Gemeente Amsterdam

Auditrapport

Beveiliging van Informatie en Informatiesystemen (BIO)

Referentie: VIC2024/audit20AJP

Opdrachtgever: Concerncontroller

Auteur: IA&BO

Proceseigenaar: cluster Digitalisering, Innovatie en Informatie

14 maart 2025 (Definitief)

1 Inleiding

Op basis van het auditjaarplan 2024-2025 heeft de afdeling Interne Audit & Beleidsonderzoek een audit uitgevoerd naar de stedelijke beheersing van BIO-compliance. Dit onderwerp is de verantwoordelijkheid van de CIO waarbij de directie Digitale Strategie en Informatie aanspreekpunt is.

In deze audit onderzoeken we de mate waarin de gemeente Amsterdam in control is voor de naleving van de Baseline Informatiebeveiliging Overheid (verder afgekort tot BIO). Dit betekent dat we nagaan in welke mate de inrichting en de uitvoering van de BIO-controls zowel centraal als decentraal bij de directies zijn gewaarborgd. De gemeente is sinds 2019[1] verplicht om de BIO na te leven en heeft in de periode 2021-2023 daartoe een stedelijk programma BIO-implementatie uitgevoerd. Vanaf 2024 wordt van de organisatie verwacht BIO-compliant te werken, als onderdeel van de reguliere bedrijfsvoering.

Op 30 april 2024 hebben wij u onze auditbrief verstuurd met hierin de gemaakte afspraken ten behoeve van de uitvoering van deze audit.

Doelstelling en centrale vraag:
In welke mate beheerst (sturing en monitoring) de gemeente Amsterdam effectief de kwaliteit van de implementatie van de Baseline Informatiebeveiliging Overheid (BIO)?

Scope:
De audit richt zich op de stedelijke beheersing van beveiliging van informatie en informatiesystemen. De audit focust zich op de volgende onderwerpen:

A. Beleid en procedures, waaronder taken, verantwoordelijkheden;
B. Monitoring met detailonderzoek naar compliance bij vijf directies: Digitalisering en Innovatie, Werk en Participatie, Inkomen, Dienstverlening en Parkeren.

Niet in scope:
Tijdens deze audit kunnen we niet het gehele onderwerp onderzoeken. Bij deze audit hebben wij niet gekeken naar BIO-controls welke in scope zijn van andere audits (o.a. centrale logische toegangsbeveiliging met stedelijk IAM, fysieke beveiliging) en centraal uitgevoerde BIO-controls welke de verantwoordelijkheid zijn van een andere directie dan de directies geselecteerd voor onze audit.

Toetsingskader:
1. De Baseline Informatiebeveiliging Overheden, gebaseerd op ISO serie 27000;
2. Centraal beleid van toepassing bij een BIO-norm.

Auditverantwoording:
Wij hebben deze audit uitgevoerd conform het Audit Charter 2024, welke is ondertekend door onze opdrachtgever, de Gemeentesecretaris. Hierin staat de reikwijdte van onze werkzaamheden en bevoegdheden beschreven. De auditcharter is te vinden op onze intranetpagina van IA&BO. Onze werkzaamheden worden uitgevoerd in overeenstemming met de normen van de beroepsgroep voor interne auditors. Dit is het Instituut voor Interne Auditors (IIA). Sinds september 2022 is IA&BO gecertificeerd.

Fully in Control:
Zoals aangegeven in de Auditbrief worden de bevindingen door IA&BO overgenomen in de Governance, Risk en Compliance Tool van Gemeente

[1] zie staatscourant van het Koninkrijk der Nederlanden 2019 nummer 26526 d.d. 16 april 2019

Amsterdam genaamd Fully in Control. Vervolgens dient de auditee de nadere opvolging in dit systeem vast te leggen.

Openbaar maken van rapporten:
Het definitieve auditrapport wordt toegestuurd aan de concerncontroller, de Stedelijk Directeur, de manager Control, de (proces)controller en ACAM. Wanneer ACAM erom verzoekt, verstrekken wij hun ook toegang tot ons dossier. De conclusies en belangrijkste bevindingen worden opgenomen in onze voortgangsrapportage die aan het GMT worden toegestuurd. Alle definitieve auditrapporten worden 6 maanden na bespreking in het Risk en Audit Comité (RAC) openbaar gemaakt.

Opzet van het rapport:
In hoofdstuk 2 hebben wij de samenvatting en conclusies opgenomen. In hoofdstuk 3 zijn onze uitgevoerde werkzaamheden en bevindingen opgenomen. In de bijlagen hebben wij deze bevindingen nader uitgewerkt. In bijlage 2 is een gedetailleerd overzicht van de geïdentificeerde risico's opgenomen en voorzien van bijbehorend auditresultaat. In bijlage 3 is een overzicht opgenomen met daarin de toetsingsresultaten (per thema[2]) zoals geconstateerd tijdens het casusonderzoek bij genoemde directies. Detailinformatie over toetsingsresultaten tijdens de casusonderzoeken zijn gedurende de audit gedeeld met de directies en hun ISO's en I-leads.

Bedankt:
Wij bedanken alle medewerkers die bij dit onderzoek betrokken zijn geweest voor hun inzet en samenwerking bij het verrichten van onze werkzaamheden. Tot het verstrekken van nadere toelichting zijn wij uiteraard bereid.

[2] In scope van de casusonderzoeken zijn 37 BIO-artikelen verdeeld over 12 thema's door I-domein in de BIO-Rasci aan de 'business', de lijndirecties, toegewezen

2 Samenvatting en conclusies

Ter beantwoording van de onderzoeksvraag *In welke mate beheerst (sturing en monitoring) de gemeente Amsterdam effectief de kwaliteit van de implementatie van de BIO?* hebben wij de belangrijkste risico's en de getroffen beheersmaatregelen geïdentificeerd. Wij zijn nagegaan of deze interne beheersmaatregelen zijn ingericht en beschreven (opzet). Vervolgens hebben we vastgesteld of de interne beheersmaatregelen bestaan zoals in opzet beschreven. De resultaten van de toetsing zijn opgenomen in bijlage 2. We hebben geen toetsing op de werking uitgevoerd. De audit heeft betrekking op de periode 2024.

Conclusie
Op basis van de door ons uitgevoerde werkzaamheden is onze conclusie dat de geïdentificeerde risico's vermeld in bijlage 2 beperkt worden beheerst.

De belangrijkste bevindingen (d.i. met prioriteit 1) zijn:

1. Beleid en kaders zijn verouderd en ontbreken deels
2. Naleving BIO is deels gerealiseerd

De gedeeltelijke realisatie van BIO-naleving is mede het gevolg van verouderde en deels ontbrekend beleid en kaders in de periode dat BIO-implementatie werd uitgevoerd.

Als gevolg van ontbreken en verouderd zijn van beleid en kaders bestaat de kans dat misverstanden ontstaan over de gemeentelijke vereisten voor goede uitvoering van informatiebeveiliging wat kan leiden tot inefficiënties en verminderde effectiviteit van de informatiebeveiliging.

De beheersing van informatiebeveiligingsrisico's door directies wordt bemoeilijkt door het niet integraal en tijdig beschikbaar zijn van informatie over de kwaliteit van informatiebeveiliging van uitbestede IT. Assurancerapportages die deze informatie kunnen verschaffen zijn niet integraal beschikbaar.

Managementreactie CIO en directie DSenI
De CIO en directie DS&I heeft op 14 maart 2025 een managementreactie gegeven op dit rapport. Samengevat heeft directie als reactie aangegeven:

We herkennen de bevindingen van de audit dat er ondanks de grote inspanningen van de afgelopen jaren (analyses, verbeterplannen en sturing daarop) en vooruitgang die is geboekt, nog méér moet gebeuren om de informatiebeveiliging op niveau te krijgen en te houden. Dat geldt te meer bij de permanent groeiende (geopolitieke) dreigingen en de wijzigende eisen vanuit Europese en landelijke wet- en regelgeving.

Wel merken we op dat de voorgestelde focus op beleid en kaders niet voldoende zal zijn: er is ook veel commitment bij de directies nodig om het voor elkaar te krijgen, we moeten scherper sturen op stedelijke processen en daarbij informatiebeveiliging nog beter inbedden in de P&C-cyclus. Het i-domein is inmiddels gestart met de aanpak van het Informatiebeveiligings-huis om te komen tot een meer eenduidige organisatie en governance. Van daaruit is de ambitie om het beleid te actualiseren en aan te vullen, om te beginnen de strategische documenten in 2025.

Voor de volledige managementreactie per bevinding verwijzen wij naar bijlage 1 van ons rapport.

3 Werkzaamheden en bevindingen

Werkzaamheden

Met betrekking tot het beoordelen van de opzet hebben wij kennis genomen van de bestaande beleidsdocumenten, procesbeschrijvingen en instructies en deze getoetst aan de controls vermeld in de Baseline Informatiebeveiliging Overheid (BIO).

Het bestaan van de beheersmaatregelen hebben wij vastgesteld aan de hand van bewijsstukken, het houden van interviews en waarnemingen ter plaatse.

Toetsing is uitgevoerd in deelonderzoeken:

1. Onderzoek naar stedelijke implementatie, dat wil zeggen naar beleid, taken en verantwoordelijkheden, inrichting van een proces voor het afleggen van verantwoording.
2. Casusonderzoek bij de eerder genoemde vijf directies naar BIO-compliance in opzet en bestaan en rekening houdend met de gevolgen van de aanwezigheid van IT in eigen beheer, dat wil zeggen zonder betrokkenheid van stedelijk functioneel beheer. Hierbij vormen de 37 BIO-controls verdeeld in 12 thema's gehanteerd tijdens de BIO-implementatie het startpunt. Voorbeelden van deze thema's zijn: Leveranciersbeheer, Logische toegangsbeveiliging en privacy,

Vertrouwen

Uit onze auditwerkzaamheden komt het beeld naar voren dat risico's gedeeltelijk worden beheerst. We zien dit ook terug bij de onderzochte directies waar we een gedeeltelijke compliance met de BIO constateren.

Positieve constatering uit de audit is de integratie van informatiebeveiligingsmaatregelen in de managementstructuur van directies, met nadruk op samenwerking en communicatie tussen Information Security Officers (ISO's), I-leads en verantwoordelijken van directies. Ook de invoering en doorontwikkeling van kwartaalrapportages met daarin de voortgang van directies in de implementatie van informatiebeveiliging zien we als een positieve ontwikkeling. Uit deze zelfrapportages komt een stijgende lijn in de voortgang van de BIO-implementatie naar voren. Ten slotte is steeds stedelijk helderheid verschaft in de taken en verantwoordelijkheden voor informatiebeveiliging.

Een belangrijke oorzaak waardoor de gemeente vijf jaar na ingang van de BIO nog altijd risico's op het gebied van informatiebeveiliging niet beheerst, is het ontbreken van helderheid over de invulling aan informatiebeveiligingsmaatregelen. Het ontbreken van helderheid is een gevolg van het deels ontbreken en verouderd zijn van operationeel/tactische beleidsdocumenten en kaders. Ook het samenvallen van de BIO-implementatie met de reorganisatie van het I-domein heeft waarschijnlijk een rol gespeeld. Andere oorzaken zijn onvoldoende prioriteit bij betrokkenen, maar ook onvolwassenheid van stedelijke processen en daarnaast onvoldoende kennis, capaciteit en continuïteit in personeelsbezetting (centraal en decentraal). Gelukkig is op een deel van deze oorzaken gedurende de looptijd van het programma Implementatie BIO bijgestuurd. Dit door het organiseren van kennissessies en personeelswerving. Inmiddels is ook gestart met de opstelling van richtlijnen voor informatiebeveiliging.

Bevindingen

Naar aanleiding van de door ons uitgevoerde werkzaamheden hebben wij de volgende bevindingen.

1. Beleid en kaders zijn verouderd en ontbreken deels

Strategische kaders zoals 1) "Het stedelijk beleidskader informatiebeveiliging versie 1.0" en 2) "Organisatie van informatiebeveiliging bij de gemeente Amsterdam" zijn vastgesteld door het College in 2020. Deze hadden uiterlijk in 2023 opnieuw vastgesteld moeten worden. In december 2024 is door de

ambtelijke organisatie, het directieteam van cluster Digitalisering Informatie en Innovatie, formeel besloten om de actualisatie en hernieuwde vaststelling van het document “Het stedelijk beleidskader informatiebeveiliging versie 1.0” uit te stellen. Als redenen zijn gegeven de komende vaststelling van de Cyberbeveiligingswet en het lopende onderzoek voor betere inrichting van het “Informatiebeveiligingshuis”. De genoemde documenten zijn inhoudelijk verouderd zoals blijkt uit het ontbreken van de vermeldingen van nieuwe afdelingen en functies welke voortvloeien uit de reorganisatie van juli 2022.

Het tactisch/operationeel beleid en kaders voor veilig verwerken van informatie en daarmee BIO-compliant werken zijn verouderd en slecht vindbaar. Daarbij is de status van een groot deel van deze tactisch/operationele kaders onbekend. Wel zijn in 2024 vier nieuwe richtlijnen opgesteld in de vakgroep Informatiebeveiliging en Continuïteit. Hiermee is gestart met het steeds verder doorvoeren van verbeteringen wat wij als een positieve ontwikkeling zien.

2. Naleving BIO is deels gerealiseerd
De onderzochte directies hebben de naleving van de BIO deels gerealiseerd. We zien over de hele linie problemen met het realiseren van een goede aansluiting op de stedelijk ingerichte processen ten behoeve van de informatiebeveiliging. Dit is een gevolg van het deels ontbreken van heldere stedelijke kaders (zie ook paragraaf vertrouwen en bevinding 1). Een positieve uitzondering vormen de BIO normen bij het thema leveranciersbeheer[3] dat in opzet voldoende is. Daarnaast verloopt de naleving van wel aanwezige processen ten behoeve van de informatiebeveiliging moeizaam. In bijlage 3 is zichtbaar dat slechts 1 thema voor de opzet een voldoende (**V**) scoort en 9 thema’s deels voldoende (**O**).

3. Onvoldoende helderheid over de verantwoordelijkheden in bijzondere situaties
Tijdens de casusonderzoeken (onderzochte directies) hebben we ook een aantal bijzondere situaties aangetroffen. Deze situaties zijn bijvoorbeeld: veel wijzigingen in verantwoordelijken, de overdracht van eigendom van applicaties tussen verschillende directies en het gezamenlijk gebruik van applicaties voor de uitvoering van taken. In deze situaties bleken de taken en verantwoordelijkheden voor hen en andere betrokkenen onvoldoende helder en eenduidig waardoor de beheersing van BIO-compliance niet aantoonbaar gemaakt kon worden.

De bevindingen zijn (met overeenkomstige nummering) nader uitgewerkt in bijlage 1. In bijlage 2 is een volledig overzicht opgenomen van alle door ons getoetste interne beheersmaatregelen met onze conclusies over de opzet, het bestaan en de effectieve werking van de getoetste beheersingsmaatregelen.

In het onderstaande schema hebben wij op basis van een risico-inschatting aangegeven welke prioriteit aan onze bevindingen moeten worden gegeven.

Wij maken daarbij het volgende onderscheid in de bevindingen:
Prioriteit 1: Zeer belangrijk, grote impact, urgent, opvolging direct vereist
Prioriteit 2: Belangrijk, gemiddelde impact, minder urgent, opvolging nodig

Prioriteit 3: Aandacht nodig, beperkte impact, niet urgent, opvolging niet noodzakelijk

[3] In de recent uitgebrachte Boardletter 2024 heeft ACAM een paragraaf gewijd aan assurancerapportages, een onderdeel van leveranciersbeheer. Dit betreft het bestaan van de maatregelen hetgeen ook in ons rapport lager heeft gescoord.

Bevindingen met prioriteit 1 worden in de voortgangsrapportages aan het GMT opgenomen. Prioriteit 2 bevindingen worden alleen aan het GMT gemeld als er geen opvolging aan wordt gegeven en prioriteit 3 bevindingen worden enkel aan de directie en management gerapporteerd.

Bevindingen	Prioriteit 3 Laag	Prioriteit 2 Midden	Prioriteit 1 Hoog
1. BELEID EN KADERS ZIJN VEROUDERD EN ONTBREKEN DEELS			X
2. NALEVING BIO IS DEELS GEREALISEERD			X
3. ONVOLDOENDE HELDERHEID OVER VERANTWOORDELIJKHEDEN IN BIJZONDERE SITUATIES		X	

Bijlage 1: Bevindingen en aanbevelingen

Bevindingen

1. Beleid en kaders zijn verouderd en ontbreken deels	PRIO 1

Achtergrond

Het doel van beleid en kaders is het geven van helderheid over de werkwijze en daarvoor benodigde taken en verantwoordelijkheden voor uitvoering van informatiebeveiliging binnen de gemeente. In de Baseline Informatiebeveiliging Overheid (BIO) zijn in hoofdstuk 5 voorschriften opgenomen over informatiebeveiligingsbeleid:

- Definiëring van een reeks aan beleidsregels ten behoeve van informatiebeveiliging welke goedgekeurd zijn door het juiste managementniveau en vervolgens gedeeld met medewerkers en relevante externe partijen (control 5.1.1).
- Minimaal de volgende onderwerpen dienen in het beleid geregeld te zijn: strategische uitgangspunten en randvoorwaarden, inbedding in het geheel van governance met specifiek aandacht voor de relatie met stedelijk beveiligingsbeleid en stedelijk informatievoorzieningsbeleid, het benoemen van gemeenschappelijke betrouwbaarheidseisen en normen, bevorderen van beveiligingsbewustzijn en de organisatie van de informatiebeveiligingsfunctie zoals de toewijzing van verantwoordelijkheden, taken en bevoegdheden en met aandacht voor ketens aan informatiesystemen (overheidsmaatregel 5.1.1.1).
- Inregelen van periodieke evaluatie en actualisatie van het informatiebeveiligingsbeleid (control 5.1.2) in aansluiting op bestaande bestuurs- en P&C-cycli en externe ontwikkelingen (overheidsmaatregel 5.1.2.1).
- De hoofdstukken 6 tot en met 18 van de BIO bevatten voorschriften voor operationele informatiebeveiliging. Voor een goede uitvoering waarbij gelijke situaties op een gelijke wijze beheerst kunnen worden, is het noodzakelijk dat de gemeente beschikt over instructies voor het geven van invulling aan deze controls. Dit kunnen o.a. zijn beleidsdocumenten, richtlijnen, procesbeschrijvingen en werkinstructies.

Bevinding

De gemeente beschikt voor informatiebeveiliging over strategische kaders en tactisch/operationele kaders.

De strategische kaders zijn in 2020 vastgesteld door het College met een geldigheidsduur van 3 jaar. Deze kaders betreffen “Het stedelijk beleidskader informatiebeveiliging versie 1.0” en “Organisatie van informatiebeveiliging bij

	de gemeente Amsterdam". Beide kaders zijn tot op heden niet geactualiseerd en opnieuw vastgesteld. Wel is door het directieteam van cluster Digitalisering, Informatie en Innovatie (afgekort tot cluster DII) in december 2024 besloten tot verlenging van de geldigheidsduur van "Het stedelijk beleidskader informatiebeveiliging versie 1.0". Actualisatie en hernieuwde vaststelling van het beleidskader is daarmee door de ambtelijke organisatie, niet het College, uitgesteld tot 2025. Ook ontbreken in het document "Organisatie van informatiebeveiliging bij de gemeente Amsterdam" de afdelingen, vakgroepen en functies welke bij de reorganisatie van het I-domein in 2022 nieuw zijn ontstaan. De functie van ISO is wel benoemd, maar taken en verantwoordelijkheden zijn niet beschreven. Voor tactisch/operationeel beleid is een grote hoeveelheid aan procesbeschrijvingen, instructies en schema's (verder aangeduid als beleidsdocumentatie) aangetroffen voor onderwerpen gerelateerd aan informatiebeveiliging. Daarbij constateerden we o.a. dat de status van het merendeel van deze beleidsdocumentatie niet was vast te stellen en er waren meerdere beleidsdocumenten voor dezelfde onderwerpen. Daarnaast is door gesprekspartners tijdens deelonderzoek twee aangegeven dat beleidsdocumentatie slecht vindbaar was en niet stedelijk beschikbaar is gesteld. Recent zijn door de vakgroep Informatiebeveiliging en Continuïteit vier nieuwe richtlijnen opgesteld waarvoor echter geen vaststelling is ontvangen. Een werkwijze voor opstellen, onderhouden en vaststellen van richtlijnen is afgesproken, maar nog niet geformaliseerd.
Risico	Als gevolg van verouderde, ontbrekende of niet vastgestelde stedelijke kaders bestaat de kans dat misverstanden ontstaan op het gebied van gemeentelijke vereisten voor de uitvoering van goede informatiebeveiliging met als gevolg inefficiënties en verminderde effectiviteit van de informatiebeveiliging.
Oorzaak	In afwachting van de Cyberbeveiligingswet en daarop gebaseerde BIO 2.0 is actualisatie met hernieuwde vaststelling van de documenten strategisch beleidskader en organisatie van de informatiebeveiliging uitgesteld tot eind 2025. Ten aanzien van tactisch/operationele kaders van onduidelijke status zijn meerdere oorzaken aan te wijzen: • Bij de samenvoeging van de IV-eenheden in nieuwe directies, afdelingen en vakgroepen zijn de diverse beleidsdocumenten, procesbeschrijvingen en instructies meegenomen. • Onvoldoende capaciteit voor actualisatie van beleid en kaders. • Onduidelijke taakverdeling tussen de nieuwe, en inmiddels weer opgeheven, afdeling Beleid & Kaders en de in 2022 ontstane vakgroepen (wie doet wat?).
Aanbeveling	Borg tijdige opstelling, actualisatie en vaststelling van beleidsdocumenten. Zorg dat deze qua aard en doelstelling passend en bruikbaar is voor de ISO's in hun communicatie met de directies. Maak hierbij onderscheid tussen strategische beleidsdocumentatie enerzijds zoals bedoeld in hoofdstuk vijf van de BIO en tactisch/operationele

	documentatie anderzijds. Stel de beleidsdocumentatie ter beschikking aan de medewerkers van business en vakgroep betrokken bij de realisatie van informatiebeveiliging. Borg daarbij dat uitsluitend definitieve en vastgestelde kaders ter beschikking worden gesteld. Hiermee kan verdere invulling worden gegeven aan de stelselverantwoordelijkheid voor Informatiebeveiliging.		
Managementreactie	De bevinding is correct. Het actualiseren en aanvullen van beleid en kaders is een belangrijk aandachtspunt voor de komende twee jaar. Daarbij sluiten we aan op de eisen van nieuwe wetgeving (CBW/BIO2) en bezien we of een aanpassing van de BIO-RASCI-tabel (taakverdeling centraal – decentraal) gewenst is. Ambitie is om de strategische beleidsdocumenten, het *Stedelijk beleidskader informatiebeveiliging* en de *Organisatie van informatiebeveiliging bij de gemeente Amsterdam*, in 2025 te actualiseren. Dit wordt vervolgens aangevuld met documenten t.a.v. tactisch beleid (formeel vastgesteld en centraal beschikbaar gesteld). Communicatie naar medewerkers is onderdeel van de aanpak. Het in 2025 nieuw gevormde *Kernteam Informatiebeveiliging*, ingericht o.b.v. de aanpak van het IB-huis, is hierbij in the lead. Zodoende wordt gestuurd vanuit één optiek, doelstelling en roadmap.	Strategische beleidsdocumenten: Q4 2025 Tactisch/operationeel beleid: permanente ontwikkeling, maar kern opstellen in 2026. Einddatum gereed: Eind 2026 Follow-up audit: nader te bezien	Verantwoordelijke directie: DS&I i.s.m. DV

2. Naleving BIO is deels gerealiseerd	**PRIO 1**

Achtergrond	De stad heeft haar informatiebeveiliging in toenemende mate georganiseerd door de inrichting van stedelijke processen ten behoeve van informatiebeveiliging. Daarbij worden directies op uniforme wijze gefaciliteerd om binnen hun directies de noodzakelijke processen te organiseren. Daar hoort ook bij het borgen van taken waarbij businessdirecties aanvragen tot mutaties verstrekken aan stedelijke directies zoals directie PenO of directie Digitale Voorzieningen.

	Opzet en bestaan van BIO-controls zijn onderzocht door integrale toetsing bij vijf directies op BIO-compliant zijn van informatiebeveiliging. In het onderzoek is rekening gehouden met de gevolgen van de aanwezigheid van IT in eigen beheer.
Bevinding	In ons onderzoek is het beeld bevestigd dat de naleving deels is gerealiseerd. In de casusonderzoeken hebben we geconstateerd dat door de directies veel werkzaamheden zijn verricht ter realisatie van de naleving van de BIO-voorschriften. Echter we hebben ook geconstateerd dat er nog stappen gezet moeten worden. In bijlage 3 is zichtbaar dat slechts één thema voor de opzet een voldoende (**V**) scoort, voor negen thema's deels voldoende (**O**) en voor twee thema's onvoldoende (**X**). Bestaan hebben we eveneens voor negen thema's deels (**O**) kunnen aantonen en voor drie thema's niet (**—**) kunnen toetsen. Veel voorkomende problemen die we hebben geconstateerd zijn: • Directies hebben bij de inrichting van hun beheersmaatregelen keuzes gemaakt op basis van best effort waarbij actuele procesbeschrijvingen van stedelijke processen werden gemist. Goede aansluiting op stedelijke processen bleek problematisch. • Business-directies blijken moeite te hebben met continuering van de uitvoering van bewustwordingsactiviteiten op het gebied van informatiebeveiliging. Om de werking te kunnen toetsen, moeten wij kunnen steunen op de opzet en het bestaan. We hebben daarom de werking dan ook bij geen enkele directie kunnen vaststellen. • Over de hele linie zien we een sterke afhankelijkheid van de processen van IT-leveranciers. Dit is vooral zichtbaar bij een onderwerp als wijzigingsbeheer dat in sterke mate afhankelijk is van de releasekalenders van leveranciers. Maar ook bij BIO-controls waarvoor uitvoering de verantwoordelijkheid is van leveranciers en directies alleen via verstrekte rapportages van leveranciers informatie beschikbaar hebben over de informatiebeveiliging. • Een bijzonder issue blijkt bij leveranciers die wel beschikken over ISO-certificaten met toelichtingen via verklaringen van toepasselijkheid, maar niet over assurancerapportages (ISAE 3402, gericht op financieel administratieve systemen). In deze situaties blijkt het stedelijke beleid met beperking van assurancerapportages tot een ISAE 3402 knellend te werken. Dit is vooral het geval bij Operationele Technologie (OT). Leveranciers verstrekken met assurancerapportages informatie aan hun afnemers over de kwaliteit van specifiek getoetste informatiebeveiligingsaspecten. We hebben bij twee thema's een onvoldoende (**X**) moeten toekennen. Deze thema's lichten we hieronder in meer detail toe. • In- en uitdiensttreding (IDU) (H7.3.1): van directies wordt verlangd dat ze als onderdeel van het proces uitdienst exitgesprekken houden. In deze exitgesprekken hoort de vertrekkende medewerker gewezen te worden op de continuering van de verantwoordelijkheid voor geheimhouding. Bij geen van de directies hebben we het onderwerp aangetroffen als onderdeel van de standaardagenda voor exitgesprekken of behandeling uitdienst. Het onderwerp ontbreekt ook op de stedelijke checklist uitdienst. • Bedrijfsmiddelen (H8.1, 11.2 en 13.2): bedrijfsmiddelen worden deels centraal beheerd en verstrekt zoals telefoons en laptops en zijn deels decentraal beheerd. Tijdens het casusonderzoek bleek dat voor directies de

	instructie niet helder was welke bedrijfsmiddelen in de inventarislijst opgenomen moesten worden. Op basis van het in te vullen controldocument voor deze controls ontstaat de indruk dat van directies wordt verwacht dat ze een integrale inventarislijst van alle bedrijfsmiddelen opstellen en eigenaarschap van bedrijfsmiddelen toewijzen. In het controldocument ontbreekt instructie hoe om te gaan met het verschil in verantwoordelijkheid tussen centraal beheerde en verstrekte bedrijfsmiddelen en decentraal beheerde bedrijfsmiddelen. Ook ontbreekt in de instructie de relatie met het thema labellen/classificeren (H8.2). Beleid voor informatiebeveiliging van bedrijfsmiddelen is nog niet stedelijk beschikbaar.
Risico	Als gevolg van gebreken in de inrichting van BIO-controls op onderwerpen bestaat de kans dat informatiebeveiligingstaken voor deze onderwerpen niet zijn belegd en niet worden uitgevoerd met als mogelijk gevolg de onttrekking van middelen en datalekken. Daarnaast bestaat een risico op een inefficiënte inrichting en uitvoering van directie overstijgende processen met de door directies zelf verzonnen procesinrichtingen waardoor centraal en decentraal uitgevoerde informatiebeveiligingsmaatregelen niet op elkaar aansluiten.
Oorzaak	• Het ontbreken van helder en eenduidige informatie over de inrichting van stedelijke processen voor informatiebeveiliging. Hiermee ontbreekt voor directies een belangrijke basis en aanknopingspunt voor de inrichting van decentrale processen van informatiebeveiliging. Zie ook bevinding 1. • De overgang van programmatisch werken (implementatieperiode) naar uitvoering van informatiebeveiliging als reguliere taak verloopt soms moeizaam. Na afloop van een vaak intensieve implementatieperiode zijn er weer andere onderwerpen en programma's die aandacht vragen. Aandacht voor continuering van een eerder geïmplementeerde bedrijfsvoeringstaak blijkt dan vaak te ontbreken. • Discontinuïteit in personeelsbezetting. • In de implementatiedocumentatie is geen aandacht besteed aan de onderlinge relaties tussen BIO-controls. • Wel aanwezig stedelijk beleid gaat alleen in op administratieve IT en niet op de gevolgen van toenemende automatisering van OT. • Het ontbreken van het onderwerp continuering van de verplichting tot geheimhouding in de stedelijke checklist uitdienst. • Het ontbreken van helderheid in het controldocument Bedrijfsvoering over de informatie waarvoor een directie zelf een inventarislijst moet bijhouden en welke informatie stedelijk wordt beheerd. • Het ontbreken van een in te vullen format voor een inventaris van bedrijfsmiddelen waarmee een directie gefaciliteerd wordt in volledigheid van de vast te leggen kenmerken.
Aanbeveling	Borg adequaat bijsturen van implementatieprogramma's ter verbetering van de gemeentelijke informatiebeveiliging.

	Onderdeel hiervan kan zijn het analyseren van verbeterplannen en voortgangsrapportages op aanvaardbaarheid van de voorgenomen planning ter verbetering van informatiebeveiliging. Ga bij bijvoorbeeld onaanvaardbaar lange doorlooptijden na wat de oorzaak hiervan is en pas bijvoorbeeld pareto-analyse[4] toe. Signaleer en bespreek de oorzaken met de directies om samen tot een oplossing te komen. Pas escalatie toe naar een hoger stedelijk niveau indien het niet mogelijk is om gezamenlijk tot een oplossing te komen. Ook hiermee kan verdere invulling worden gegeven aan de stelselverantwoordelijkheid voor Informatiebeveiliging.		
Managementreactie	De bevinding wordt herkend: ▪ Er zijn directies die hun BIO-verbeterplan hebben afgerond, er zijn directies waar we goede stappen maken en er zijn directies waar het moeizaam gaat. Elk kwartaal maken we een overzicht op cluster/directieniveau dat wordt meegenomen in de kwartaalrapportages van het i-domein per cluster. Er wordt dus gemonitord en bijgestuurd, maar we moeten erkennen dat we niet altijd prioriteit krijgen bij de directies. ▪ Het afronden van een verbeterplan is een belangrijke stap, maar ook daarna is structurele aandacht nodig bij alle directies. Bij een aantal directies is een IB-jaarplan in gebruik als instrument om periodiek de status en risico's te actualiseren. Het is belangrijk om dit bij alle directies door te voeren. ▪ De aansluiting tussen centrale processen en decentrale uitvoering is niet in alle gevallen helder waardoor onduidelijkheid ontstaat voor de directies en controls tussen wal en schip kunnen vallen. In het kader van de implementatie van CBW/BIO2, waarvoor inmiddels een projectteam is gestart, zal bezien worden of andere vormen van control mogelijk en gewenst zijn. Het *Kernteam Informatiebeveiliging* is in the lead om voorstellen te doen voor de drie bullits.	Binnen welk tijdsbestek: In 2025 zal bezien worden of een aangescherpte sturing mogelijk en wenselijk is. Einddatum gereed: Aanpak monitoring: eind 2025. De feitelijke monitoring loopt de komende jaren door en wordt onderdeel van de reguliere PDCA cyclus. Follow-up audit: Nader te bezien	Verantwoordelijke directie: DS&I i.s.m. DV

[4] Een Pareto-analyse is een methode die gebruikt wordt om de belangrijkste oorzaken van een probleem of resultaat te identificeren. Deze analyse is gebaseerd op het Pareto-principe, ook wel bekend als de 80/20-regel. Volgens deze regel zou 80% van de resultaten voortkomen uit 20% van de oorzaken.

3. Onvoldoende helderheid over de verantwoordelijkheden in bijzondere situaties	PRIO 3

Achtergrond	De BIO-implementatie is gestart met het toewijzen van verantwoordelijkheden voor BIO-controls aan toenmalige directies, vastgelegd in een BIO-RASCI. De BIO-RASCI is vastgesteld door het GMT in 2022. Dit was voorafgaand aan de reorganisatie van het I-domein in juli 2022. Vervolgens is iedere directie gevraagd om zorg te dragen voor implementatie van de toegewezen BIO-controls, middels het stedelijk programma BIO-implementatie. Het stedelijk programma is geëindigd per 31 december 2023. Nadere detaillering van de wijze waarop invulling gegeven wordt aan de taken en bevoegdheden is opgenomen in de stedelijke beleidsdocumentatie voor zover actueel en aanwezig.
Bevinding	Tijdens de casusonderzoeken hebben we enkele bijzondere situaties geconstateerd waar verantwoordelijkheid voor informatiebeveiliging nog onvoldoende gewaarborgd bleek. Deze situaties hebben we hier verder toegelicht. • Het komt voor dat er applicaties gebruikt worden waarbij één business directie applicatie-eigenaar is en een andere business directie medegebruiker. Door de betrokken directies (eigenaar en medegebruiker) wordt op verschillende wijzen invulling gegeven aan de verantwoordelijkheid voor BIO-controls. Ook verstrekken applicatie-eigenaren geen rapportages aan medegebruikers waaruit de naleving van BIO-compliance blijkt. Voorbeelden zijn applicaties als ZorgNed en Smile. • Bij één van de directies was sprake van eigendomsoverdracht van applicaties. Bij de eigendomsoverdracht heeft geen overdracht van informatiebeveiligingsmaatregelen plaats gevonden waardoor de ontvangende directie geen inzicht had in uit te voeren werkzaamheden bij ontvangst van de applicaties en voor een deel van de BIO-controls de informatiebeveiliging opnieuw moest bedenken en inrichten. • Bij één van de directies bleek informatiebeveiliging deels niet aantoonbaar als gevolg van personeelswisselingen.
Risico	Als gevolg van onvoldoende duidelijkheid over de benodigde invulling van verantwoordelijkheden voor BIO-controls generiek of in specifieke situaties bestaat de kans dat de taken op het gebied van informatiebeveiliging inefficiënt en daardoor mogelijk ineffectief worden uitgevoerd met als gevolg gebreken in de informatiebeveiliging.
Oorzaak	• Er is geen beleid of procedure aangetroffen voor de wijze waarop invulling aan informatiebeveiliging moet worden gegeven in de situatie waar sprake is van medegebruikerschap van een applicatie. • Er is geen beleid of procedure aangetroffen voor de werkwijze bij overdracht van applicatie-eigendom en de bijbehorende informatiebeveiligingsmaatregelen. • Informatiebeveiliging is onvoldoende onderdeel geweest van de onboarding bij deze directie.

Aanbeveling	Biedt helderheid over taken en verantwoordelijken bij meer bijzondere situaties door een kaderstellend document op te stellen. Voorbeelden van dergelijke situaties zijn medegebruikerschap en overdracht van applicatie-eigendom. De toepassing van het inbeheernameproces kan onderdeel zijn van dit nieuwe kader.		
Managementreactie	Het is inderdaad niet geheel duidelijk wie wat moet doen in bijzondere situaties, zoals het gebruik van applicaties door meerdere directies of de overdracht van applicaties. Dit zal een onderwerp moeten zijn bij de uitwerking van het tactisch/ beleid. Nadere detaillering van verantwoordelijkheden, zodanig dat e.e.a. ook bij de bijzondere situaties helder is. Het *Kernteam Informatiebeveiliging* is in the lead.	Binnen welk tijdsbestek: Conform bevinding 1: uitwerking van het tactisch/operationeel beleid in 2026. Einddatum gereed: 2026 Follow-up audit: Nee	Verantwoordelijke directie: DS&I i.s.m. DV

Bijlage 2: Overzicht van gecontroleerde beheersmaatregelen

Symbool	Betekenis
V	Opzet, Bestaan en/of Effectieve Werking is vastgesteld.
O	Opzet, Bestaan en/of Effectieve Werking is gedeeltelijk vastgesteld.
X	Opzet, Bestaan en/of Effectieve Werking is niet vastgesteld.
—	Opzet, Bestaan en/of Effectieve Werking is niet getoetst.

Risico	Beheersmaatregelen	Opzet	Bestaan	Toelichting
R1 Als gevolg van het ontbreken van een effectief geheel van sturing en verantwoording bestaat de kans dat de gemeentelijke informatiebeveiliging kwaadwillenden de kans geeft op kunnen binnendringen in gemeentelijke systemen waar ze niet voor gerechtigd zijn waardoor gegevens gegijzeld (beschikbaarheid), verminkt (integriteit, plegen van fraude) of gelekt (vertrouwelijkheid) kunnen worden.	**IB1 Beleid, procedures en taken** De gemeente geeft met beleid en procedures nadere invulling aan de controls en overheidsmaatregelen opgenomen in de BIO en instrueert daarmee de gemeentelijke entiteiten ten aanzien van de wijze van naleving van de BIO. Beleid en procedures zijn integraal ter beschikking gesteld aan de medewerkers verantwoordelijk voor de informatiebeveiliging en naleving van de BIO voor de gemeentelijke entiteiten. Bewustwording en training is onderdeel van de communicatie over het ingestelde beleid met procedures.	O	O	**Bevinding 1** **Bevinding 3**
	IB2 Monitoring De gemeente heeft monitoring (in brede zin) ingericht ten behoeve van: • Centraal inzicht in gebreken aanwezig in decentrale beveiliging van informatie en informatiesystemen (de gemeentelijke verantwoordingsstructuur t.a.v. BIO-implementatie). • Centraal ontvangen van signalen waarvoor opvolging benodigd is • Centraal inzicht in uitgevoerde (externe) toetsingen en de daaruit verkregen resultaten).	O	O	**Bevinding 2**

Bijlage 3: Overzicht van toetsingsresultaten BIO-controls

Symbool	Betekenis
V	Opzet en/of Bestaan is vastgesteld.
O	Opzet en/of Bestaan is gedeeltelijk vastgesteld.
X	Opzet en/of Bestaan is niet vastgesteld.
—	Opzet en/of Bestaan is niet getoetst.

Thema	BIO-artikelen[5]	Opzet	Bestaan	Toelichting
1. Logische toegangsbeveiliging	6.1.2, 9.2.2, 9.2.5, 9.2.6, 9.4.1	O	O	
2. IDU	7.3.1	X	—	**Bevinding 2**
3. Bedrijfsmiddelen	8.1.1, 8.1.2, 8.1.3, 8.1.4, 11.2.5, 11.2.6, 13.2.4	X	—	**Bevinding 2**
4. Bewustwording	7.2.1, 7.2.3, 12.1.1	O	O	
5. Classificatie/labelen	8.2.1, 8.2.2, 8.2.3	O	O	
6. Privacy en bescherming P-gegevens	18.1.4	O	O	
7. Informatiebeveiligingscontinuïteit	17.1.1, 17.1.2	O	O	
8. Beheer van eisen / leveranciersbeheer	14.1.1, 15.1.2, 15.2.1, 15.2.2, 18.1.1	V	O	
9. Wijzigingsbeheer	12.1.2, 14.2.9, 14.3.1	O	O	
10. Incidentbeheer	12.4.1, 16.1.2, 16.1.5, 16.1.7	O	O	
11. Toezicht en Naleving	18.2.2, 18.2.3	O	O	
12. Delen gegevens met derden (rest)	13.2.2	O	—	

Directiespecifiek	BIO-artikelen[6]	Opzet	Bestaan	Toelichting
Informatiebeveiliging in projectmatig werken	6.1.5	V	V	

[5] 37 BIO-artikelen verdeeld over 12 thema's door I-domein in de BIO-Rasci aan de 'business', de lijndirecties, toegewezen.
[6] BIO-artikelen door I-domein toegedeeld aan een directie in aanvulling op de 37 BIO-controls verdeeld over 12 thema's