Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport follow-up ADR-bevindingen Verwijzingsportaal bankgegevens 2023 bij Justid Opsporing

Definitief

Colofon

Titel	Onderzoeksrapport follow-up ADR-bevindingen Verwijzingsportaal Bankgegevens 2023 bij Justid Opsporing
Uitgebracht aan	DG-Ondermijning van het ministerie van Justitie en Veiligheid
Datum	8 juli 2024
Kenmerk	2024-0000375298

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Aanleiding opdracht

Op grond van het Besluit verwijzingsportaal bankgegevens van 10 september 2020 heeft de Auditdienst Rijk (ADR) in de periode oktober 2022 tot en met januari 2023 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. Naar aanleiding van dat onderzoek zijn de belangrijkste bevindingen beschreven in het onderzoeksrapport "Beheer Verwijzingsportaal Bankgegevens" (kenmerk 2023-00000995113) dat is uitgebracht op 18 april 2023.

Om verdere invulling te geven aan de bepalingen in het Besluit verwijzingsportaal bankgegevens heeft het Directoraat-Generaal Ondermijning van het ministerie van Justitie en Veiligheid (JenV) de ADR gevraagd een onderzoek uit te voeren naar de opvolging van de bevindingen zoals deze door de ADR in 2023 zijn gerapporteerd over het beheer VB bij Justid.

Doel onderzoek en onderzoeksvragen
Het doel van het onderzoek is aan de lezer van het rapport inzicht te geven in de opvolging van de door de ADR in 2023 gerapporteerde bevindingen met betrekking tot het beheer van het VB door Justid Opsporing.

Met dit rapport willen wij een antwoord geven op de volgende onderzoeksvraag:
Wat is de status van de openstaande bevindingen uit het onderzoeksrapport "Beheer Verwijzingsportaal Bankgegevens" (kenmerk: 2023-0000099513) dat is uitgebracht op 18 april 2023?

Peildatum onderzoek
De peildatum van ons onderzoek is 23 mei 2024. 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.

Managementsamenvatting

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 Ondermijning 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.

Dit rapport bevat de uitkomsten van het onderzoek bij Justid Opsporing en geeft antwoord op de volgende onderzoeksvraag:
Wat is de status van de openstaande bevindingen uit het onderzoeksrapport "Beheer Verwijzingsportaal Bankgegevens" (kenmerk: 2023-0000099513) dat is uitgebracht op 18 april 2023?

Justid Opsporing heeft veel aandacht besteed aan het oplossen van de openstaande tekortkomingen op de ADR-bevindingen 2023

Naar aanleiding van ons onderzoek naar de opvolging van de ADR-bevindingen 2023, hebben wij vastgesteld dat Justid Opsporing veel tijd in het oplossen van de bij de vorige audit geïdentificeerde afwijkingen heeft gestoken. Nog niet alle bevindingen zijn afgehandeld. Van de 50 geconstateerde afwijkingen[1] bij de bevindingen van de vorige audit zijn 30 afwijkingen opgelost.

In de vorige auditrapportage is er een onderscheid gemaakt tussen bevindingen die direct aandacht vragen van Justid Opsporing en verbetermogelijkheden:

a) *Bevindingen die direct de aandacht vragen van Justid Opsporing.*
In totaal waren er voor de vier bevindingen bij de vorige audit 18 afwijkingen geconstateerd. Tijdens dit onderzoek is gebleken dat 12 afwijkingen zijn opgelost, waarmee de ADR één bevinding heeft kunnen afsluiten. Drie bevindingen vanuit de vorige audit zijn nog niet volledig opgelost.
(zie §1.2, §1.3 en §1.5)

b) *Bevindingen die als verbetermogelijkheden voor de onderdelen van het beheer VB bij Justid Opsporing zijn aangemerkt.*
In totaal waren er voor de vier bevindingen bij de vorige audit 32 afwijkingen geconstateerd. Tijdens dit onderzoek is gebleken dat hiervan 18 afwijkingen zijn opgelost. Voor twee van de vier bevindingen vanuit de vorige audit zijn nog niet (volledig) opgelost.
(zie §2.2 en §2.4)

[1] Voor een tweetal afwijkingen (zie bijlage 1: 1.4A en 1.4B) is er sprake van een dubbeltelling omdat deze betrekking hebben op bevindingen die direct de aandacht vragen van Justid Opsporing (§ 2.4 vorige rapport) en bevindingen die als verbetermogelijkheden zijn aangemerkt (§ 3.3 vorige rapport).

In deze samenvatting beperken wij ons op nadere uitwerking van de drie bevindingen die nog niet volledig zijn opgelost en aangemerkt kunnen worden als direct aandacht voor Justid Opsporing.

Er is aandacht nodig voor het opzetten en het inrichten van de BIO-maatregelen voor het VB en de uitvoering van onafhankelijke controle hierop *(zie § 1.5 en § 2.4 van dit rapport)*

Vijf jaar na de vaststelling van de BIO is het opzetten en het inrichten van de BIO-maatregelen bij Justid Opsporing nog niet afgerond. Justid Opsporing onderkent het belang van de BIO en streeft ernaar in 2024 de specifieke BIO-maatregelen voor het VB ingericht te hebben. Om dit mede te kunnen realiseren heeft Justid Opsporing een deskundige ingehuurd.

Een volledig inzicht van de invoering van de BIO-maatregelen (incl. tijdspad) binnen Justid Opsporing hebben wij niet ontvangen.

Bij de vorige audit was gemeld dat Justid Opsporing bezig was een beperkt aantal BIO-maatregelen op te zetten en in te richten (17 van 250 BIO-maatregelen (ongeveer 7%)). ADR heeft op 9 april 2024 bij Justid Opsporing het Excel overzicht 'voortgang implementatie BIO Controls' (BIO-dashboard) ingezien. Volgens dat overzicht blijkt dat een groot aantal BIO-maatregelen voor het VB niet zijn ingericht.

Volgens dat dashboard is voor de 250 BIO-maatregelen ingericht:
- 16 van 49 systeem specifieke BIO-maatregelen (33%),
- 1 van 131 generieke BIO-maatregelen (1%) en
- 0 van 70 overige BIO-maatregelen (0%).

Daarnaast is er is geen volledig ingerichte periodieke controle van het VB op naleving van het beleid en alle maatregelen voor informatiebeveiliging (BIO). Justid Opsporing is bezig de periodieke controle in te richten. Deze controle zal worden uitgevoerd door Informatiebeveiliging Functionarissen binnen Justid Opsporing.

Er is aandacht nodig voor het periodiek rapporteren door de IT-leveranciers aan Justid Opsporing *(zie § 1.2 van dit rapport)*

Justid Opsporing heeft in 2023 geen rapportage (bijvoorbeeld in-control-verklaring) van ontvangen over de getroffen beveiligingsmaatregelen en de mate waarin wordt voldaan aan de BIO. Justid Opsporing is met overeengekomen om dit alsnog geregeld te krijgen.

Voor de rapportage over de getroffen beveiligingsmaatregelen en de mate waarin wordt voldaan aan de BIO verwijst Justid Opsporing voor de naar de ISO-certificeringen van 2022 (met geldigheid tot en met 2025). Deze certificering is verkregen naar aanleiding van het onderzoeksrapport van 22 december 2022 en heeft betrekking op het toepassingsgebied van de ISO 9001 en ISO 27001. Voor het jaar 2023 hebben wij geen rapportage ontvangen of voldoet aan de gesteld BIO-maatregelen vanuit Justid Opsporing.

Justid Opsporing heeft niet in kaart gebracht of het toepassingsgebied en de reikwijdte van de ISO27001 certificering passend is voor de dienstverlening aan Justid Opsporing en of deze voldoet aan de gestelde BIO-maatregelen vanuit Justid Opsporing. Justid Opsporing zal met nog concrete afspraken maken over het periodiek aantonen dat voldoet aan de gestelde BIO-maatregelen van Justid Opsporing voor het VB.

Voor de voorziening Security Information & Event Management (SIEM) is er aandacht nodig over de definitieve besluitvorming van externe toetsing en de afwikkeling van de openstaande acties in 2020 *(zie § 1.3 van dit rapport)*

Justid Opsporing heeft voor het Verwijzingsportaal bankgegevens (VB) een systeem voor Security Information & Event Management (SIEM) ingericht. Het doel van de SIEM is om verdachte gebeurtenissen op het gebied van informatiebeveiliging te detecteren, zodat Justid Opsporing op basis hiervan de gegevens kan analyseren.

In 2018 is in de stuurgroep VB toegezegd dat er een externe toetsing van de SIEM zal plaatsvinden. Deze externe toetsing is nog niet uitgevoerd. De stuurgroep VB heeft besloten in het vierde kwartaal 2024 een definitief besluit te nemen of een externe toetsing van het SIEM moet plaatsvinden.

In 2020 waren voor de inrichting van SIEM een viertal openstaande acties. Er is geen informatie door Justid Opsporing aangereikt waaruit de stand van zaken rondom deze openstaande acties blijkt.

Context

Het Verwijzingsportaal Bankgegevens (VB)

Het VB is een digitale voorziening voor de geautomatiseerde verstrekking van gegevens die worden opgevraagd door de daartoe wettelijk bevoegde overheidsdiensten (o.a. Politie, FIOD, Koninklijke Marechaussee, Opsporingsdienst Nederlandse Arbeidsinspectie en de Belastingdienst).

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 Opsporing van het ministerie Justitie en Veiligheid. Het VB fungeert 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 wordt afgewisseld door een opvolgaudit met beperkte reikwijdte.

Leeswijzer

In hoofdstuk 1 gaan wij in op de status van de opvolging van de vier ADR-bevindingen die direct de aandacht van Justid Opsporing vragen.
In hoofdstuk 2 geven wij een weergave van de opvolging van de vier ADR-bevindingen, die zijn aangemerkt als verbetermogelijkheden in het beheer door Justid Opsporing.

In hoofdstuk 3 geven wij een toelichting op het door ons uitgevoerde onderzoek.

In bijlage 1 "Overzicht afwijkingen n.a.v. audit 2023" zijn de geconstateerde afwijkingen van de vorige audit per toetsingsnummer weergegeven.

In bijlage 2 is de reactie 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 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. Drie van de vier bevindingen, die vanuit de vorig audit direct aandacht van Justid Opsporing vragen, zijn nog niet volledig opgelost

1.1 Inleiding

In het onderzoeksrapport Beheer Verwijzingsportaal Bankgegevens van 18 april 2023 (kenmerk 2023-0000099513) waren onderstaande bevindingen (titels) gerapporteerd, die direct aandacht van Justid Opsporing vragen.

De bevindingen zijn onderbouwd aan de hand van toetsingsnummers. In bijlage 1 "Overzicht afwijkingen n.a.v. audit 2023" zijn de geconstateerde afwijkingen van de vorige audit per toetsingsnummer weergegeven.

1) "Er is te weinig zicht op de dienstverlening door IT-dienstverlener" *< paragraaf 2.1 van vorig rapport>*

- Tijdens het onderzoek in 2023 had deze bevinding betrekking op 7 geconstateerde afwijkingen (zie bijlage 1: 2.1A, 2.1B, 2.1C, 2.1D, 2.2A, 2.2B en 2.3A).
- Voor de resultaten uit dit onderzoek wordt verwezen naar §1.2.

2) "De voorziening voor het detecteren van oneigenlijke toegang of oneigenlijk gebruik van het VB is niet af"*< paragraaf 2.2 van vorig rapport>*

- Tijdens het onderzoek in 2023 had deze bevinding betrekking op 3 geconstateerde afwijkingen (zie bijlage 1: 8.2A, 8.2B en 8.2C).
- Voor de resultaten uit dit onderzoek wordt verwezen naar §1.3.

3) "Het is onzeker of voorzieningen voor calamiteiten volledig en tijdig herstel van het VB mogelijk maken" *< paragraaf 2.3 van vorig rapport>*

- Tijdens het onderzoek in 2023 had deze bevinding betrekking op 6 geconstateerde afwijkingen (zie bijlage 1: 9.1A, 9.3A, 9.3B, 9.3C, 9.4A en 9.4B).
- Voor de resultaten uit dit onderzoek wordt verwezen naar §1.4.

4) "Invoering van de BIO binnen Justid Opsporing staat nog aan het begin; het tijdspad voor invoering van de hele BIO is onduidelijk" *< paragraaf 2.4 van vorig rapport>*

- Tijdens het onderzoek in 2023 had deze bevinding betrekking op 2 geconstateerde afwijkingen (zie bijlage 1: 1.4A en 1.4B).
- Voor de resultaten uit dit onderzoek wordt verwezen naar §1.5.

In totaal waren voor de bovenstaande bevindingen 18 afwijkingen geconstateerd. Naar aanleiding van dit onderzoek is gebleken dat van de 18 geconstateerde afwijkingen van de vorige audit:
- 12 afwijkingen zijn opgelost;
- 6 afwijkingen niet zijn opgelost.

1.2 Geen inzicht op de getroffen BIO-beveiligingsmaatregelen bij de IT-dienstverleners en hun toeleveranciers

Bevinding uit eerder ADR-onderzoek < paragraaf 2.1>

Bevinding 2023: "Er is te weinig zicht op de dienstverlening door IT-dienstverlener"

Bij het onderzoek in 2023 had de bovenstaande bevinding betrekking op 7 geconstateerde afwijkingen (zie bijlage 1: 2.1A, 2.1B, 2.1C, 2.1D, 2.2A, 2.2B en 2.3A).

Tijdens dit onderzoek is gebleken dat van de 7 geconstateerde afwijkingen van de vorige audit:
- 5 afwijkingen zijn opgelost;
- 2 afwijkingen niet zijn opgelost.

Bevindingen nog niet opgelost

Justid Opsporing heeft van , inclusief van hun toeleveranciers, geen rapportage over 2023 (bijvoorbeeld in-control-verklaring) ontvangen over de getroffen beveiligingsmaatregelen en de mate waarin wordt voldaan aan de BIO. Justid Opsporing is met overeengekomen om dit alsnog geregeld te krijgen. (zie bijlage 1: 2.1C en 2.2B)

Voor de rapportage over de getroffen beveiligingsmaatregelen en de mate waarin wordt voldaan aan de BIO verwijst Justid Opsporing voor de naar de ISO-certificeringen van 2022 (met geldigheid tot en met 2025). Deze certificering is verkregen naar aanleiding van het onderzoeksrapport van 22 december 2022 en heeft betrekking op het toepassingsgebied van de ISO 9001 en IS 27001. Voor het jaar 2023 hebben wij geen rapportage ontvangen of voldoet aan de gesteld BIO-maatregelen vanuit Justid Opsporing.

Justid Opsporing heeft niet in kaart gebracht of het toepassingsgebied en de reikwijdte van de ISO27001 certificering passend is voor de dienstverlening aan Justid Opsporing en of deze voldoet aan de gestelde BIO-maatregelen vanuit Justid Opsporing. Justid Opsporing zal met nog concrete afspraken maken over het periodiek aantonen dat voldoet aan de gestelde BIO-maatregelen van Justid Opsporing voor het VB. Justid Opsporing zal daarbij zelf eerst in kaart brengen welke BIO-maatregelen relevant zijn voor om vervolgens de BIO-maatregelen te plotten op de maatregelen vanuit de ISO-toetsing.
(zie bijlage 1: 2.1C en 2.2B)

Uit de afgesloten contracten met de IT-leveranciers is niet op te maken dat en als IT-dienstverleners de aan hen opgelegde BIO-eisen ook heeft door vertaald naar de toeleveranciers van respectievelijk .
(zie bijlage 1: 2.2B)

Bevindingen opgelost

Justid Opsporing heeft de keten van toeleveranciers per IT-dienstverlener in beeld.
(zie bijlage 1: 2.2A)

Justid Opsporing heeft met en contractueel afgesproken dat deze IT-leveranciers moeten voldoen aan passend beveiligingsniveau volgens de BIO.
(zie bijlage 1: 2.1A en 2.1B)

Voor is er een in-control verklaring afgegeven op 28-02-2024. Hierin geeft het management van aan BIO-compliant te zijn. (zie bijlage 1: 2.1C)

Justid Opsporing ontvangt rapportages over het serviceniveau van en . Justid ontvangt geen rapportages over het serviceniveau van . (zie bijlage 1: 2.3A)

De jaarlijkse evaluatie van de dienstverlening door Justid Opsporing met de IT-dienstverleners ( ) heeft in februari 2024 plaatsgevonden, waarbij is vastgesteld in hoeverre IT-dienstverleners voldeden aan de beveiligingseisen.
(zie bijlage 1: 2.1D)

Justid Opsporing heeft met ingang van medio 2023 het netwerkbeheer deels in eigen beheer. Justid Opsporing zal geen gebruik meer maken van de diensten van voor het VB. Medio 2024 zal het beheer volledig belegd zijn bij Justid Opsporing. Justid Opsporing heeft daarvoor geen rapportages over het serviceniveau van ontvangen. *voert alleen overleggen met de (toeleverancier van) over de dienstverlening van (DWR-werkplekken) en is geen gesprekspartner van Justid Opsporing.*
(zie bijlage 1: 2.1A)

1.3 Externe toetsing van de SIEM nog niet plaatsgevonden, besluitvorming hierover is belegd naar 4e kwartaal 2024; geen inzicht in stand van zaken van openstaande actiepunten 2020 voor SIEM

Bevinding uit eerder ADR-onderzoek < paragraaf 2.2>

Bevinding 2023: "De voorziening voor het detecteren van oneigenlijke toegang of oneigenlijk gebruik van het VB is niet af"

Bij het onderzoek in 2023 had de bovenstaande bevinding betrekking op 3 geconstateerde afwijkingen (zie bijlage 1: 8.2A, 8.2B en 8.2C).

Tijdens dit onderzoek is gebleken dat van de 3 geconstateerde afwijkingen van de vorige audit:
- 1 afwijking is opgelost;
- 2 afwijkingen niet zijn opgelost.

<u>Bevindingen nog niet opgelost</u>
Justid Opsporing heeft voor het Verwijzingsportaal bankgegevens (VB) een systeem voor Security Information & Event Management (SIEM) ingericht. Het doel van de SIEM is om verdachte gebeurtenissen op het gebied van informatiebeveiliging te detecteren, zodat Justid Opsporing op basis hiervan de gegevens kan analyseren. Over de huidige voorziening de volgende bevindingen nog niet opgelost:

Tijdens de vorige audit is opgemerkt dat er de volgende openstaande punten van 2020 rondom de SIEM nog niet waren opgepakt:
- Logging omgeving back-up en restore testen en beschrijven;
- Follow-up procedures bij alerts in overleg met Information Security Officer;
- Proces opzetten om gedefinieerde regels uit te wisselen met bij het VB betrokken partijen;
- Koppelingen van de SIEM aan andere systemen van Justid.

Er is geen informatie door Justid Opsporing aangereikt waaruit de stand van zaken rondom deze openstaande acties blijkt.
(zie bijlage 1: 8.2B)

In 2018 is in de stuurgroep VB toegezegd dat er een externe toetsing van de SIEM zal plaatsvinden. Deze externe toetsing is nog niet uitgevoerd.
Het projectteam VB heeft in de memo "Externe toetsing van de SIEM" van 27 februari 2024 aan de coördinatiegroep VB gevraagd om de externe toetsing van de SIEM voorlopig uit te stellen. Deze memo is op 28 maart 2024 besproken in het stuurgroep VB. De stuurgroep heeft besloten in het vierde kwartaal 2024 een definitief besluit te nemen of een externe toetsing van het SIEM moet plaatsvinden. Het verslag van de stuurgroep vergadering was ten tijde van het onderzoek nog niet vastgesteld en daardoor nog niet beschikbaar om met ADR te delen.
(zie bijlage 1: 8.2C).

Bevindingen opgelost
De SIEM signaleert een tal gebeurtenissen die een indicatie kunnen zijn voor afwijkende met de , afwijkende combinatie met en mutaties op de VB. Justid Opsporing heeft een risico-inschatting uitgevoerd op basis waarvan deze gebeurtenissen zijn geselecteerd.
(zie bijlage 1: 8.2A)

1.4 Voorzieningen van het VB voor calamiteiten zijn volledig getest (restore en uitwijk)

Bevinding uit eerder ADR-onderzoek < paragraaf 2.3>

Bevinding 2023: "Het is onzeker of voorzieningen voor calamiteiten volledig en tijdig herstel van het VB mogelijk maken"

Bij het onderzoek in 2023 had de bovenstaande bevinding betrekking op 6 geconstateerde afwijkingen (zie bijlage 1: 9.1A, 9.3A, 9.3B, 9.3C, 9.4A en 9.4B).

Tijdens dit onderzoek is gebleken dat alle 6 geconstateerde afwijkingen van de vorige audit zijn opgelost.

Bevindingen opgelost

In de Back-up & Disaster Handleiding VB zijn beschrijvingen opgenomen over de bescherming van gegevens (encryptie van data van de back-up op tape), de beveiliging van de verbinding tussen de productieomgeving en de uitwijkomgeving en wie toegang mag hebben tot de back-up tool en de data in de back-up.
(zie bijlage 1: 9.1A)

Op 12 maart 2024 heeft een restoretest plaatsgevonden van een back-uptape, die naar de -uitwijklocatie is gebracht. Hiervan is een testverslag opgesteld. Voor deze test zijn de belangrijkste servers voor het VB getest. Bij deze test is vastgesteld dat deze servers benaderbaar waren.
(zie bijlage 1: 9.3A en 9.3B)

Op 20 februari 2024 heeft er een restoretest plaatsgevonden van de back-up die elk uur op de uitwijkomgeving wordt geplaatst (zie bijlage 1: 9.3C).
De uitwijktest heeft op 11 maart 2024 plaatsgevonden. In het testverslag is aangegeven welke servers zijn geïmporteerd naar de uitwijklocatie om de werking van VB aan te kunnen tonen.
(zie bijlage 1: 9.4A)

Uit het testverslag kan afgeleid worden dat het VB op de uitwijkomgeving in volle omvang bruikbaar was. Deze test was geslaagd. Justid Opsporing heeft ook stappen ondernomen van het terugzetten vanuit uitwijkomgeving naar Justid-omgeving en hiervan een verslag van gemaakt. Deze test was geslaagd. Gebleken is dat de

database goed benaderbaar was en dat de records uit de uitwijktest konden worden bevraagd.
(zie bijlage 1: 9.4A)

1.5 Implementatie BIO-maatregelen vraagt direct de aandacht; het VB wordt niet periodiek beoordeeld op naleving van het beleid en de maatregelen voor informatiebeveiliging (BIO)

Bevinding uit eerder ADR-onderzoek < paragraaf 2.4>

Bevinding 2023: "Invoering van de BIO binnen Justid Opsporing staat nog aan het begin; het tijdspad voor invoering van de hele BIO is onduidelijk"

Bij het onderzoek in 2023 had de bovenstaande bevinding betrekking op 2 geconstateerde afwijkingen (zie bijlage 1: 1.4A en 1.4B). Tijdens het onderzoek is gebleken dat de 2 geconstateerde afwijkingen van de vorige audit niet zijn opgelost.

<u>Bevindingen nog niet opgelost</u>

Een volledig inzicht van de invoering BIO (incl. tijdspad) binnen Justid Opsporing ontbreekt. ADR heeft op 9 april 2024 bij Justid het Excel overzicht 'voortgang implementatie BIO Controls' (BIO-dashboard) ingezien. Volgens dat overzicht blijkt dat een groot aantal BIO-maatregelen voor het VB niet zijn ingericht
(zie bijlage 1: 1.4A).

Justid Opsporing is bezig de BIO-maatregelen gefaseerd in te voeren. Daarbij heeft Justid Opsporing bepaald de volgorde van de implementatie van de BIO-maatregelen voor het VB. Te weten:
1) Specifieke BIO-maatregelen
2) Generieke BIO-maatregelen
3) Overige BIO-maatregelen

Van de prioritering met betrekking tot de implementatie van de BIO-maatregelen door het management van Justid Opsporing hebben wij geen schriftelijke besluitvorming hierover ontvangen.

Volgens het BIO-dashboard (waargenomen op 9 april 2024) is voor de 250 BIO-maatregelen ingericht:
- 16 van 49 systeem specifieke BIO-maatregelen (33%),
- 1 van 131 generieke BIO-maatregelen (1%) en
- 0 van 70 overige BIO-maatregelen (0%).

Er is geen volledig ingerichte periodieke controle van het VB op naleving van het beleid en alle maatregelen voor informatiebeveiliging (BIO). Justid Opsporing is bezig de periodieke controle in te richten. Deze controle zal worden uitgevoerd door Informatiebeveiliging Functionarissen binnen Justid Opsporing.

Wij hebben niet geanalyseerd wat de oorzaak is dat Justid Opsporing vijf jaar na de vaststelling van de BIO nog bezig is met de opzet en de inrichting van een beperkt aantal BIO-maatregelen (17 van 250 maatregelen).
(zie bijlage 1: 1.4B).

2. Twee van de vier bevindingen, die bij de vorige audit waren aangemerkt als verbetermogelijkheden, zijn nog niet volledig opgelost

2.1 Inleiding

In het onderzoeksrapport Beheer Verwijzingsportaal Bankgegevens van 18 april 2023 (kenmerk 2023-0000099513) waren onderstaande bevindingen (titels) gerapporteerd die aangemerkt waren als verbetermogelijkheid .

In bijlage 1 "Overzicht afwijkingen n.a.v. audit 2023" zijn de geconstateerde afwijkingen van de vorige audit per toetsingsnummer weergegeven.

1. "Beleid van Justid en praktische inrichting van het beheer sluiten niet altijd op elkaar aan" < *paragraaf 3.1 van vorig rapport*>

- Tijdens het onderzoek in 2023 had deze bevinding betrekking op 22 geconstateerde afwijkingen (zie bijlage 1: 3.4A, 6.1A, 6.1B, 6.3A, 6.4A, 6.5A, 6.5B, 7.3A, 7.3B, 7.4A, 7.5A, 8.1A, 8.1B, 8.3A, 8.3B, 8.4A, 8.4B, 8.5A, 8.5B, 8.5C, 8.5D en 10.1A).
- Voor de resultaten uit dit onderzoek wordt verwezen naar §2.2.

2. "Besluitvorming over wijzigingen in twee stappen kan de risico-afweging en traceerbaarheid verbeteren" < *paragraaf 3.2 van vorig rapport*>

- Tijdens het onderzoek in 2023 had deze bevinding betrekking op 4 geconstateerde afwijkingen (zie bijlage 1: 5.1A, 7.1A, 7.1B en 10.2A).
- Voor de resultaten uit dit onderzoek wordt verwezen naar §2.3.

3. "Toezicht is in opzet geregeld maar beperkt ingericht" < *paragraaf 3.3 van vorig rapport*>

- Tijdens het onderzoek in 2023 had deze bevinding betrekking op 5 geconstateerde afwijkingen (zie bijlage 1: 1.1A, 1.2A, 1.3A, 1.4A en 1.4B).
- Voor de resultaten uit dit onderzoek wordt verwezen naar §2.4.

4. "De rol van de Information Security Officier (ISO) in het wijzigingstraject kan verduidelijkt worden" < *paragraaf 3.4 van vorig rapport*>

- Tijdens het onderzoek in 2023 had deze bevinding betrekking op 1 geconstateerde afwijking (zie bijlage 1: 5.2A).
- Voor de resultaten uit dit onderzoek wordt verwezen naar §2.5.

In totaal waren er voor de bevindingen, die aangemerkt waren als verbetermogelijkheden 32 afwijkingen geconstateerd.
Tijdens dit onderzoek is gebleken dat van de 32 geconstateerde afwijkingen van de vorige audit:
- 18 afwijkingen zijn opgelost;
- 14 afwijkingen niet zijn opgelost.

2.2 Op een aantal onderdelen is het beleid Justid Opsporing nog niet volledig beschreven en ingericht

Bevinding uit eerder ADR-onderzoek < paragraaf 3.1>

Bevinding 2023: "Beleid van Justid en praktische inrichting van het beheer sluiten niet altijd op elkaar aan"

Bij het onderzoek in 2023 had de bovenstaande bevinding betrekking op 22 geconstateerde afwijkingen (zie bijlage 1: 3.4A, 6.1A, 6.1B, 6.3A, 6.4A, 6.5A, 6.5B, 7.3A, 7.3B, 7.4A, 7.5A, 8.1A, 8.1B, 8.3A, 8.3B, 8.4A, 8.4B, 8.5A, 8.5B, 8.5C, 8.5D en 10.1A).

Tijdens dit onderzoek is gebleken dat van de 22 geconstateerde afwijkingen van de vorige audit:
- 11 afwijkingen zijn opgelost;
- 11 afwijkingen niet zijn opgelost.

Bevindingen nog niet opgelost

In het logisch toegangsbeveiligingsbeleid 2.0 d.d. 29 maart 2023 is geen beschrijvingen opgenomen met betrekking tot het logische toegangspad van beheerders en gebruikers. Daarnaast ontbreekt een beschrijving van de handelwijze voor groeps-, test-, systeem- of serviceaccounts.
(zie bijlage 1: 6.1A)

Bij de vorige audit was geconstateerd dat de beoordeling van accounts en van speciale bevoegdheden voor het VB in 2021 en in de periode 1 januari 2022 t/m 1 oktober 2022 niet heeft plaatsgevonden. Ten tijde van ons onderzoek heeft Justid Opsporing aangegeven dat een controle van accounts en van speciale bevoegdheden voor het laatst in september 2023 is uitgevoerd. ADR heeft na meerdere verzoeken aan Justid Opsporing geen controleverslag op accounts en van speciale bevoegdheden voor VB van september 2023 ontvangen. De geplande controle in het eerste kwartaal 2024 heeft nog niet plaatsgevonden. Deze controle zal uitgevoerd worden in het derde kwartaal 2024 over de periode januari t/m juni 2024.
(zie bijlage 1: 6.4A)

De tekortkoming betrekking hebbend op de inconsistentie tussen de documenten "Password Policy - Wachtwoordbeleid Justid 1.0", "IB-9-031 Logisch Toegangsbeveiligingsbeleid" en "IB-5.1-044 IBO Integraal Beveiligingsplan" over de wachtwoordinstellingen zijn nog niet opgelost. De ingestelde wachtwoordinstellingen voor 'Account lockout duration' en 'Reset account lock-out counter after' in de Domain Default Policy ( ) is niet volgens het beschreven beleid 'Wachtwoordbeleid VB' (versie 1.0 van 21 maart 2024. De wachtwoordinstelling voor het maximumaantal foutieve inlogpogingen is volgens het beleid ingericht.
(zie bijlage 1: 6.5A en 6.5B)

Een beschrijving van de periodieke controle op aanwezigheid van kwetsbaarheden is in het document "VB-Patching" van 1 september 2023 niet aangetroffen.
(zie bijlage 1: 7.3A)

In het document "Protocol Encryptie - Justid_Opsporing_IBO - v1.0" van 19-9-2023 is het beleid voor toepassing van versleuteling voor VB" beschreven. Volgens §8.9 van het beleid wordt de communicatie tussen bevragende VB-organisaties (opsporingsorganisaties) met Justid Opsporing en de verstrekkende VB-organisaties (banken) met Justid Opsporing het beleid onderling vastgesteld. Het beleid voor VB hierover is niet beschreven. Justid Opsporing geeft aan dat de verantwoordelijkheid voor de communicatie (interfaces) tussen bevragende VB-organisatie (opsporingsorganisaties) met Justid Opsporing en de verstrekkende VB-organisaties

(banken) bij Justid Verbindingen en Veiligheid berust en niet bij Justid Opsporing. Wij zijn van mening dat Justid Opsporing ook verantwoordelijk is dat het VB op een correcte wijze blijft functioneren en dat geldt ook over de interfaces tussen de bevragende VB-organisaties en verstrekkende VB-organisaties met het systeem VB. Als de werking van de interfaces bij Verbindingen en Veiligheid belegd is, lijkt het ons logisch dat Justid Opsporing met Justid Verbindingen en Veiligheid ook afspraken maakt over de beveiligingsniveau en eisen (BIO) voor het VB en de periodieke rapportage.
Justid Opsporing geeft aan dat er met Justid Verbindingen en Veiligheid wel afspraken zijn gemaakt, maar of deze volledig is en ook de BIO raakt wordt nog nagegaan.
(zie bijlage 1: 7.4A)

Het document "VB - Logging en Monitoring" (versie 0.4) bevat geen richtlijnen met betrekking tot het verwerken van rapportages uit monitoringtools, het uitvoeren van regelmatige controles op de monitoringactiviteiten en het uitvoeren van regelmatige controles op gelogde activiteiten (log-informatie) van gebruikers c.q. beheerders. Daarnaast heeft er geen onafhankelijke controle plaatsgevonden op het uitvoeren van de monitoringactiviteiten en op de gelogde activiteiten van gebruikers c.q. beheerders.
(zie bijlage 1: 8.1A, 8.1B, 8.5B en 8.5D)

Er is geen nieuw beleid aangereikt waarin een nadere uitwerking over de beoordeling van de logging van activiteiten van beheerders staat beschreven. Daarnaast heeft er geen controle plaatsgevonden op de gelogde activiteiten (log-informatie) van gebruikers c.q. beheerders.
(zie bijlage 1: 8.5A en 8.5B)

<u>Bevindingen opgelost</u>

De gelogde incidentinformatie voor het VB wordt 5 jaar in het SIEM-systeem bewaard.
(zie bijlage 1: 3.4A)

In de werkinstructie "Bijzonder Accounts Opsporing IBO" van 16 april 2024 is de handelwijze voor groeps-, test-, systeem- of serviceaccounts opgenomen. Bij de reikwijdte is aangegeven dat deze werkinstructie van toepassing is voor VB.
(zie bijlage 1: 6.1B)

Bij de vorige audit hadden wij niet kunnen vaststellen welke rol de leidinggevende heeft gehad bij het wijzigen, het deactiveren en het opheffen van twee accounts. In het jaar 2023 was één medewerker vertrokken uit dienst (december 2023). Voor de medewerker hebben wij uit de mail van de leidinggevende van 13 december 2023 kunnen opmaken dat de leidinggevende opdracht heeft gegeven om de rechten VB van de vertrokken medewerker in te trekken.
(zie bijlage 1: 6.3A)

In het document "VB – Patching" van 1 september 2023 is beschreven:
- Hoe omgegaan dient te worden met het tijdig signaleren van kwetsbaarheden;
- Welke bronnen daarbij worden geraadpleegd;
- Hoe omgegaan dient te worden met reguliere-, kritieke- en spoedpatches van kwetsbaarheden.

(zie bijlage 1: 7.3A en 7.3B)

In het document "Protocol Encryptie – Justid/Opsporing/IBO" van 5 september 2023 zijn de sleutelbeheerrollen en de verantwoordelijkheden (RACI-matrix) beschreven. Functiescheidingen zijn impliciet uit de RACI-matrix af te leiden.
(zie bijlage 1: 7.5A)

Het document "VB - Logging en Monitoring" (versie 0.4) is een beschrijving opgenomen over welke monitoringsactiviteiten moeten worden uitgevoerd en de inhoud van de logregel verder gespecificeerd.
(zie bijlage 1: 8.1B, 8.4A en 8.4B)

Vijf beheerders kunnen loginformatie wijzigen en verwijderen. Van de VB Beheerders die op het VB Beheerportaal inloggen worden alle activiteiten gelogd in de VB Database. Op de logging van het beheerportaal is hashing toegevoegd zodat het zichtbaar is wanneer de logging achteraf is aangepast.
(zie bijlage 1: 8.5C)

In het beleid voor logging en monitoring zijn de uitgangspunten voor logging beschreven. In een Excel overzicht is de bewaartermijn per bevraging VB inzichtelijk gemaakt.
(zie bijlage 1: 10.1A)

2.3 Formele besluitvormingen over wijzigingen in VB in twee stappen (voorbereiding door Product Owner en akkoord door manager van Justid Opsporing of de teamleider) zijn ingericht

Bevinding uit eerder ADR-onderzoek < paragraaf 3.2>

Bevinding 2023: "Besluitvorming over wijzigingen in twee stappen kan de risico-afweging en traceerbaarheid verbeteren"

Bij het onderzoek in 2023 had de bovenstaande bevinding betrekking op 4 geconstateerde afwijkingen (zie bijlage 1: 5.1A, 7.1A, 7.1B en 10.2A).

Tijdens dit onderzoek is gebleken dat de 4 geconstateerde afwijkingen naar aanleiding van de vorige audit zijn opgelost.

<u>Bevindingen opgelost</u>

In het wijzigingsprotocol van 11 april 2024 is een beschrijving opgenomen hoe omgegaan dient te worden met grote en kleine wijzigingen. Wijzigingen die impact hebben op het koppelvlak wordt een Request for Change formulier (RFC) opgesteld. Deze RFC wordt beoordeeld door de projectmanager DGO en de Product Owner. Na deze beoordeling wordt de RFC voorgelegd aan de coördinatiegroep VB die indien nodig advies uitbrengt aan de stuurgroep voor de definitieve goedkeuring. Technische- en overige wijzigingen worden goedgekeurd door de Product Owner. Wijzigingen worden meegenomen in de planning van een release. Een release wordt formeel goedgekeurd door de Product Owner. Van een wijziging met raakvlak op de koppelvlakken en een overig wijziging is vastgesteld dat de besluitvorming voor de change is uitgevoerd volgens het protocol.
(zie bijlage 1: 5.1A)

In het document "VB-CMDB Beheer" (versie 0.3) zijn werkafspraken over het beheer van de CMDB beschreven. Het formeel goedkeuringsproces bij het doorvoeren van wijzigingen van configuratie-item in de CMDB wordt het wijzigingsprotocol gevolgd.
(zie bijlage 1: 7.1A, en 7.1B)

Bij de vorige audit was aangegeven dat er geen formele besluitvorming terug te vinden was over de wijziging die betrekking had op de verwijdering van de tijdelijke opslag van vraag- en antwoordberichten in het VB. Wij hebben vastgesteld dat in de registratietool de Product Owner een formele goedkeuring voor de wijziging heeft gegeven.
(zie bijlage 1: 10.2A).

2.4 Toezicht op informatiebeveiliging ontbreekt; een groot deel van BIO-maatregelen is nog niet ingericht

Bevinding uit eerder ADR-onderzoek < paragraaf 3.3>

Bevinding 2023: "Toezicht is in opzet geregeld maar beperkt ingericht"

Bij het onderzoek in 2023 had de bovenstaande bevinding betrekking op 5 geconstateerde afwijkingen (zie bijlage 1: 1.1A, 1.2A, 1.3A, 1.4A en 1.4B).

Tijdens dit onderzoek is gebleken dat van de 5 geconstateerde afwijkingen van de vorige audit:
- 2 afwijkingen zijn opgelost;
- 3 afwijkingen niet zijn opgelost.

Bevindingen nog niet opgelost

Het (volledig) uitvoeren (of initiëren) interne audit en de jaarlijkse Self-Assessment BIO is niet eenduidig uit de jaarplanning 2024 af te leiden.
(zie bijlage 1: 1.1A)

Volledig inzicht invoering BIO (incl. tijdspad) binnen Justid Opsporing ontbreekt. De Information Security Officer heeft aangegeven dat een groot aantal BIO-maatregelen niet zijn ingericht. Daarnaast is er geen volledig ingerichte periodieke controle van het VB op naleving van het beleid en alle maatregelen voor informatiebeveiliging (BIO) < zie ook §1.5 bevinding over de implementatie van BIO maatregelen>.
(zie bijlage 1: 1.4A en 1.4B)

Bevindingen opgelost

De verantwoordelijkheid voor het opstellen (inclusief toezicht) van de Privacy Impact Assessments (PIA) voor het VB ligt bij de verwerkersverantwoordelijke. Hiermee wordt voor het VB de opsporingsdiensten (bijv. Politie, FIOD, KMAR, OD-NLA) bedoeld. Het initiatief van het opstellen van de PIA's met de opsporingsdiensten ligt bij DGO. Justid Opsporing wordt beschouwd als een verwerker. Justid Opsporing maakt geen gebruik van sub-verwerkers. Justid Opsporing heeft echter wel afspraken (in de vorm van een SLA) gemaakt met IT-leveranciers (, en). Deze IT-leveranciers worden niet gezien als sub-verwerkers. Justid Opsporing maakt geen gebruik van persoonsgegevens in het webportaal VB. Alleen metagegevens VB worden gelogd. De metagegevens bevatten geen persoonsgegevens.

De verwerkersverantwoordelijke dient om de 3 jaar een PIA op te stellen (inclusief toezicht) óf bij grote wijzigingen. VB 1.0 is in 2020 voor het eerste in gebruik genomen. De driejaarcyclus is hierbij niet van toepassing omdat het projectteam VB bezig is met een nieuwe versie van het VB (VB 2.0) welk in 2024 wordt geïmplementeerd. Over versie VB 2.0 zal opnieuw een PIA uitgevoerd worden door de verwerkersverantwoordelijke waarbij Justid op verzoek van de verwerkersverantwoordelijke mede een bijdrage zal leveren.

(zie bijlage 1: 1.2A en 1.3A)

2.5 De rol van de ISO in het wijzigingsproces is beschreven en aantoonbaar ingericht

Bevinding uit eerder ADR-onderzoek < paragraaf 3.4>

Bevinding 2023: "De rol van de Information Security Officer (ISO) in het wijzigingstraject kan verduidelijkt worden"

Bij het onderzoek in 2023 had de bovenstaande bevinding betrekking op 1 geconstateerde afwijking (zie bijlage 1: 5.2A). Tijdens dit onderzoek is gebleken dat de geconstateerde afwijking van de vorige audit is opgelost.

Bevindingen opgelost
In het wijzigingsprotocol wordt toegelicht hoe Justid Opsporing omgaat met wijzigingen voor het VB die de beveiliging beïnvloeden. In dit protocol is de rol van de ISO beschreven. De Information Security Officer die toegang heeft tot het Product Backlog, wordt op de hoogte gesteld van de wijziging. De ISO beoordeelt de wijziging en legt zijn goedkeuring vast in de backlog. Voor een wijziging is als voorbeeld aangetoond dat de ISO hierbij betrokken is geweest.
(zie bijlage 1: 5.2A)

3. Verantwoording onderzoek

3.1 Werkzaamheden en afbakening

De opdrachtbevestiging voor het onderzoek "follow-up ADR-bevindingen Verwijzingsportaal bankgegevens 2023 bij Justid" (d.d. 5 maart 2023; kenmerk 2024-0000198585) is op 12 maart 2024 goedgekeurd door de plaatsvervangend directeur-generaal van .

Het doel van de opdracht is aan de lezer van het rapport inzicht te geven in de opvolging van de door de ADR in 2023 gerapporteerde bevindingen met betrekking tot het beheer van het VB door Justid Opsporing. Dit rapport focust zich op Justid Opsporing en geeft antwoord op de onderzoeksvraag: Wat is de status van de openstaande bevindingen uit het onderzoeksrapport "Beheer Verwijzingsportaal Bankgegevens" (kenmerk: 2023-0000099513) dat is uitgebracht op 18 april 2023?

In het onderzoek is gebruik gemaakt van het toetsingskader "Beheer Verwijzingsportaal Banken" (versie 1.0) van 24 augustus 2022, dat is gehanteerd bij het onderzoek "Beheer Verwijzingsportaal Bankgegevens" bij Justid in 2023.

Het onderzoek is uitgevoerd in de periode maart 2024 tot en met juni 2024. Tijdens het onderzoek is regelmatig afgestemd met contactpersonen bij DGO en Justid Opsporing.

Het onderzoek is gestart met een analyse van de documentatie die per onderzochte openstaande bevinding is aangeleverd. Vervolgens zijn interviews gehouden met medewerkers van Justid Opsporing die ons per onderzochte openstaande bevinding van relevante informatie konden voorzien. Daarnaast zijn voor een aantal openstaande bevindingen waarnemingen gedaan.

De resultaten van documentatieanalyse, interviews, waarnemingen en een samenvatting van de bevindingen zijn in een toetsingsformulier vastgelegd. De toetsingsformulieren zijn op 29 april 2024 bij Justid Opsporing teruggelegd voor een reactie.
Op 23 mei 2024 zijn de (samenvattende)bevindingen en de reacties van Justid Opsporing besproken met de manager van Justid opsporing.

Het conceptrapport is op 11 juni 2024 fysiek teruggelegd bij de manager van Justid Opsporing voor een reactie. De manager van Justid Opsporing heeft op 18 juni 2024 een reactie gegeven, die is besproken in een overleg tussen Justid Opsporing en ADR op 20 juni 2024. In dat overleg is de afhandeling van de gemaakte opmerkingen vastgesteld.

Het conceptrapport is op 20 juni 2024 opgeleverd aan DGO voor een reactie. DGO heeft op 26 juni 2024 gereageerd. DGO en ADR hebben op 3 juli 2024 de verwerking van opmerkingen van DGO over het rapport afgestemd.

Afbakening
Bij het onderzoek Justid Opsporing is de volgende afbakening gehanteerd:

- Justid Opsporing heeft beheerwerkzaamheden belegd bij drie IT-dienstverleners nl. (voorheen), en . De uitbestede beheerwerkzaamheden vallen buiten de scope van dit onderzoek. De contracten met deze partijen vallen binnen het onderzoek (proces contractmanagement).

- Justid Opsporing maakt gebruik van diensten die worden geleverd door en . De contracten met en zijn afgesloten door de Directie Informatievoorziening en Inkoop van J&V. Justid Opsporing is hier niet verantwoordelijk voor. Deze contracten vallen buiten de scope van dit onderzoek.

3.2 Gehanteerde Standaard

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.

3.3 Verspreiding rapport

De opdrachtgever, de plaatsvervangend directeur-generaal van DGO, is eigenaar van dit rapport. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Hoewel het rapport de context van het onderzoek zo goed mogelijk probeert te beschrijven, is het mogelijk dat iemand die de context niet (volledig) kent, de uitkomsten anders interpreteert dan bedoeld.

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.

4. Ondertekening

Den Haag, 8 juli 2024

Projectleider Auditdienst Rijk
Auditdienst Rijk

Bijlage 1 Overzicht afwijkingen n.a.v. audit 2023

Tijdens het onderzoek in 2023 waren de volgende afwijkingen geconstateerd.

Toets-nummer	§ in rapport 2023	Omschrijving afwijkingen audit 2023	Opgelost Ja/nee
1.1A	3.3	De verantwoordelijkheid voor het blijven voldoen aan geldende kaders voor informatiebeveiliging is belegd en beschreven in beleid voor Justid Opsporing en verder gedetailleerd in beleid voor IBO. Het toezicht op het voldoen aan de BIO is belegd bij de ISO IBO die daarover verantwoording afgelegd aan de CISO Justid. IBO geeft aan dat enkele onderdelen uit het Beveiligingsbeleidsplan niet zijn belegd: interne audit en de jaarlijkse self assessment voor BIR-maatregelen door alle afdelingen. In het nieuwe concept integraal beveiligingsbeleid voor Justid wordt wel ingegaan op de interne audit-rol als onderdeel van de IB Governance.	Nee
1.2A	3.3	De verantwoordelijkheden binnen Justid voor het opstellen en uitvoeren van het privacy-beleid zijn beschreven. Volgens het privacy-beleidskader is de privacy officer de interne toezichthouder en adviseur. De huidige PIA voor het VB is in 2018 opgesteld. De privacy officer geeft aan de PIA die door het project VB2 opgeleverd is, te gebruiken voor de actualisatie van de huidige PIA door Justid. De privacy officer houdt geen toezicht op het treffen van voorgenomen maatregelen die in een PIA opgenomen zijn. De privacy officer geeft aan dat dit de taak is van het management.	Ja
1.3A	3.3	Voor verwerkersovereenkomsten en -afspraken is de PDCA-cyclus niet ingericht. Er wordt niet gecheckt of bepalingen in verwerkersafspraken worden nagekomen en er vindt geen periodieke controle plaats of bepalingen in verwerkersafspraken nog voldoen.	Ja
1.4A	2.4 en 3.3	In verwerkersafspraken over het VB (zie 1.1) geeft de directeur Justid aan dat verwerking plaatsvindt op infrastructuur die voldoet aan de BIR (voorloper van de BIO), dat toegang, verwerking en opslag plaats vindt volgens de maatregelen behorend bij BBN2 (het standaardniveau)	Nee

		van de BIR en dat Justid Opsporing de Verwerkingsverantwoordelijke voldoende inzicht geeft in het geboden beveiligingsniveau en de overeengekomen getroffen beveiligingsmaatregelen. Volledig Inzicht invoering BIO (incl. tijdspad) binnen Justid Opsporing ontbreekt.	
1.4B	2.4 en 3.3	Er is geen ingerichte periodieke controle van het VB op naleving van het beleid en alle maatregelen voor informatiebeveiliging (BIO).	Nee
2.1A	2.1	Justid Opsporing heeft niet bepaald welke beveiligingsmaatregelen met welke IT-dienstverlener overeengekomen moeten zijn.	Ja
2.1B	2.1	Het contract met vermeldt dat de BIO van toepassing is. Rapportage over de door getroffen beveiligingsmaatregelen is in het contract vastgelegd. De contracten met en zijn minder specifiek over de beveiligingsmaatregelen die van toepassing zijn. Het passende beveiligingsniveau is in deze contracten niet beschreven. De beveiligingseisen voor de housing bij worden door de bepaald.	Ja
2.1C	2.1	IT-dienstverleners rapporteren niet periodiek aan Justid over getroffen beveiligingsmaatregelen en de mate waarin wordt voldaan aan de BIO. Het is de keuze van Justid Opsporing dat IT-dienstverleners alleen rapporteren in het geval van incidenten.	Nee
2.1D	2.1	Er is geen jaarlijkse evaluatie van de dienstverlening door Justid waarbij wordt vastgesteld in hoeverre IT-dienstverleners voldoen aan beveiligingseisen.	Ja
2.2A	2.1	Toeleveranciers niet in beeld	Ja
2.2B	2.1	IT-dienstenleveranciers geven geen inzicht in de beheersmaatregelen die zij genomen hebben om de aan hen opgelegde eisen ook door te vertalen naar hun toeleveranciers.	Nee
2.3A	2.1	Er worden geen rapportages over het serviceniveau door IT-dienstverleners opgeleverd aan Justid Opsporing. Dat is een keuze van Justid.	Ja
3.4A	3.1	Bewaartermijnen van logging-gegevens ib-incident niet ingesteld	Ja
5.1A	3.2	Voor wijzigingen die van invloed zijn op de koppelvlakken van het VB met bevragers en verstrekkers wordt de risico-afweging binnen de projectgroep bij DGO uitgevoerd. Voor overige wijzigingen vindt er geen zichtbare risico-afweging plaats	Ja
5.2A	3.4	Het onderwerp beveiliging komt niet expliciet naar voren in het hele testtraject. Tijdens het ontwikkelproces wordt code gescand op security issues. Daarna ontbreekt in het wijzigingsproces de aandacht voor beveiliging. De ISO beoordeelt testplannen voor het VB niet op	Ja

		het uitvoeren van relevante beveiligingstesten. Justid Opsporing geeft aan dat het de bedoeling is om bij grote wijzigingen een pentest te doen. Rapport: Uit interviews met medewerkers van Justid Opsporing blijkt dat er onduidelijkheid is over de rol die de ISO heeft binnen het wijzigingsproces. Dit heeft betrekking op twee aspecten: Door de ISO beoordelen of testplannen voldoende ingaan op beveiliging; Goedkeuring door de ISO binnen het wijzigingsproces.	
6.1A	3.1	Voor de volgende onderwerpen ontbreekt een beschrijving in het Logisch Toegangsbeveiligingsbeleid: - het logische toegangspad van gebruikers/beheerders; - omgaan met groepsaccounts.	Nee
6.1B	3.1	De procesbeschrijving Accountbeheer Opsporing IBO beschrijft het verlenen van toegang tot informatiesystemen bij Opsporing/IBO aan geautoriseerde personen. In deze procesbeschrijving zijn drie typen accounts buiten scope geplaatst: systeemaccounts, groepsaccounts en testaccounts. M.a.w. voor deze accounts is geen beleid geformuleerd binnen Opsporing/IBO.	Ja
6.3A	3.1	In het Logisch Toegangsbeveiligingsbeleid is aangegeven dat leidinggevenden verantwoordelijk zijn voor het in gang zetten van het wijzigen of deactiveren/opheffen een gebruikersaccount wanneer een medewerker van functie wijzigt of de organisatie verlaat. Wij hebben twee recent ingetrokken accounts in detail bekeken. Het betreft twee accounts in het AD-domein " ". Een van de accounts is ingetrokken vanwege langdurige afwezigheid van de beheerder. Hier lag geen formele opdracht aan ten grondslag ligt. We hebben niet kunnen vaststellen welke rol de leidinggevende heeft gehad bij het wijzigen /deactiveren /opheffen van deze twee accounts	Ja
6.4A	3.1	In het Logisch Toegangsbeveiligingsbeleid staat beschreven: - Alle gebruikersaccounts en de toegekende toegangsrechten worden twee keer per jaar beoordeeld door de leidinggevende. De beoordeling wordt vastgelegd; - De speciale bevoegdheden (o.a. admin rollen) worden minimaal ieder kwartaal beoordeeld.	Nee

		In de procesbeschrijving Accountbeheer Opsporing IBO zijn controleactiviteiten op het accountbeheer door de Procescoördinator (controle 2x per jaar), Information Security Officer (controle 2x per jaar) en de Servicedesk (geen frequentie van de controle) nader beschreven. Beoordeling van accounts en van speciale bevoegdheden voor het VB heeft in 2021 en in de periode 1 januari 2022 t/m 1 oktober 2022 niet plaatsgevonden.	
6.5A	3.1	Wachtwoordvereisten worden beschreven in Password Policy - Wachtwoordbeleid Justid 1.0, IB-9-031 Logisch Toegangsbeveiligingsbeleid en IB-5.1-044 IBO Integraal Beveiligingsplan. Er is geen consistentie tussen deze drie documenten over de aspecten complexiteit, geldigheid, aantal inlogpogingen, lock-out reset. NB Aangegeven is dat het document Password Policy - Wachtwoordbeleid Justid leidend is.	Nee
6.5B	3.1	Uit de Policy voor het blijkt dat wachtwoordeninstelling volgens het specifieke beleid Password Policy - Wachtwoordbeleid Justid voor VB zijn ingesteld. v.w.b. lengte, complexiteit, geldigheid en historie. Uit de default domain policy zijn twee aspecten van wachtwoorden niet op te maken: - het maximum aantal foutieve inlogpogingen; - de blokkering na vijf foutieve inlogpogingen (lock-out reset).	Nee
7.1A	3.2	Het document VB-CMDB beheer geeft weer welke basisgegevens voor een configuratie-item worden vastgelegd. Het document verwijst naar een Excel sheet als CMDB en licht de tabbladen daarin toe. Dit document bevat geen procedure of werkafspraken over beheer van de CMDB en hoe de goedkeuring van de wijziging van configuratie-items verloopt.	Ja
7.1B	3.2	Er ontbreekt een formeel goedkeuringsproces bij het doorvoeren van wijzigingen van configuratie-items in de CMDB.	Ja
7.3A	3.1	In het patchbeleid Justid (uit 2018) bevat geen beschrijving: - hoe omgegaan dient te worden met het tijdig signaleren van kwetsbaarheden - welke bronnen daarbij worden geraadpleegd - de periodieke controle op aanwezigheid van kwetsbaarheden; - hoe te handelen bij spoedpatches (binnen 1 week).	Deels

7.3B	3.1	In het document VB – Patching zijn de periodieke geautomatiseerde updates beschreven. Dit document gaat niet in op hoe omgegaan dient te worden met reguliere- en spoedpatches.van kwetsbaarheden.	Ja
7.4A	3.1	Er is geen vastgesteld beleid voor toepassing van versleuteling voor het VB en de communicatie met bevragers en verstrekkers.	Nee
7.5A	3.1	is een concept beleid voor het gebruik, de bescherming en de levensduur van cryptografische sleutels. Dat gaat in op o.a.: - De BIO maatregelen die van toepassing zijn; - Wie verantwoordelijk is voor implementatie en sleutelbeheer; - Life cycle management. Er zijn onderdelen nog niet uitgewerkt (Sleutelbeheerrollen, Functiescheiding, RACI).	Ja
8.1A	3.1	Het Logging en Monitoring beleid bevat geen beschrijving over uitgangspunten voor monitoringactiviteiten zoals: - welke monitoringsactiviteiten moeten worden uitgevoerd, - hoe om te gaan met rapportages uit monitoringtools en - het uitvoeren van periodieke controle op monitoringsactiviteiten.	Nee
8.1B	3.1	Er wordt niet periodiek gecontroleerd of de monitoringactiviteiten worden uitgevoerd zoals beschreven.	Nee
8.2A	2.2	De risico-inschatting op basis waarvan deze use cases gekozen zijn, ontbreekt.	Ja
8.2B	2.2	In 2020 zijn acties onderkend rondom SIEM. Een aantal acties staan nog open.	Nee
8.2C	2.2	In 2018 is in de stuurgroep VB toegezegd dat er een externe toetsing van de SIEM zou plaatsvinden. Deze toetsing is niet uitgevoerd.	Nee
8.3A	3.1	Bijlage 1 van het Logging- en monitoringbeleid voor Justid bevat een template voor het vastleggen van informatie over logging: welke logging is ingericht, de bewaartermijn, de bewaarlocatie. Voor het VB is deze template niet gevuld.	Ja
8.3B	3.1	Het document VB - Logging en Monitoring bevat enkele technische aspecten van de logging van het VB. Er is geen volledige vertaling van het Justid-brede loggingbeleid naar de logging van het VB.	Ja
8.4A	3.1	In het Logging- en monitoringbeleid van Justid (dat ook geldt voor het VB) staat beschreven waaraan een logregel minimaal moet voldoen. In document VB - Logging en Monitoring is de inhoud van de logregel niet verder gespecificeerd.	Ja
8.4B	3.1	We hebben de inhoud van de logregels van de twee use cases van de SIEM vergeleken met de door het Logging- en monitoringbeleid van Justid Opsporing voorgeschreven inhoud. De logregels	Ja

		voldoen op onderdelen niet aan de vastgestelde eisen. Ontbrekende onderdelen zijn: - Omschrijving van ; - ; - .	
8.5A	3.1	Het logging- en monitoringbeleid van Justid beschrijft op hoofdlijnen de activiteiten van beheerders die gelogd moeten worden, het aanleggen van logfiles en de bescherming van logfiles. De beoordeling van de logging van activiteiten van beheerders is in het beleid niet uitgewerkt.	Nee
8.5B	3.1	De logging van activiteiten van systeembeheerders m.b.t. VB is beperkt uitgewerkt: - In document VB - Logging en Monitoring wordt ingegaan op de bewaartermijn en de toegang tot logbestanden. De te loggen activiteiten van beheerders en de beoordeling van de logging zijn niet in detail uitgewerkt. - Een user story in beschrijft de logging van gebruik van de systeemfuncties Beheer banken en Beheer Nieuwsberichten. De user story heeft status Design.	Nee
8.5C	3.1	De loginformatie is toegankelijk voor alle beheerders. Beheerders kunnen loginformatie wijzigen en verwijderen. De log-informatie is daarmee niet beschermd. Dit is niet conform het logging- en monitoringbeleid van Justid Opsporing.	Ja
8.5D	3.1	De log-informatie wordt niet periodiek beoordeeld.	Nee
9.1A	2.3	Er is geen beschrijving van de volgende aspecten in Backup & Disaster Recovery Handleiding VB aangetroffen: - hoe omgegaan dient worden met het beschermen van gegevens: encryptie van data van de back-up op schijf en tape, beveiliging van de verbinding met de uitwijk-omgeving; - wie toegang mag hebben tot de back-up tool en de data in de back-up.	Ja
9.3A	2.3	Er wordt bij deze test niet gecheckt of een bestand van een back-uptape die naar de -uitwijklocatie is gebracht, teruggezet kan worden.	Ja
9.3B	2.3	Een test van het terugzetten van een volledige back-up vanaf een back-uptape met een controle of het VB daarna volledig functioneert, is niet uitgevoerd.	Ja
9.3C	2.3	Er vindt geen restoretest plaats van de back-up die elk uur op de uitwijkomgeving wordt geplaatst.	Ja
9.4A	2.3	Het testverslag bevat geen informatie over de omvang van de test (welke componenten zijn getest).	Ja
9.4B	2.3	Het testverslag geeft geen inzicht of het VB op de uitwijkomgeving in volle omvang bruikbaar was. < geen inzicht in hersteltijd >	Ja

10.1A	3.1	In het beleid voor logging en monitoring zijn de uitgangspunten voor logging beschreven. Het beleid bevat geen verdere uitwerking van te bewaren gegevens per bevraging.	Ja
10.2A	3.2	Er is geen formele besluitvorming terug te vinden over de verwijdering van de tijdelijke opslag.	Ja

Bijlage 2 Managementreactie Justid Opsporing

Justitiële Informatiedienst
Ministerie van Justitie en Veiligheid

> Retouradres Postbus 484 2501 CL Den Haag

DEP. VERTROUWELIJK

Justitiële Informatiedienst
Informatiehuishouding
Opsporing

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

Contactpersoon
Afdeling Opsporing

Datum 5 juli 2024
Betreft Reactie Justitiële Informatiedienst opvolgaudit rapport VB

Onze referentie
Managementreactie
Justid/Opsporing 2024

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 Ondermijning (DGO) een opvolgaudit uitgevoerd naar het beheer van het VB door Justid, een in beheer bij Justid/Opsporing, naar aanleiding van de audit gedaan in 2023.

Justid/Opsporing heeft kennisgenomen van het rapport 'Onderzoeksrapport Follow-up ADR-bevindingen Verwijzingsportaal Bankgegevens 2023' en onze reactie op de bevindingen verdeeld in de volgende vier hoofdpunten:

1) Justid/Opsporing heeft veel aandacht besteed aan het oplossen van de openstaande tekortkomingen op de ADR-bevindingen 2023
Tijdens ons onderzoek naar de opvolging van de ADR-bevindingen 2023 hebben wij vastgesteld dat Justid/Opsporing er veel tijd heeft ingestoken om de geconstateerde afwijkingen ten tijde van de vorige audit op te lossen. Het einddoel van op te volgen tekortkomingen moet nog bereikt worden. Van de 50 geconstateerde afwijkingen bij de bevindingen van de vorige audit zijn 30 afwijkingen opgelost.

Reactie Justid/Opsporing:
Justid/Opsporing herkent zich in de conclusie van het opvolgaudit onderzoek die ADR heeft uitgevoerd. Dat geldt zowel voor dat Justid/Opsporing veel tijd heeft gestoken in het oplossen van de geconstateerde afwijkingen en de zorg besteedt aan de algemene inrichting van het beheer en leveranciers management van het VB;

2) Er is aandacht nodig voor het opzetten en het inrichten van de BIO-maatregelen voor het VB en de uitvoering van onafhankelijke controle hierop *(zie § 1.5 en § 2.4 van het rapport)*

Bij de vorige audit was gemeld dat Justid/Opsporing bezig was een beperkt aantal BIO-maatregelen op te zetten en in te richten (17 van 250 BIO-maatregelen (ongeveer 7%)). ADR heeft op 9 april 2024 bij Justid het Excel overzicht 'voortgang implementatie BIO Controls' (BIO-dashboard) ingezien. Volgens dat

Justitiële Informatiedienst
Informatiehuishouding
Opsporing

Datum
4 juli 2024

Onze referentie
Managementreactie
Justid/Opsporing 2024

overzicht blijkt dat een groot aantal BIO-maatregelen voor het VB niet zijn ingericht.

Volgens dat dashboard is voor de 250 BIO-maatregelen ingericht:
- 16 van 49 systeem specifieke BIO-maatregelen (33%),
- 1 van 131 generieke BIO-maatregelen (1%) en
- 0 van 70 overige BIO-maatregelen (0%).

Reactie Justid/Opsporing:
We werken hard aan de BIO-maatregelen en hebben sinds het meetmoment weer een aantal stappen gemaakt.

- 20 van 49 systeem specifieke BIO-maatregelen (41%),
- 14 van 131 generieke BIO-maatregelen (11%) en
- 0 van 70 overige BIO-maatregelen (0%).

Als Justid/Opsporing ervaren we ook dat de BIO compliance meer tijd kost als verwacht. We gaan daarom hier nog meer prioriteit aangeven door ook teamleden van de teams te betrekken bij het uitwerken.

3) Er is aandacht nodig voor het periodiek rapporteren door de IT-leveranciers en aan Justid Opsporing *(zie § 1.2 van het rapport)*
Justid heeft in 2023 geen rapportage (bijvoorbeeld in-control-verklaring) van ( ) ontvangen over de getroffen beveiligingsmaatregelen en de mate waarin wordt voldaan aan de BIO. Justid/Opsporing is met overeengekomen om dit alsnog geregeld te krijgen.

Voor de rapportage over de getroffen beveiligingsmaatregelen en de mate waarin wordt voldaan aan de BIO verwijst Justid/Opsporing voor de ( ) naar de ISO-certificeringen van 2022 (met geldigheid tot en met 2025). Deze certificering is verkregen naar aanleiding van het onderzoeksrapport van 22 december 2022 en heeft betrekking op het toepassingsgebied van de ISO 9001 en ISO 27001. Wij zijn van mening dat de onderzoeksresultaten 2022 een moment opname is.

Reactie Justid/Opsporing:
De afgelopen jaren zijn er veel stappen gezet in het leveranciersmanagement. Hiermee zijn ook een aantal bevindingen uit de audit over het leveranciersmanagement met de opvolgaudit opgelost. We hebben regelmatig overleg met onze leveranciers waar de In Control verklaringen en BIO-compliance vast onderdeel is van het overleg. Leverancier is van mening dat met de afgegeven ISO certificaten en afgegeven auditverklaring zij voldoende hebben aangetoond in control te zijn. We gaan met deze auditbevinding met nog concrete afspraken maken over het periodiek aantonen dat voldoet aan de gestelde BIO-maatregelen.

4) Voor de voorziening Security Information & Event Management (SIEM) is er aandacht nodig over de definitieve besluitvorming van

Justitiële Informatiedienst
Informatiehuishouding
Opsporing

Datum
4 juli 2024

Onze referentie
Managementreactie
Justid/Opsporing 2024

externe toetsing en de afwikkeling van de openstaande acties in 2020 *(zie § 1.3 van het rapport)*
Justid/Opsporing heeft voor het Verwijzingsportaal bankgegevens (VB) een systeem voor Security Information & Event Management (SIEM) ingericht. Het doel van de SIEM is om verdachte gebeurtenissen op het gebied van informatiebeveiliging te detecteren, zodat Justid/Opsporing op basis hiervan de gegevens kan analyseren.

In 2018 is in de stuurgroep VB toegezegd dat er een externe toetsing van de SIEM zal plaatsvinden. Deze externe toetsing is nog niet uitgevoerd. De stuurgroep VB heeft besloten in het vierde kwartaal 2024 een definitief besluit te nemen of een externe toetsing van het SIEM moet plaatsvinden. In 2020 waren voor de inrichting van SIEM een viertal openstaande acties. Er is geen informatie door Justid/Opsporing aangereikt waaruit de stand van zaken rondom deze openstaande acties blijkt.

Reactie Justid/Opsporing:
Justid/Opsporing is een project gestart voor het uitbreiden van de bestaande SIEM en opvolging van de SIEM bevindingen. Dit project is in 2024 tijdens de opvolgaudit in volle gang en heeft nog niet alle aanbevelingen verwerkt. De verwachting is dat dit in Q4 van 2024 gereed is.

Opvolging bevindingen
Justid/Opsporing heeft op basis van deze opvolgaudit een bevindingen- en aanbevelingenmatrix opgesteld met de intentie om deze binnen een redelijke termijn op te volgen. De audit werkgroep gaat de opvolging hiervan stimuleren. 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 hebben onze volledige aandacht.

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(070) 342 77 00