deze naar de laatste paar wijzigingen in het eerste kwartaal 2025 heeft gekeken en niet naar de wijzigingen over de hele controleperiode. Uitgaande van sprints van drie weken komt het aantal wijzigingen per jaar neer op ongeveer 17 releases (wijzigingen). Bij 17 releases per jaar kan volstaan worden dat verspreid over de controleperiode van een jaar 5 wijzigingen getoetst worden. Een overzicht van alle wijzigingen voor het VB over het controlejaar heeft ADR niet ontvangen.

Aanbeveling (Justid Opsporing)

- Draag er zorg voor dat bij het toetsen van de werking voor de BIO-maatregelen 12.1.2.1, 14.2.3.0 en 14.2.9.1 verspreid over de controleperiode voldoende steekproefposten worden getoetst.

2.4 Bevindingen en aanbevelingen die betrekking hebben op beheersmaatregelen 5.1 tot en met 5.3

Dashbord ISO Justid Opsporing (1 april 2025) toont niet de juiste werkelijkheid weer van geplande/uitgevoerde BIO-controles

Het dashboard van ISO Justid Opsporing van 1 april 2025 toont niet in alle gevallen een juiste weergave van de werkelijkheid.

Volgens het dashboard ISO blijkt:

De BIO-maatregel 12.1.2.1 is als generiek aangemerkt, maar uitgevoerd op 25 maart 2025 als specifieke BIO-maatregel. In het dashboard ISO ontbreekt een registratie van de uitkomsten van deze uitgevoerde BIO-maatregel.

Op basis van een niet aangereikte BIO-sjabloon voor de betreffende BIO-maatregelen (12.1.2.1, 12.1.4.1, 14.2.2.2, 14.2.3, 14.2.9.1, 14.2.9.2, 14.3.1) is in het dashboard ISO wel akkoord meegegeven voor opzet, bestaan en werking.

Volgens het dashboard ISO geldt voor BIO 12.1.4.2 dat het BIO-sjabloon is ingevuld en ingeleverd. Volgens het BIO-sjabloon is voor opzet, bestaan en werking akkoord gegeven. Weliswaar ontbreekt op het sjabloon een onderbouwing en toelichting van de gegeven conclusies.

De uitvoering van de BIO-controles 14.2.9.1, 14.2.9.2 en 14.3.1 is niet aangetroffen. Volgens dashboard ISO hadden deze controles rond 2 oktober 2024 dienen plaats te vinden.

BIO-maatregel 14.2.2 is als een generieke maatregel aangemerkt. Deze maatregel is als specifiek zijnde door Justid Opsporing VB opgepakt. De registratie van de uitgevoerde controle op BIO 14.2.2 (inclusief resultaten) ontbreekt in het dashboard ISO.

ADR mist een proactieve tijdige en kwalitatieve zichtbare monitoring van de realisatie van de tijdige en kwalitatieve uitvoering van de geplande BIO-controles. Justid Opsporing heeft hierop de volgende toelichting meegegeven:

- a) Per interview met de ISO op 24 april 2025 is meegedeeld dat de ISO de voortgang van uit te voeren controles met behulp van het dashboard ISO bewaakt.
- b) Per interview met de teamleider VB op 12 mei 2025 is meegedeeld dat per controle een verantwoordelijke functionaris wordt aangewezen. Deze functionaris is ook verantwoordelijk voor de uitvoer van de controle op de geïmplementeerde BIO-maatregel. Aangezien dit niet altijd goed gaat, wordt Topdesk gebruikt, omdat hier terugkerende activiteiten kunnen worden gemaakt, waardoor de terugkerende controles middels een toegekende activiteit door de functionaris moeten worden opgepakt. Alleen blijft de aangewezen functionaris wel verantwoordelijk voor het uitvoeren van de controle.

Voor de BIO-maatregelen die niet voorzien zijn van een BIO-sjabloon of een topdeskmelding heeft de ADR geen nadere analyse uitgevoerd.

Aanbevelingen (Justid Opsporing)

- Draag er zorg voor een strakkere monitoring op de tijdige uitvoering van de geplande BIO-controles.
- Draag er zorg voor dat de ISO de resultaten van de uitgevoerde BIO-controles beoordeelt en zijn bevindingen vastlegt op het BIO-sjabloon of in de topdeskregistratie (later: in het nieuwe GRC-tool).

Kwalitatieve vastlegging BIO-sjablonen/topdeskregistratie is een aandachtspunt

Voor de BIO-maatregelen 12.1.2.1, 12.1.4.1, 12.1.4.2, 14.2.2, 14.2.3 en 14.2.9.1 geldt dat het BIO-sjabloon en/of Topdeskregistratie in opzet, bestaan, werking en conclusie niet is voorzien van een onderbouwing/toelichting (kwalitatieve vastlegging).

Voor de BIO-maatregelen die niet voorzien zijn van een goede onderbouwing in het BIO-sjabloon of de topdeskmelding heeft de ADR geen nadere analyse uitgevoerd.

Aanbeveling (Justid Opsporing)

- Draag er zorg voor de kwalitatieve vastlegging van de onderbouwde conclusie (incl. verwijzing naar beoordeelde documentatie en/of

screenshots) in het BIO-sjabloon en/of Topdeskregistratie voor opzet, bestaan en werking.

Controles niet uitgevoerd door een onafhankelijke functionaris

De uitvoering van de controle op de BIO-maatregelen 12.1.2.1, 12.1.4.1, 12.1.4.2, 14.2.3.0, 14.2.9.1 en 14.2.9.2 heeft plaatsgevonden door een functionaris die zelf betrokken is in het proces. Er is sprake van geen onafhankelijke controle.

- De Product Owner VB heeft de controles op de BIO-maatregelen 12.1.2.1, 12.1.4.1, 12.1.4.2 en 14.2.3.0 uitgevoerd.
- DevOps beheerder (uit dienst) heeft de controles op de BIO-maatregelen 14.2.9.1 en 14.2.9.2 uitgevoerd op 25 september 2024 respectievelijk 5 mei 2024.

In het document "Controleprotocol BIO maatregelen VB: test op bestaan en werking 2025" is aangegeven dat de controle wordt afgetekend door Teamleider VB of Product Owner VB. Deze aftekening is niet aangetroffen op het BIO-sjabloon en/of topdeskregistratie voor:

- De controles op de BIO-maatregelen 12.1.2.1, 12.1.4.1, 12.1.4.2 en 14.2.3.0 door de teamleider VB;
- De controles op de BIO-maatregelen 14.2.9.1 en 14.2.9.2 door de teamleider VB of Product Owner.

In de Baseline Informatiebeveiliging Overheid (BIO) (versie 1.04) van 4 november 2019 is in § 2.7 "Rollen" aangegeven dat de BIO wel verplicht om de controls en overheidsmaatregelen die bij de rollen staan intern toe te delen en hierbij rekening te houden met voldoende functiescheiding.

Binnen primaire functiescheidingen wordt onderscheid gemaakt tussen beschikkende-, bewarende-, registrerende- en controlerende functie.

Het aantal functionarissen dat operationele werkzaamheden doet voor het VB is bij Justid Opsporing beperkt. Daarnaast is de ISO niet alleen betrokken voor het VB, maar ook voor andere informatiesystemen bij Justid Opsporing. De manager Justid Opsporing heeft aangegeven dat het wenselijk is om een Informatie Beveiligingsfunctionaris aan te trekken. Binnen Justid is geen gehoor gegeven aan het verzoek van de manager Justid Opsporing.

Aanbeveling (Justid Opsporing)

- Draag in eerste instantie zorg voor dat de uitvoering van de BIO-controles plaatsvindt door een functionaris die niet betrokken is bij het proces. Als blijkt dat dit gezien de organisatiegrootte voor het VB niet realiseerbaar is, bepaal aanvullende beheersingsmaatregelen. Hierbij kan gedacht worden aan de inhoudelijke beoordeling door de ISO op de uitgevoerde BIO-controles en dat deze functionaris zijn beoordeling vastlegt op het BIO-sjabloon of in de topdeskregistratie en dashboard ISO (later: in het nieuwe GRC-tool).

Zichtbare beoordeling ISO op BIO-sjablonen/topdeskregistratie niet aangetroffen

Een zichtbare beoordeling door de ISO op de uitgevoerde BIO-controles (12.1.2.1, 12.1.4.1, 12.1.4.2, 14.2.3.0, 14.2.9.1 en 14.2.9.2) is niet aangetroffen op het BIO-sjabloon en/of in de topdeskmelding.

De ISO heeft op 24 mei 2025 meegedeeld dat hij aan de hand van de BIO-sjablonen en/of Topdeskmeldingen de uitgevoerde BIO-controle inhoudelijk beoordeelt. Daarbij zoekt deze functionaris de onderliggende aangeleverde documentatie (audittrail) op en let daarbij op de status van het document (definitief of concept) en de datum (recent of verouderd).

Op basis hiervan worden in het dashboard ISO de conclusies voor opzet, bestaan en werking meegegeven, die bepalend zijn voor de kwantitatieve bestuurlijke informatie over uitgevoerde BIO-controles.

Aanbeveling (Justid Opsporing)

- Draag er zorg voor dat de ISO de resultaten van de uitgevoerde BIO-controles beoordeelt en zijn bevindingen vastlegt op het BIO-sjabloon of in de topdeskregistratie en dashboard ISO (later: in het nieuwe GRC-tool).

2.5 Bevindingen en aanbeveling die betrekking hebben op beheersmaatregel 5.4

Voor de norm 5.4 ontbreekt een beschrijving van de BIO-maatregel betrekking hebbende op de periodieke controle die plaatsvindt op wijzigingen aan het systeem VB, zodanig dat ongeautoriseerde wijzigingen worden gesignaleerd. Justid Opsporing heeft voor de beheersmaatregel 5.4 van het toetsingskader geen nadere invulling gegeven voor wat betreft planning/uitvoering van controles op het proces "Wijzigingenbeheer".

Voor het wijzigingenbeheer zijn buiten de benoemde BIO-maatregelen bij beheersmaatregel 5.1, 5.2 en 5.3 verder geen BIO-maatregelen benoemd in de Baseline Informatiebeveiliging Overheid (BIO) (versie 1.04) van 4 november 2019.

Voor het proces "Wijzigingenbeheer" kunnen wellicht ook andere beheersingsmaatregelen van belang zijn, waarvoor geen BIO-maatregelen geformuleerd zijn, om vast te stellen dat het proces goed of niet goed verloopt.

Aangezien het proces "Wijzigingenbeheer" niet volledig is geautomatiseerd en er handmatige handelingen aan het proces ten grondslag liggen, zal het wijzigingenbeheer als zodanig nog een onafhankelijke procescontrole nodig hebben, buiten de al ingerichte controles binnen het proces. Daarnaast kunnen er parameter wijzigingen (o.a. sessie management en SIEM-functionaliteiten (use-cases)), die

betrekking hebben op de goede werking van het systeem VB buiten de CI/CD pipeline om worden doorgevoerd, waardoor mogelijk van het proces “Wijzigingenbeheer” kan worden afgeweken.

Aanbeveling (Justid Opsporing)

Als wijzigingenbeheer niet effectief is, kan een wijziging kwetsbaarheden, fouten of ongewenste functionaliteiten aanbrengen in de productie omgeving die de werking van het VB of de integriteit van de data aantast.

- Draag er zorg voor een periodieke onafhankelijke controle op het proces “Wijzigingenbeheer” waarbij de onafhankelijke functionaris beoordeelt of
 - a) Wijzigingen volgens het proces zijn verlopen (functiescheiding, mandaat autoriseerder en goedkeurder, vastlegging (logging) en uitvoer tests);
 - b) Er wijzigingen zijn die buiten het proces om zijn doorgevoerd en daarom niet geregistreerd zijn, bijvoorbeeld door logreview;
 - c) De gebruikte populatie voor de controles volledig en juist is;
 - d) Correctieve acties door de organisatie zijn ondernomen indien er naar aanleiding van de periodieke controle oneigenlijke wijzigingen zijnesignaleerd.

Wellicht kan deze controle samengevoegd worden met de controles op BIO-maatregelen benoemd bij beheersingsmaatregelen 5.1, 5.2 en 5.3.

3 Bevindingen en aanbevelingen onderzoeksvraag 3 - “Logische Toegangsbeveiliging”

In dit hoofdstuk zijn de bevindingen en aanbevelingen opgenomen die betrekking hebben op de onderzoeksvraag: “Welke bevindingen en aanbevelingen heeft de ADR over de uitgevoerde verbijzonderde controle door Justid Opsporing op het beheerproces “Logische toegangsbeveiliging” voor het VB over de periode 4^e kwartaal 2024 tot en met het 1^e kwartaal 2025?”

Voor de meest relevante bevindingen hebben wij een aanbeveling meegegeven.

Voor het beheerproces “Logische Toegangsbeveiliging” is in de onderstaande tabel per norm aangegeven welke BIO-maatregelen van toepassing zijn. Deze BIO-maatregelen zijn afgeleid uit de Baseline Informatiebeveiliging Overheid (BIO) (versie 1.04) van 4 november 2019. Voor de uitvoering van de verbijzonderde controle op de BIO-maatregelen maakt Justid onderscheid tussen generieke BIO-maatregelen en specifieke BIO-maatregelen voor VB. De benoemde generieke BIO-maatregelen zijn ook relevant voor VB. Justid Opsporing heeft per BIO-maatregel aangegeven welke BIO maatregelen belegd zijn bij het Cluster Beveiliging van Justid (generiek) en Justid Opsporing (specifiek).

6 Logische toegangsbeveiliging (scope onderzoek VB bij Justid 2025)			
Nr	Beheersmaatregel	Belegd bij Justid Cluster Beveiliging	Belegd bij Justid Opsporing
		Generieke BIO-maatregelen	Specifiek BIO-maatregelen
6.1	<i>Er is een beleid (uitgewerkt in procedures) voor toegang met waarin o.a. het volgende is uitgewerkt:</i> <i>- het logische toegangspad van gebruikers/beheerders;</i> <i>- uitgegeven van speciale bevoegdheden;</i> <i>- autorisatiematrix waarin wordt beschreven welke functies welke rollen / autorisatierechten behoren te krijgen;</i> <i>- het proces toekennen/wijzigen/verwijderen</i>	9.1.1	9.2.1.1, 9.4 (raakvlakken met 9.4.1.1, 9.4.1.2, 9.4.2.1, 9.4.2.2, 9.4.3.1, 9.4.3.2, 9.4.3.3, 9.4.3.4, 9.4.3.5),

	van gebruikers- / beheerdersaccounts (inclusief rechten; - twee-factor authenticatie; - thuiswerken; - eisen van wachtwoordinstellingen (lengte, geldigheidsduur, complexiteit, versleuteling etc.); - Beheer van toegang van externe partijen; - omgaan met groepsaccounts; - periodieke controle op accounts en toegangsrechten.		
6.2	Het verlenen en muteren van accounts en toegangsrechten vindt plaats na goedkeuring door een bevoegde functionaris. Er is een actueel overzicht (mandaatregister) aanwezig waaruit blijkt welke personen beslissende bevoegdheden hebben voor het verlenen van een bepaald type (niveau) toegangsrechten / functieprofielen. Er bestaat functiescheiding tussen het aanvragen, autoriseren en doorvoeren van wijzigingen in accounts en toegangsrechten.		9.2.2, 9.2.2.1, 9.2.2.3
6.3	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd en bij wijzigingen behoren ze te worden aangepast.		9.2.6
6.4	Alle uitgegeven toegangsrechten worden periodiek geëvalueerd. Dit interval is beschreven in het toegangsbeleid en is bepaald op basis van het risiconiveau. De uitkomsten van de evaluatie en de opvolging daarvan worden vastgelegd.		9.2.5.3 (Overige bevoegdheden ieder halfjaar), 9.2.3.1 (interval speciale bevoegdheden ieder kwartaal)
6.5	Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen. Dit conform het beleid voor toegang.		9.4.3: (9.4.3.1, 9.4.3.2, 9.4.3.3, 9.4.3.4, 9.4.3.5)

6.6	<i>Wachtwoorden worden versleuteld opgeslagen (niet in de originele vorm, in leesbare tekst) NB: BIO-maatregel ontbreekt, niet opgenomen in de BIO. Vaststellen bij Justid Opsporing</i>	ADR	ADR
6.7	<i>Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.</i>		9.4.2.1
6.8	<i>Accounts zijn altijd persoonsgebonden zodat handelingen altijd te herleiden zijn naar één verantwoordelijke.</i>		9.2.1.2

3.1 Bevindingen en aanbevelingen die betrekking hebben op beheersmaatregel 6.1

BIO-controles 9.4.3.1, 9.4.3.2 en 9.4.3.3 niet aangetroffen

Voor BIO-maatregelen 9.4.3.1, 9.4.3.2 en 9.4.3.3 is geen BIO-sjabloon en/of Topdeskregistratie aangereikt. Voor deze BIO-maatregelen heeft de ADR het BIO-sjabloon van de BIO-maatregel 9.4.2.1 ontvangen. Het is op basis van het BIO-sjabloon van 9.4.2.1 niet duidelijk hoe de BIO-maatregelen 9.4.3.1, 9.4.3.2, 9.4.3.3 worden afgedekt. ADR mist een proactieve tijdige en kwalitatieve zichtbare monitoring van de realisatie van de tijdige en kwalitatieve uitvoering van de geplande BIO-controles. (Zie § 3.3 "Dashboard ISO Justid Opsporing (1 april 2025) toont niet de juiste werkelijkheid weer van geplande/uitgevoerde BIO-controles" en § 3.5 "Zichtbare beoordeling ISO op BIO-sjablonen/topdeskregistratie niet aangetroffen")

Aanbevelingen (Justid Opsporing)

- Draag zorg voor een strakkere monitoring op de tijdige uitvoering van de geplande BIO-controles.
- Draag er zorg voor dat de ISO de resultaten van de uitgevoerde BIO-controles beoordeelt en zijn bevindingen vastlegt op het BIO-sjabloon of in de topdeskregistratie en dashboard ISO (later: in de nieuwe GRC-tool).

Zichtbare beoordeling ISO op BIO-sjablonen/topdeskregistratie niet aangetroffen

Herzien frequentie evaluatie Logische Toegangsbeleid

Cluster Beveiliging heeft op 18 maart 2025 het document "BIO controls ADR" d.d. 18 maart 2025 aangereikt en voor de generieke BIO-maatregel BIO 9.1.1 aangeven dat het Logisch Toegangsbeleid (vastgesteld 1 maart 2023) minimaal 1x in de drie jaar wordt herzien. ADR is van mening dat gezien de veranderingen in de nieuwe

wetgevingen (o.a. Cyberbeveiligingswet, inclusief kader BIO 2.0) en externe spanningen (lokale en internationale cyberbedreiging) het Logisch Toegangsbeveiligingsbeleid net als het Integraal Beveiligingsbeleid ieder jaar moeten worden geëvalueerd in plaats van minimaal 1x per drie jaar. De CISO heeft meegedeeld dat voor de generieke beheersmaatregelen geen BIO-sjablonen zijn ontwikkeld vanwege veranderingen door de komst van de BIO2 en de lopende marktverkenning naar een nieuwe GRC-tool (zie § 1.7 "BIO-sjablonen (Topdeskregistratie)").

Aanbevelingen (Cluster Beveiliging)

- Draag er zorg voor dat het Logisch Toegangsbeleid jaarlijks wordt herzien en formeel vastgesteld.
- Draag er zorg voor dat de eerste lijn (o.a. Justid Opsporing) tijdig over het hernieuwd Logisch Toegangsbeleid wordt geïnformeerd, zodat de eerste lijn op basis van dit beleid zorg kan dragen voor aanpassingen van de inrichting van hun informatiesystemen (zoals Justid Opsporing voor het VB).

3.2 Bevinding en aanbevelingen die betrekking hebben op beheersmaatregel 6.6

Controle op de versleuteling van wachtwoorden niet beschreven

Voor de norm 6.6 van het toetsingskader ontbreekt in de BIO versie 1.04zv d.d. 17 juni 2020 een beschrijving van een BIO-maatregel die betrekking heeft op de versleuteling van wachtwoorden. Onder BIO-maatregel 9.4.3 "Systeem voor wachtwoordbeheer" is geen maatregel opgenomen over de versleuteling van wachtwoorden.

Justid Opsporing heeft voor de norm 6.6 geen controlemaatregel gepland c.q. uitgevoerd. Echter zien wij wel onder de bewijslast van BIO-maatregel 9.4.3.5 bij norm 6.1 en norm 6.5 dat er van wachtwoordversleuteling sprake is.

Voor wachtwoordversleuteling zijn de volgende documenten op 1 april 2025 aangereikt:

1. Screenshot "ww versleutelds" d.d. 24 maart 2025: aangetoond wachtwoordinstelling voor versleuteling op databaseniveau is ingesteld
2. Screenshot "Password Policy" d.d. 27 maart 2025: wachtwoordversleuteling is ingeregeld.

Aanbevelingen (Cluster Beveiliging en Justid Opsporing)

- Formuleer een specifieke controle op de versleuteling van wachtwoorden die is afgeleid uit de BIO2.0 (maatregel 2.0.8.2.09). De sterkte van de cryptografie wordt gebaseerd op de actuele adviezen van het NCSC en de Unit Weerbaarheid van de AIVD.

- Draag er zorg voor dat deze controle in de jaarlijkse planning van uit te voeren BIO-controles wordt opgenomen en wordt uitgevoerd volgens de planning.

3.3 **Bevindingen en aanbevelingen die betrekking hebben op beheersmaatregelen 6.1 tot en met 6.8**

Dashboard ISO Justid Opsporing (1 april 2025) toont niet de juiste werkelijkheid weer van geplande/uitgevoerde BIO-controles

Het dashboard van ISO Justid Opsporing van 1 april 2025 toont niet in alle gevallen een juiste weergave van de werkelijkheid.

Volgens het dashboard ISO blijkt dat:

Op basis van een niet aangereikt BIO-formulier (of topdeskregistratie) voor de betreffende BIO-maatregelen is in het dashboard ISO bij opzet, bestaan en werking akkoord meegegeven. Dit geldt voor: 9.2.1.1, 9.2.1.2, 9.2.2, 9.2.2.1, 9.2.3.1, 9.2.5.3, 9.2.6, 9.4.1.1, 9.4.1.2, 9.4.2.1, 9.4.2.2, 9.4.3.1, 9.4.3.3, 9.4.3.4, 9.4.3.5.

De uitvoering van de BIO-controles 9.4.1.1, 9.4.1.2, 9.4.2.2, 9.4.3.4 en 9.4.3.5 is niet aangetroffen.

- Volgens dashboard ISO is aangegeven dat de controles 9.4.1.1, 9.4.1.2 en 9.4.3.4 op zijn laatst is uitgevoerd op 13 november 2023.
- Volgens dashboard ISO staat de BIO-controle 9.2.1.2 vier keer per jaar gepland, waarvan de laatste controle op 18 september 2023 is uitgevoerd.
- Voor de controles 9.4.2.2 en 9.4.3.5 is in het dashboard aangegeven dat de laatste controledatum 19 november 2024 is geweest.

Voor BIO-maatregelen 9.4.3.1, 9.4.3.2 en 9.4.3.3. is geen BIO-sjabloon en/of Topdeskregistratie aangereikt. Voor deze BIO-maatregelen heeft de ADR het BIO-sjabloon van BIO-maatregelen 9.4.2.1 ontvangen. Het is op basis van het BIO-sjabloon van 9.4.2.1 niet duidelijk hoe de BIO-maatregelen 9.4.3.1, 9.4.3.2, 9.4.3.3 worden afgedekt.

Voor BIO-maatregel 9.2.1.2 is geen BIO-sjabloon en/of Topdeskregistratie aangereikt.

Voor BIO-maatregelen 9.2.2, 9.2.2.1, 9.2.2.3 en 9.2.6 zijn geen uitgevoerde controles (BIO-sjablonen en/of topdeskmeldingen) aangereikt. Volgens het dashboard ISO is de laatste controle voor BIO-maatregelen 9.2.2.3 en 9.2.6 uitgevoerd op 25 maart 2025 respectievelijk 27 oktober 2023.

Volgens de planning in het dashboard ISO wordt BIO-controle 9.2.3.1 één keer per jaar uitgevoerd. Echter in het dashboard is er geen laatste controle datum

ingevoerd, waardoor niet vast te stellen is of de controle in de controleperiode is uitgevoerd. Het lijkt erop dat de controle nooit is uitgevoerd.

ADR mist een proactieve tijdige en kwalitatieve zichtbare monitoring van de realisatie van de tijdige en kwalitatieve uitvoering van de geplande BIO-controles. Justid Opsporing heeft hierop de volgende toelichting meegegeven:

- a) Per interview met de ISO op 24 april 2025 is meegedeeld dat de ISO de voortgang van uit te voeren controles met behulp van het dashboard ISO bewaakt.
- b) Per interview met de teamleider VB op 12 mei 2025 is meegedeeld dat per controle een verantwoordelijke functionaris wordt aangewezen. Deze functionaris is ook verantwoordelijk voor de uitvoer van de controle op de geïmplementeerde BIO-maatregel. Aangezien dit niet altijd goed gaat, wordt Topdesk gebruikt, omdat hier terugkerende activiteiten kunnen worden gemaakt, waardoor de terugkerende controles middels een toegekende activiteit door de functionaris moeten worden opgepakt. Alleen blijft de aangewezen functionaris wel verantwoordelijk voor het uitvoeren van de controle.

Voor de BIO-maatregelen die niet voorzien zijn van een BIO-sjabloon of een topdeskmelding heeft de ADR geen nadere analyse uitgevoerd.

Aanbevelingen (Justid Opsporing)

- Draag er zorg voor een strakkere monitoring op de tijdige uitvoering van de geplande BIO-controles.
- Draag er zorg voor dat de ISO de resultaten van de uitgevoerde BIO-controles beoordeelt en zijn bevindingen vastlegt op het BIO-sjabloon of in de topdeskregistratie (later: in de nieuwe GRC-tool).

Kwalitatieve vastlegging BIO-sjablonen/topdeskregistratie is een aandachtspunt

Voor BIO-maatregelen 9.2.1.1, 9.4.2.1, 9.2.3.1, 9.2.5.3 geldt dat het BIO-sjabloon en/of Topdeskregistratie in opzet, bestaan, werking en conclusie niet is voorzien van een onderbouwing/toelichting (kwalitatieve vastlegging).

Voor de BIO-maatregelen die niet voorzien zijn van een goede onderbouwing in het BIO-sjabloon of de topdeskmelding heeft de ADR geen nadere analyse uitgevoerd.

Aanbeveling (Justid Opsporing)

- Draag er zorg voor de kwalitatieve vastlegging van de onderbouwde conclusie (incl. verwijzing naar beoordeelde documentatie en/of screenshots) in het BIO-sjabloon en/of Topdeskregistratie voor opzet, bestaan en werking.

Controles niet uitgevoerd door een onafhankelijke functionaris

De uitvoering van de BIO-maatregelen 9.2.1.1, 9.2.3.1 en 9.4.2.1 heeft plaatsgevonden door een functionaris (DevOps beheerder) die zelf betrokken is in het proces. Er is geen sprake van een onafhankelijke controle.

- De DevOps beheerder (uit dienst) heeft de controles BIO 9.2.1.1 en 9.4.2.1 uitgevoerd op 27 maart 2025 respectievelijk 4 november 2024.
- Voor BIO 9.2.3.1 is er geen BIO-sjabloon en/of Topdeskregistratie aangereikt. Wel is er een Exceloverzicht "autorisatiematrix" aangereikt. Uit het Exceloverzicht ontbreekt de onderbouwing/toelichting en conclusie waaruit blijkt dat voldaan wordt aan de BIO-maatregel 9.2.3.1. De DevOps beheerder (uit dienst) lijkt volgens het Excel-overzicht "Autorisatiematrix" de controle BIO 9.2.3.1 te hebben uitgevoerd.
- Voor BIO 9.2.5.3 is er geen BIO-sjabloon aangereikt, maar wel een topdeskregistratie. De DevOps beheerder (uit dienst) heeft de controle uitgevoerd op 10 februari 2025. Uit de topdeskregistratie ontbreekt de onderbouwing/toelichting en conclusie waaruit blijkt dat voldaan wordt aan de BIO-maatregel 9.2.5.3. Deze controle is afgetekend door Product Owner VB.

In het document "Controleprotocol BIO maatregelen VB: test op bestaan en werking 2025" is aangegeven dat de controle wordt afgetekend door Teamleider VB of Product Owner VB. Deze aftekening is niet aangetroffen op het BIO-sjabloon en/of topdeskregistratie voor de BIO-maatregelen 9.2.1.1, 9.4.2.1, en 9.2.3.1.

In de Baseline Informatiebeveiliging Overheid (BIO) (versie 1.04) van 4 november 2019 is in § 2.7 "Rollen" aangegeven dat de BIO wel verplicht om de controls en overheidsmaatregelen die bij de rollen staan intern toe te delen en hierbij rekening te houden met voldoende functiescheiding.

Binnen primaire functiescheidingen wordt onderscheid gemaakt tussen beschikkende-, bewarende-, registrerende- en controlerende functie.

Het aantal functionarissen dat operationele werkzaamheden doet voor het VB is bij Justid Opsporing beperkt. Daarnaast is de ISO niet alleen betrokken voor het VB, maar ook voor andere informatiesystemen. De manager Justid Opsporing heeft aangegeven dat het wenselijk is om een Informatie Beveiligingsfunctionaris aan te trekken. Binnen Justid is geen gehoor gegeven aan het verzoek van de manager Justid Opsporing.

Aanbeveling (Justid Opsporing)

- Draag in eerste instantie zorg voor dat de uitvoering van de BIO-controles plaatsvindt door een functionaris die niet betrokken is bij het proces. Als

blijkt dat dit gezien de organisatiegrootte voor het VB niet realiseerbaar is, bepaal aanvullende beheersingsmaatregelen. Hierbij kan gedacht worden aan de inhoudelijke beoordeling door de ISO op de uitgevoerde BIO-controles en dat deze functionaris zijn beoordeling vastlegt op het BIO-sjabloon of in de topdeskregistratie en dashboard ISO (later: in de nieuwe GRC-tool).

3.5 Bevinding en aanbeveling die betrekking hebben op beheersmaatregelen 6.1, 6.4 en 6.8

Zichtbare beoordeling ISO op BIO-sjablonen/topdeskregistratie niet aangetroffen

Een zichtbare beoordeling door de ISO op de uitgevoerde BIO-controles (9.2.1.1, 9.2.5.3 en 9.4.2.1) is niet aangetroffen op het BIO-sjabloon en/of in de topdeskmelding.

De ISO heeft op 24 mei 2025 meegedeeld dat hij aan de hand van de BIO-sjablonen en/of Topdeskmeldingen de uitgevoerde BIO-controle inhoudelijk beoordeelt. Daarbij zoekt deze functionaris de onderliggende aangeleverde documentatie (audittrail) op en let daarbij op de status van het document (definitief of concept) en de datum (recent of verouderd).

Op basis hiervan worden in het dashboard ISO de conclusies voor opzet, bestaan en werking meegeven, die bepalend zijn voor de kwantitatieve bestuurlijke informatie over uitgevoerde BIO-controles.

Aanbeveling (Justid Opsporing)

- Draag er zorg voor dat de ISO de resultaten van de uitgevoerde BIO-controles beoordeelt en zijn bevindingen vastlegt op het BIO-sjabloon of in de topdeskregistratie en dashboard ISO (later: in de nieuwe GRC-tool).

4 Bevindingen en aanbevelingen

onderzoeksvraag 4 - "Back-up, restore en uitwijk"

In dit hoofdstuk zijn de bevindingen en aanbevelingen opgenomen die betrekking hebben op de onderzoeksvraag: "Welke bevindingen en aanbevelingen heeft de ADR over de uitgevoerde verbijzonderde controle door Justid Opsporing op het beheerproces "Back-up, restore en uitwijk" voor het VB over de periode 4^e kwartaal 2024 tot en met het 1^e kwartaal 2025?"

Voor de meest relevante bevindingen hebben wij een aanbeveling meegegeven.

Voor het beheerproces "Back-up, restore en uitwijk" is in de onderstaande tabel per norm aangegeven welke BIO-maatregelen van toepassing zijn. Deze BIO-maatregelen zijn afgeleid uit de Baseline Informatiebeveiliging Overheid (BIO) (versie 1.04) van 4 november 2019. Voor de uitvoering van de verbijzonderde controle op de BIO-maatregelen maakt Justid onderscheid tussen generieke BIO-maatregelen en specifieke BIO-maatregelen voor VB. De benoemde generieke BIO-maatregelen zijn ook relevant voor VB. Justid Opsporing heeft per BIO-maatregel aangegeven welke BIO maatregelen belegd zijn bij het Cluster Beveiliging van Justid (generiek) en Justid Opsporing (specifiek).

9 Back-up, restore en uitwijk (scope onderzoek VB bij Justid 2025)			
Nr	Beheersmaatregel	Belegd bij Justid Cluster Beveiliging	Belegd bij Justid Opsporing
		Generieke BIO-maatregelen	Specifieke BIO-maatregelen
9.1	<i>Er is een back-upbeleid waarin de eisen voor het bewaren en beschermen van gegevens zijn gedefinieerd en vastgesteld.</i>	12.3.1.1, 12.3.1.3	12.3.1.2;
9.2	<i>Het back-upproces voorziet in opslag van de back-up op een op dusdanige afstand van de bron dat een mogelijke calamiteit bij de bron geen effect heeft op de back-up.</i>	12.3.1.4	
9.3	<i>De restore procedure (terugzetten van een back-up) wordt minimaal jaarlijks getest en na een grote wijziging.</i>		12.3.1.5
9.4	<i>Uitwijkvoorzieningen worden jaarlijks getest.</i>		17.1.3.1

4.1 Bevindingen en aanbevelingen die betrekking hebben op beheersmaatregel 9.1 en 9.2

Generieke BIO-maatregelen 12.3.1.1, 12.3.1.3 en 12.3.1.4 uitgevoerd als specifiek, uitkomsten controles niet opgenomen in dashboard ISO

De BIO-maatregelen 12.3.1.1 en 12.3.1.3 zijn als generiek aangemerkt, maar deze zijn als specifieke maatregelen uitgevoerd door DevOps engineer VB. Een registratie van de uitgevoerde BIO-maatregelen (conclusies opzet, bestaan en werking) ontbreekt in het dashboard. Volgens de BIO-sjablonen betreft het een jaarcontrole die is uitgevoerd op 25 maart 2025. De BIO-controles 12.3.1.1 en 12.3.1.3 dienen voor VB als specifiek te worden aangemerkt i.p.v. generiek.

De BIO-maatregel 12.3.1.4 heeft betrekking op het proces back-up dat voor VB voorziet in opslag van de back-up op een op dusdanige afstand van de bron dat een mogelijke calamiteit bij de bron geen effect heeft op de back-up. In het Exceloverzicht "BIO controls ADR" d.d. 18 maart 2025 is door Cluster Beveiliging aangegeven dat BIO 12.3.1.4 uitgevoerd dient te worden door Justid Opsporing. Deze controle dient voor VB als specifiek te worden aangemerkt i.p.v. generiek. ADR heeft van Justid Opsporing voor BIO-maatregel 12.3.1.4 een leeg BIO-sjabloon (template) ontvangen. Daarentegen is een Topdeskmelding gemaakt, waarin het lijkt dat de controle op 25 maart 2025 is uitgevoerd en dat deze controle als specifieke maatregel is beschouwd. In de topdeskregistratie ontbreken een toelichting/onderbouwing en de conclusies van de uitgevoerde controle ontbreekt. In het dashboard ISO ontbreekt een registratie van deze uitgevoerde BIO-maatregel.

Aanbevelingen (Justid Opsporing)

- Draag er zorg voor dat de BIO-maatregelen 12.3.1.1, 12.3.1.3 en 12.3.1.4 aangemerkt worden als specifiek zijnde en dat de kwantitatieve en kwalitatieve uitvoering van de controles belegd zijn bij Justid Opsporing.
- Draag er zorg voor dat de uitkomsten van de controle op BIO-maatregelen 12.3.1.1, 12.3.1.3 en 12.3.1.4 meegenomen worden in het dashboard ISO.

4.2 Bevindingen en aanbeveling die betrekking hebben op beheersmaatregel 9.4

Kwalitatieve vastlegging testresultaten is een aandachtspunt

In de BIO-maatregel 17.1.3.1 wordt in de Topdeskmelding door de DevOps beheerder (uit dienst) verwezen naar een uitwijktest verslag en dat deze is goedgekeurd door Teamleider VB.

De uitwijktest heeft in januari/februari 2025 plaatsgevonden. Justid Opsporing heeft als audittrail de volgende documenten aangereikt:

1. "20250114 Verslag inwijk naar primaire verwerkingslocatie_def" (akkoord Teamleider VB op 3 februari 2025, uitgevoerde controle op 14 januari 2025)
2. "20250114 Verslag restore vanaf back-up disk naar uitwijk_def"
3. "20250114 Verslag restore vanaf back-up tape naar uitwijk_def"

ADR en de geïnterviewde DevOps engineer hebben vastgesteld dat

- In de vastlegging van de verschillende testen conclusies ontbreken;
- In de vastlegging van de uitgevoerde testen (documenten 1 en 3) in 2025 in een aantal gevallen dezelfde screenshots met dezelfde datum is gehanteerd als in de screenshots bij de uitwijktest in maart 2024. Het lijkt erop dat de screenshots uit het verslag van 2024 gebruikt zijn om het verslag van 2025 op te vullen.
- In de verslaglegging van de uitgevoerde test (document 3) niet volledig is. Er ontbreekt een aantal screenshots zoals bijvoorbeeld: punt 7 "Catalogiseren voltooid", punt 8 "Encrypted Back-up tape zichtbaar", punt 11 "Decryptie is succesvol".

Aanbeveling (Justid Opsporing)

- Draag zorg voor een juiste en volledige vastlegging van de screenshots in het testverslag en dat deze betrekking hebben op de actuele uitgevoerde testdatum.

4.3 Bevindingen en aanbevelingen die betrekking hebben op beheersmaatregel 9.1 tot en met 9.4

Dashboard ISO Justid Opsporing (1 april 2025) toont niet de juiste werkelijkheid weer van geplande/uitgevoerde BIO-controles

Het dashboard van ISO Justid Opsporing van 1 april 2025 toont niet in alle gevallen een juiste weergave van de werkelijkheid.

Volgens dat dashboard blijkt dat:

De BIO-maatregelen 12.3.1.1 en 12.3.1.3 zijn als generiek aangemerkt, maar deze zijn als specifieke maatregelen uitgevoerd door DevOps engineer VB (uit dienst). Een registratie van deze uitgevoerde BIO-maatregelen (conclusies opzet, bestaan en werking) ontbreekt in het dashboard. Volgens de BIO-sjablonen betreft het een jaarcontroles die zijn uitgevoerd op 25 maart 2025.

Voor BIO-maatregel 12.3.1.2 (uitgevoerd op 19 november 2024) zijn de geregistreerde conclusies (opzet, bestaan en werking) juist overgenomen van het BIO-sjabloon in het dashboard ISO.

ADR heeft van Justid Opsporing voor BIO-maatregel 12.3.1.4 een leeg BIO-sjabloon (template) ontvangen. Daarentegen is een Topdeskmelding gemaakt, waarin lijkt dat de controle op 25 maart 2025 is uitgevoerd en dat deze controle als specifieke maatregel is beschouwd. In de Topdeskregistratie ontbreken een toelichting/onderbouwing en de conclusies van de uitgevoerde controle ontbreekt. In het dashboard ISO ontbreekt een registratie van deze uitgevoerde BIO-maatregel

Het dashboard ISO toont voor de BIO-maatregel 12.3.1.5 aan dat de opzet, bestaan en werking als effectief is aangegeven, terwijl volgens dashboard het BIO-sjabloon niet is ingevuld/ingeleverd. De controle is uitgevoerd op 19 november 2024. Het BIO-sjabloon en/of Topdeskregistratie wordt in opzet, bestaan, werking niet voorzien van een onderbouwing/toelichting. Wel is in het BIO-sjabloon bij de conclusie voor opzet, bestaan en werking aangegeven dat deze effectief is.

Het dashboard ISO toont voor BIO 17.1.3.1 aan dat de opzet, bestaan en werking als effectief is aangegeven, terwijl het BIO-sjabloon niet is ingevuld/ingeleverd. De controle is uitgevoerd op 7 februari 2025. Alleen voor de werking is een Topdeskregistratie aangemaakt. In deze registratie ontbreekt een onderbouwing en de conclusie.

(zie § 4.3 - Kwalitatieve vastlegging BIO-sjablonen/Topdeskregistratie is een aandachtspunt).

Aanbeveling (Justid Opsporing)

- Draag er zorg voor dat de ISO de resultaten van de uitgevoerde BIO-controles beoordeelt en zijn bevindingen vastlegt op het BIO-sjabloon of in de Topdeskregistratie (later: in de nieuwe GRC-tool).

Kwalitatieve vastlegging BIO-sjablonen/topdeskregistratie is een aandachtspunt

Voor BIO-maatregelen 12.3.1.1, 12.3.1.2, 12.3.1.3, 12.3.1.5 en 17.1.3.1 geldt dat het BIO-sjabloon en/of Topdeskregistratie in opzet, bestaan, werking en conclusie niet is voorzien van een onderbouwing/toelichting (kwalitatieve vastlegging).

Voor BIO 17.1.3.1 is er geen BIO-sjabloon aangereikt. Wel is er voor deze BIO-maatregel een Topdeskmelding gemaakt. In de acties van de DevOps beheerder (uit dienst) wordt verwezen naar een uitwijktest verslag en dat deze is goedgekeurd door de Teamleider VB. De uitkomsten van de uitwijktesten (onderbouwing/toelichting en conclusie) zijn niet opgenomen in de Topdeskregistratie. In de Topdeskregistratie heeft de Teamleider VB op 20 maart 2025 de uitgevoerde taak voor gezien aangemerkt.

Voor de BIO-maatregelen die niet voorzien zijn van een goede onderbouwing in het BIO-sjabloon of de topdeskmelding heeft de ADR geen nadere analyse uitgevoerd.

Aanbeveling (Justid Opsporing)

- Draag zorg voor de kwalitatieve vastlegging van de onderbouwde conclusie (incl. verwijzing naar beoordeelde documentatie en/of screenshots) in het BIO-sjabloon en/of Topdeskregistratie voor opzet, bestaan en werking.

Controles niet uitgevoerd door een onafhankelijke functionaris

De DevOps beheerder (uit dienst) heeft de controles op BIO-maatregelen 12.3.1.1 (25 maart 2025), 12.3.1.2 (19 november 2024) en 12.3.1.3 (25 maart 2025) en 12.3.1.5 (19 november 2024) uitgevoerd. Deze functionaris is zelf betrokken bij het proces. Er is geen sprake van een onafhankelijke controle. In het document "Controleprotocol BIO maatregelen VB: test op bestaan en werking 2025" is aangegeven dat de controle wordt afgetekend door Teamleider VB of Product Owner VB. Deze aftekening is niet aangetroffen op het BIO-sjabloon en/of Topdeskregistratie.

Ondanks dat in de Topdeskmelding een korte beschrijving van de uitkomsten van de uitwijktesten (onderbouwing/toelichting en conclusie) ontbreekt heeft de teamleider VB op 20 maart 2025 de uitgevoerde taak voor gezien aangemerkt.

In de Baseline Informatiebeveiliging Overheid (BIO) (versie 1.04) van 4 november 2019 is in § 2.7 "Rollen" aangegeven dat de BIO wel verplicht om de controls en overheidsmaatregelen die bij de rollen staan intern toe te delen en hierbij rekening te houden met voldoende functiescheiding.

Binnen primaire functiescheidingen wordt onderscheid gemaakt tussen beschikkende-, bewarende-, registrerende- en controlerende functie.

Het aantal functionarissen dat operationele werkzaamheden doet voor het VB is bij Justid Opsporing beperkt. Daarnaast is de ISO niet alleen betrokken voor het VB, maar ook voor andere informatiesystemen. De manager Justid Opsporing heeft aangegeven dat het wenselijk is om een Informatie Beveiligingsfunctionaris aan te trekken. Binnen Justid is geen gehoor gegeven aan het verzoek van de manager Justid Opsporing.

Aanbeveling (Justid Opsporing)

- Draag in eerste instantie zorg dat de uitvoering van de BIO-controles plaatsvindt door een functionaris die niet betrokken is bij het proces. Als blijkt dat dit gezien de organisatiegrootte voor het VB niet realiseerbaar is, bepaal aanvullende beheersingsmaatregelen. Hierbij kan gedacht worden aan de inhoudelijke beoordeling door de ISO op de uitgevoerde BIO-controles en dat deze functionaris zijn beoordeling vastlegt op het BIO-sjabloon of in de topdeskregistratie en dashboard ISO (later: in de nieuwe GRC-tool).

Zichtbare beoordeling ISO op BIO-sjablonen/Topdeskregistratie niet aangetroffen

Een zichtbare beoordeling door de ISO op de uitgevoerde BIO-controles (12.3.1.1, 12.3.1.2, 12.3.1.3, 12.3.1.4, 12.3.1.5 en 17.1.3.1) is niet aangetroffen op het BIO-sjabloon en/of in de Topdeskmelding.

De ISO heeft op 24 mei 2025 meegedeeld dat hij aan de hand van de BIO-sjablonen en/of Topdeskmeldingen de uitgevoerde BIO-controle inhoudelijk beoordeelt.

Daarbij zoekt deze functionaris de onderliggende aangeleverde documentatie (audittrail) op en let daarbij op de status van het document (definitief of concept) en de datum (recent of verouderd).

Op basis hiervan worden in het dashboard ISO de conclusies voor opzet, bestaan en werking meegeven, die bepalend zijn voor de kwantitatieve bestuurlijke informatie over uitgevoerde BIO-controles.

Aanbeveling (Justid Opsporing)

- Draag er zorg voor dat de ISO de resultaten van de uitgevoerde BIO-controles beoordeelt en zijn bevindingen vastlegt op het BIO-sjabloon of in de topdeskregistratie en dashboard ISO (later: in de nieuwe GRC-tool).

5 Verantwoording onderzoek

5.1 Werkzaamheden en afbakening

De opdrachtbevestiging voor het onderzoek "Beheer Verwijzingsportaal Bankgegevens Justid 2025" (kenmerk 2025-00000760039) is op 12 maart 2025 goedgekeurd door de plaatsvervangend directeur-generaal van DGO, drs. M.C. van Tuyl.

Het doel van de opdracht is het geven van bevindingen en aanbevelingen bij de opzet, het bestaan en de werking van de verbijzonderde controle op de naleving van de BIO-maatregelen voor het VB door Justid Opsporing voor de volgende processen:

1. Governance van privacy en informatiebeveiliging;
2. Wijzigingenbeheer;
3. Logische toegangsbeveiliging;
4. Back-up, restore en uitwijk.

Het beoordelen van de opzet en het vaststellen van het bestaan betreft een momentopname zoals deze tot stand is gekomen op 1 april 2025. De werking heeft betrekking hebben op de periode 4e kwartaal 2024 en 1e kwartaal 2025.

Bij het onderzoek zijn de volgende onderzoeksvragen gehanteerd:

1. Welke bevindingen en aanbevelingen heeft de ADR over de uitgevoerde verbijzonderde controle door Justid op het beheerproces "Governance van privacy en informatiebeveiliging" voor het VB?
2. Welke bevindingen en aanbevelingen heeft de ADR over de uitgevoerde verbijzonderde controle door Justid op het beheerproces "Wijzigingenbeheer" voor het VB?
3. Welke bevindingen en aanbevelingen heeft de ADR over de uitgevoerde verbijzonderde controle door Justid op het beheerproces "Logische toegangsbeveiliging" voor het VB?
4. Welke bevindingen aanbevelingen heeft de ADR over de uitgevoerde verbijzonderde controle door Justid op het beheerproces "Back-up, restore en uitwijk" voor het VB?

Voor dit onderzoek is het toetsingskader "Beheer Verwijzingsportaal Banken versie 1.1" van 28 februari 2025 gehanteerd. Dit kader is op 28 februari 2025 goedgekeurd door DGO.

Het onderzoek is uitgevoerd in de periode april 2025 tot en met juni 2025. Tijdens het onderzoek is regelmatig afgestemd met contactpersonen bij DGO en Justid Opsporing.

Het onderzoek van ADR is gericht op de uitgevoerde verbijzonderde BIO-controles door Justid Opsporing en het Cluster Beveiliging van Justid. Als de BIO-controle is uitgevoerd heeft ADR een analyse op deze controle uitgevoerd om vast te stellen of zij tot dezelfde conclusies kunnen komen voor de opzet, bestaan en werking die gegeven zijn door Justid Opsporing. Voor de BIO-maatregelen die niet zijn voorzien van een BIO-sjabloon (of Topdeskmelding) of het ontbreken van een onderbouwing van de conclusies voor opzet, bestaan en werking in het BIO-sjabloon (Of Topdeskmelding) heeft de ADR geen nadere analyse uitgevoerd.

Het onderzoek is gestart met een analyse van de documentatie die betrekking heeft op de uitgevoerde BIO-maatregelen door Justid Opsporing en het Cluster Beveiliging van Justid gericht op de onderzochte processen in scope. Vervolgens zijn interviews gehouden met medewerkers van Justid Opsporing en het Cluster Beveiliging van Justid, die ons per uitgevoerde BIO-maatregel voor VB van relevante informatie hebben voorzien. Daarnaast zijn voor een aantal BIO-maatregelen waarnemingen ter plaatse gedaan.

De resultaten van de documentatieanalyses, interviews, waarnemingen en een samenvatting van de bevindingen zijn in een toetsingsformulier vastgelegd. De toetsingsformulieren zijn op 26 mei 2025 bij Justid Opsporing afgeleverd voor een reactie. Op 24 juni 2025 zijn de (samenvattende)bevindingen en de reacties van Justid Opsporing besproken met de manager van Justid opsporing.

Het conceptrapport is op 18 juli 2025 voorgelegd bij de manager van Justid Opsporing voor een reactie. De manager van Justid Opsporing heeft op 22 augustus 2025 een gezamenlijke reactie van de opdrachtgever DGO gegeven, die is besproken in een overleg tussen Justid Opsporing en de opdrachtgever DGO en ADR op 28 augustus 2025. In dat overleg is de afhandeling van de gemaakte opmerkingen vastgesteld. Tijdens het overleg heeft de contactpersoon van de opdrachtgever DGO aangegeven dat het rapport definitief gesteld kan worden.

Afbakening

Bij het onderzoek Justid Opsporing is de volgende afbakening gehanteerd:

- ADR is uitgegaan van de geregistreerde stand van de nog uit te voeren/uitgevoerde verbijzonderde controles op BIO-maatregelen door Justid voor de benoemde vier beheersprocessen in de scope volgens het gehanteerde dashboard van Justid op 1 april 2024;
- De beheersprocessen in de scope worden onderzocht voor zover deze betrekking hebben op de door Justid beheerde infrastructuur;

- ADR heeft de uitgevoerde verbijzonderde controle door Justid Opsporing op de processen in scope onderzocht. Als de controle niet door Justid Opsporing is uitgevoerd, is overeengekomen dat ADR zelf de controle niet zal uitvoeren.

5.2 Gehanteerde standaard en kwaliteitsborging

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing. Dit onderzoek verschaft geen zekerheid in de vorm van een oordeel of conclusie, omdat het een onderzoeksopdracht betreft en geen controle-, beoordelings- of andere assurance-opdracht. Als hier wel sprake van was geweest, dan zouden we wellicht andere zaken hebben geconstateerd en gerapporteerd.

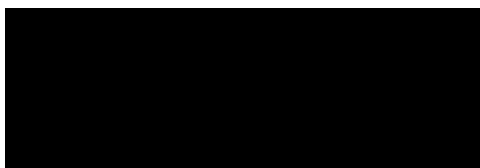
De opdracht is uitgevoerd volgens de algemene uitgangspunten voor de uitoefening van de interne auditfunctie bij de rijksdienst. Daarbij hoort ook een stelsel van kwaliteitsborging. Een onderdeel daarvan is dat er een onafhankelijke kwaliteitstoetsing heeft plaatsgevonden op deze onderzoeksopdracht.

5.3 Verspreiding rapport

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Voor openbaarmaking door het opdrachtgevende ministerie van door de ADR aan dit ministerie uitgebrachte rapporten gelden de voorschriften uit de Wet open overheid. De minister van Financiën stuurt elk halfjaar een overzicht van door de ADR uitgebrachte rapporten naar de Tweede Kamer.

6 Ondertekening

Den Haag, 6 oktober 2025



Auditmanager

Auditdienst Rijk

Bijlage 1 Managementreactie Justid Opsporing



Ministerie van Justitie en Veiligheid

> Retouradres Postbus 484 2501 CL Den Haag

Justitiële Informatiedienst

Directie
Informatiehuishouding
Opsporing

Turfmarkt 147
2511 DP Den Haag
Postbus 484
2501 CL Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon

Datum 22 september 2025
Betreft Reactie Justitiële Informatiedienst Audit rapport VB 2025

Onze referentie
Managementreactie
Justid/Opsporing 2025

Geachte heer, mevrouw,

De afdeling Opsporing van de Justitiële Informatiedienst (Justid) voert sinds september 2019 het beheer over het Verwijzingsportaal Bankgegevens (VB). De Auditdienst Rijk (ADR) heeft in opdracht van DG Ondernijning (DGO) een audit uitgevoerd naar het beheer van het VB door Justid Opsporing in de periode april tot en met juni 2025.

Justid Opsporing heeft kennisgenomen van het rapport 'Rapport - Onderzoek Beheer Verwijzingsportaal Bankgegevens Justid 2025'. De ADR benadrukt dat Justid Opsporing veel werk heeft verzet in de korte periode sinds het vorige auditrapport (juli 2024), met de professionalisering van het proces rond de BIO-controles en inrichting ervan.

Het rapport geeft ook aan dat nog niet alles is gerealiseerd. Er zijn al veel stappen gezet en de basis voor het proces van BIO-controles staat. Wij nemen de bevindingen en aanbevelingen over en hebben een bevindingen- en aanbevelingenmatrix opgesteld met de intentie om deze binnen een redelijke termijn op te volgen. Ook met de bevindingen die gelden voor de Justid-brede werkwijze gaan wij aan de slag.

De audit werkgroep gaat de opvolging hiervan stimuleren en monitoren. De voortgang zal periodiek worden gerapporteerd aan de manager Justid Opsporing en uiteraard wordt ook de opdrachtgever DGO op de hoogte gehouden.

Wij danken u wederom voor het audit onderzoek. Uw bevindingen en aanbevelingen worden opgevolgd en hebben daarvoor onze volledige aandacht.

Hoogachtend,



Auditdienst Rijk

Postbus 20201

2500 EE Den Haag