Interim-auditrapport
2024

Ministerie van Algemene Zaken

Samenvatting

Hierbij bieden wij u ons interim-auditrapport aan dat wij hebben opgesteld in het kader van onze wettelijke taak over 2024 bij het ministerie van Algemene Zaken. In dit rapport beschrijven wij de stand van zaken van bevindingen uit 2023 en signaleren we risico's en ontwikkelingen waar we uw aandacht voor vragen.

Opvolging bevindingen auditrapport 2023
In ons auditrapport over 2023 rapporteerden wij twee lichte bevindingen over het beheer. Deze bevindingen hadden enerzijds betrekking op het inkoopbeheer bij de Dienst Publiek en Communicatie (DPC) en anderzijds op de General IT Controls (GITC).

Omdat DPC het gedeelte van het inkoopbeheer waarop de ADR bevinding betrekking had heeft overgedragen aan de Rijksinkoopsamenwerking en Inhuurdesk is deze bevinding komen te vervallen.

Met betrekking tot de in 2023 gerapporteerde bevindingen over de GITC zijn uit onze werkzaamheden een aantal verbeteringen zichtbaar.

Nieuwe aandachtspunten
Uit onze werkzaamheden in 2024 is een aandachtspunt naar voren gekomen waarover wij ook in ons interim-auditrapport 2023 hebben gerapporteerd. Uit onze werkzaamheden is gebleken dat een gedeelte van de eigen interne controlewerkzaamheden van het ministerie van Algemene Zaken niet volledig en niet tijdig zijn uitgevoerd.

Een ander aandachtspunt voor onze controle betreft de versnelde verhuizing van het ministerie. Hierbij zijn door ons aanvullende risico's onderkend. Hiervoor zullen wij aanvullende werkzaamheden uitvoeren.

Inhoudsopgave

Inleiding

Hierbij bieden wij u ons interim-auditrapport aan dat wij hebben opgesteld in het kader van onze wettelijke taak over 2024 bij het ministerie van Algemene Zaken. In dit rapport beschrijven wij de voortgang ten aanzien van de bevindingen uit voorgaande periodes en signaleren wij risico's en ontwikkelingen waar wij uw aandacht voor vragen.

Met ingang van 2024 hanteert de ADR een nieuwe presentatiewijze om het relatieve belang van de gerapporteerde bevindingen uit het onderzoek naar het begrotingsbeheer, het financieel beheer, de materiële bedrijfsvoering en de daartoe bijgehouden administraties weer te geven. In plaats van een score naar ernst van de bevinding, kennen wij voortaan een prioritering toe aan de door ons gesignaleerde bevindingen. Om snel inzicht te geven in het geheel van onze bevindingen, presenteren wij deze voortaan niet alleen in de vorm van een tabel maar ook in een zogenaamde 'heatmap', waarbij de assen gevormd worden door de inschattingen van kans en impact.

Onze prioritering is de resultante van een inschatting van de kans dat een risico zich voordoet, en de impact hiervan op het financieel-, materieel- en IT-beheer gerelateerd aan de financiële verantwoording. Hierbij wegen wij nadrukkelijk mee in welke mate de door de organisatie getroffen beheersmaatregelen doeltreffend zijn in het mitigeren van het risico. Het is de verantwoordelijkheid van het management om de door ons gesignaleerde risico's in het grotere geheel te plaatsen van alle risico's die door de organisatie beheerst moeten worden.

In ons auditrapport 2023 hebben wij een aanzet gemaakt in het beschrijven van de kans en impact van onze bevindingen. Op basis van de actuele stand van zaken hebben wij een prioritering toegekend aan deze bevindingen die wij in dit interim-auditrapport hebben gepresenteerd volgens de nieuwe rapportagewijze. Per jaareinde zullen wij deze bevindingen uit 2023 opnieuw evalueren en nagaan of dit leidt tot wijzigingen, bijvoorbeeld als gevolg van getroffen beheersmaatregelen. De uitkomsten hiervan worden opgenomen in ons auditrapport 2024 dat in maart 2025 verschijnt.

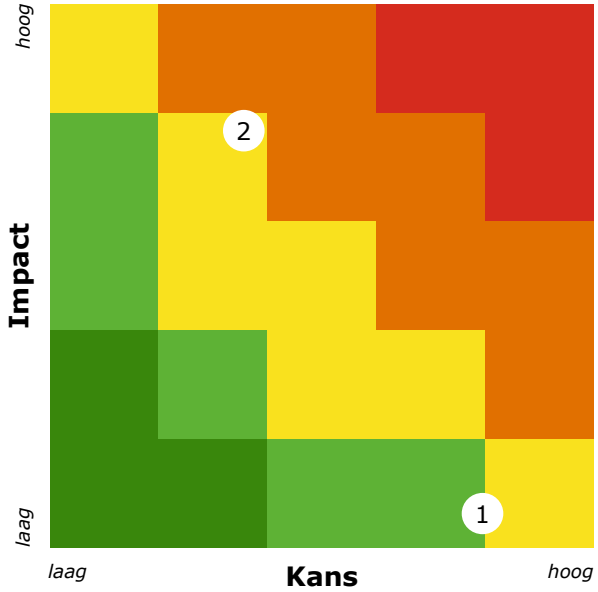
Overzicht voortgang bevindingen 2023

Financieel beheer en jaarrekening

1	Inkoopbeheer DPC		↙

IT Beheer

2	GITC		=



↗ *Verslechterd* ↙ *Verbetering zichtbaar* = *Ongewijzigd*

Voortgang bevindingen 2023

In ons auditrapport over 2023 rapporteerden wij twee lichte bevindingen over het beheer. Deze bevindingen hadden betrekking op:

- Het inkoopbeheer van DPC
- De General IT Controls (GITC:
  - Gebruikersbeheer (SQL-database, en de Active Directory).
  - Datafixes.
  - Beveiliging van componenten.

Inkoopbeheer DPC

De bevinding ten aanzien van het inkoopbeheer bestond uit twee onderwerpen:

- Ontoereikende dossiervorming bij Europese aanbestedingen.
- Onrechtmatigheden als gevolg van overbruggingsovereenkomsten.

Doordat de overbruggingsovereenkomsten ook voor 2024 nog deels van kracht zijn zal deze bevinding (die ook deels een externe oorzaak heeft) ook voor 2024 van toepassing zijn. In het verbeterplan van AZ (inclusief DPC) zijn maatregelen beschreven die de registratie van de uit de overbruggingen voortvloeiende onrechtmatigheid moet verbeteren. De werking daarvan kunnen wij pas vaststellen bij de werkzaamheden met betrekking tot de jaarrekeningcontrole.

Doordat de Europese aanbestedingen sinds 2024 niet meer door DPC maar door de Rijksinkoopsamenwerking (RIS) worden uitgevoerd is ook de dossiervorming daaromtrent belegd bij de RIS en is dit deel van de bevinding over het inkoopbeheer als opgelost beschouwd.

GITC

<u>Gebruikersbeheer</u>

AZ heeft in 2024 een controle ingesteld op de leden van groepen binnen Active Directory (AD) voor zowel reguliere gebruikers als beheerders waarbij indien nodig correcties plaatsvinden. AZ heeft daarmee onze aanbeveling uit 2023 opgevolgd.

AZ is bezig met de implementatie van een centrale logmanager waarna en er periodieke monitoring gaat plaatsvinden op onpersoonlijke accounts.

Zowel beheerders- als reguliere rechten worden niet definitief, maar periodiek uitgegeven. Na afloop van deze periode vindt verificatie plaats of de rechten nog benodigd zijn.

<u>Wachtwoordbeheer</u>

In oktober 2024 is het wachtwoordbeleid van AZ aangepast van minimaal 8 karakters naar minimaal 12 karakters en daarmee wordt aan de vereisten van het GITC-normenkader van de ADR voldaan.

Voortgang bevindingen 2023

Beveiliging van Componenten
Bij AZ zijn voor Windows verschillende aandachtspunten rondom de Beveiliging van Componenten. AZ gebruikt het Nationaal Cyber Security Centrum (NCSC) als enige bron voor meldingen van nieuwe kwetsbaarheden, daarnaast geeft AZ tevens aan gebruik te maken van meldingen vanuit additionele bronnen van de leveranciers. Het consistent bijhouden van kwetsbaarheden en de monitoring hiervan heeft de ADR nog niet in de praktijk kunnen vaststellen. Volgens de documentatie is er een onderhoudscontract met een leverancier, maar de details en afspraken zijn niet vastgelegd in een beleid. De Chief Information Security Officer (CISO) heeft de bevoegdheid om een spoedpatchproces te starten, maar het is onduidelijk hoe vaak en systematisch kwetsbaarheden door de CISO worden onderzocht.

Daarnaast monitort het departement niet alle systemen actief. Er zijn wel controles ingeregeld en het netwerktoegangspunt wordt gemonitord, maar AZ voert onvoldoende monitoring uit op de onderliggende componenten zoals het Operating System (OS). Hierdoor bestaat een kans dat kwetsbaarheden worden misbruikt zonder dat dit wordt opgemerkt. Dit heeft potentieel een hoge impact.

Kwetsbaarheden op OS-niveau monitort het CISO-office op basis van de tool Cortex XDR. Bij openstaande kwetsbaarheden wordt er een ticket voor de Backoffice aangemaakt om dit op te lossen. Na iedere (Windows) updateronde wordt er een ticket aangemaakt voor het CISO-office om te valideren of alle kwetsbaarheden gepatcht zijn. AZ gaat in de komende jaren SOC-monitoring inrichten. In 2025 wordt gestart met de implementatie van een Security Incident & Event Management (SIEM), waarop de in te richten SOC-dienstverlening aansluit.

Datafixes
Datafixes betreft de mogelijkheid om data rechtstreeks in de database te muteren zonder gebruik te maken van de applicaties. In dit proces is bij AZ geen functiescheiding aanwezig. De database administrator is zowel verantwoordelijk voor het uitvoeren van mutaties op de database als voor het rapporteren over deze wijzigingen.

Het advies is om functiescheiding in te richten voor dit proces. AZ heeft aangegeven dit risico te accepteren. Wij zullen dit punt als aandachtspunt blijven monitoren.

Aandachtspunten 2024

Uitvoeren interne controles door Algemene Zaken

In het 'Handboek administratief beheer en controleverbanden' onderkent AZ het risico op fouten in juistheid en rechtmatigheid in de administratie alsmede de verantwoording die hierover moet worden afgelegd. Om dit risico te mitigeren zijn in het handboek controles beschreven die maandelijks vóór en na de maandafsluiting moeten worden uitgevoerd.

Wij hebben vastgesteld dat de controles vooraf niet tijdig zijn vastgelegd (met uitzondering van augustus). Hierdoor is het niet mogelijk om vast te stellen of de betreffende controles tijdig zijn uitgevoerd. De controles na de maandafsluiting zijn eveneens uitgevoerd waarbij door ons is vastgesteld dat de vastlegging hiervan niet tijdig heeft plaatsgevonden.

Deze controles zijn van belang om de administratie vrij te houden van fouten en om eventuele fouten tijdig te herstellen. Daarnaast is deze controle van belang voor de afstemming van administratieve standen, dit mede in verband met de externe rapportageplicht.

Naast de maandelijkse controles zijn in het handboek periodieke controle beschreven. Het handboek schrijft voor dat deze periodieke controles uitgevoerd dienen te worden na het afsluiten van periode 8 (maandafsluiting augustus) en periode 12 (jaarafsluiting). Deze periodieke controles bestaan uit:

- bestandscontroles,
- verbandscontroles en
- overige controles (onder andere ten aanzien van belastingen en WKR)

Door AZ is aangegeven dat de controle na 8 maanden, in verband met onderbezetting van de afdeling ASC, niet worden uitgevoerd.

Risico

Door het niet (tijdig) uitvoeren van de eigen interne controles loopt het ministerie het risico dat fouten niet of niet tijdig worden ontdekt en gecorrigeerd. Dit kan uiteindelijk leiden tot het opleveren van een niet getrouwe jaarrekening. Als de controle na 12 maanden wel (op een gedegen manier) wordt uitgevoerd kan dit risico worden beperkt. Doordat de controle na 8 maanden niet is uitgevoerd heeft dit wel tot gevolg dat de controle na 12 maanden, naar verwachting, meer tijd zal vergen. Wij adviseren dan ook om in 2025 te bezien of er (extra) capaciteit kan worden vrijgemaakt voor de uitvoering van de controle na 8 maanden.

Verhuizing ministerie van Algemene Zaken

In 2020 is gestart met de renovatie van het Binnenhof. In 2022 werd bekend dat de tijdelijke locatie voor het ministerie van Algemene Zaken de Bezuidenhoutseweg 73 zou worden. De benodigde verbouwing hiervoor werden niet tijdig uitgevoerd. In de zomer van 2024 is door de gemeente Den Haag, met het oog op veiligheid, besloten dat het Binnenhof niet langer gebruik mocht worden. Dit was aanleiding om de eerder geplande gefaseerde verhuizing naar de Turfmarkt met spoed naar voren te halen.

Risico

Doordat de opgestelde verhuisplannen voor een ordelijke verhuizing zijn aangepast, onderkennen wij aanvullende risico's:

- Continuïteit van de IT ondersteuning inclusief de beveiliging van de systemen.
- Hogere kosten, zonder budgettaire dekking, doordat verbouwingskosten worden doorbelast aan AZ.
- Vermissing van Kunst en ICT-middelen.
- Extra uitgaven, zonder budgettaire dekking (o.a. in verband met aanpassingen in de ICT).
- Afwijken van aanbestedingsregels als gevolg van de spoed die voortvloeit uit de eerdere verhuizing. Waardoor er sprake is van onrechtmatige uitgaven.

Ten aanzien van de hogere kosten als gevolg van de benodigde verbouwingen op de Turfmarkt is door het ministerie aangegeven dat deze niet voor rekening komen van het ministerie maar ten laste komen van het Rijksvastgoedbedrijf (RvB). Ten aanzien van de kunstcollectie en de ICT-middelen heeft Algemene Zaken in opzet voldoende waarborgen genomen om het risico op vermissing hiervan te mitigeren. We vragen aandacht voor het naleven van deze beschreven waarborgen om het risico ook in de praktijk te beperken.

Met betrekking tot de extra uitgaven en het naleven van de aanbestedingsregels zullen wij aanvullende werkzaamheden uitvoeren bij de jaarrekeningcontrole begin 2025.

Privacy

Rijksbreed AVG onderzoek

De rijksoverheid verwerkt bij de uitvoering van haar publieke taken grote hoeveelheden persoonsgegevens van burgers. Zij draagt daarom een grote verantwoordelijkheid om deze gegevens op een gepaste manier te behandelen en te beschermen. Sinds de Algemene Verordening Gegevensbescherming (AVG) op 25 mei 2018 van kracht is geworden, werkt de rijksoverheid gestaag aan implementatie en naleving. Een tekort aan privacybescherming kan nadelige gevolgen hebben voor de persoonlijke levenssfeer van de burger door identiteitsdiefstal, openbaarmaking en/of misbruik van hun persoonlijke gegevens met alle mogelijke gevolgen van dien.

Uit rijksbrede AVG-onderzoeken van de ADR in 2019, 2020 en 2022 bleek de implementatie en naleving daarvan nog een uitdaging, hoewel de Rijksoverheid de laatste jaren heeft gewerkt aan een hoger volwassenheidsniveau. De ADR voert op verzoek van CIO-Rijk namens de leden van het CIO-beraad in 2024 opnieuw een rijksbreed AVG-onderzoek uit met als aandachtspunten de inrichting en implementatie van privacy by design & default (privacywaarborgen als standaard functionaliteit in nieuwe IT-voorzieningen), de monitoring en opvolging van de resultaten uit Data Protection Impact Assessments (DPIA's - maatregelen om de geconstateerde privacy risico's bij de verwerking van persoonsgegevens te mitigeren). Het onderzoek resulteert in departementale deelrapporten en een geaggregeerd overkoepelend rapport van de belangrijkste bevindingen uit het onderzoek alsmede aangetroffen goede voorbeelden voor de interdepartementale ontwikkeling en samenwerking.

Voor Algemene Zaken valt op dat:

- Het register van werkwerkingsactiviteiten actueel en volledig is. Het DPIA-dashboard was op het moment van het Rijksbrede AVG onderzoek niet actueel.
- De noodzakelijke DPIA’s zijn uitgevoerd.
- De controle- en monitoringsactiviteiten door de Privacy Officer zijn uitgevoerd.
- Verzoeken van betrokkenen zijn afgehandeld.

Implementatie NIS2 en Cyberbeveiligingswet

NIS2 en Cyberbeveiligingswet
De *Network and Information Security Directive* (NIS2) is een EU-richtlijn die gericht is op het creëren van een hoog gezamenlijk niveau van cyberbeveiliging in de Europese Unie. De richtlijn wordt momenteel omgezet in nationale wetgeving: de cyberbeveiligingswet. Deze wet gaat gelden voor de meeste organisaties van de rijksoverheid en bevat een zorg- en meldplicht, die strikte eisen aan de leden van het bestuur van de organisaties stelt. Naar verwachting wordt de cyberbeveiligingswet in de loop van 2025 van kracht. Van de rijksoverheid mag worden verwacht dat ze zorgt voor het naleven van deze wet zodat de overheid weerbaar is tegen cyberrisico's die de verwerking van gevoelige informatie en de voorbeeldfunctie van de rijksoverheid met zich meebrengen. Het niet naleven kan leiden tot (ernstige) verstoring van de dienstverlening, bestuurlijke boetes, imagoschade en verminderd vertrouwen van burgers in de rijksoverheid. Het is daarom van belang tijdig inzichtelijk te maken aan welke eisen (nog niet volledig) wordt voldaan en waar nodig aanvullende maatregelen te treffen.

Voor het Ministerie van Algemene Zaken valt op dat:
- Een GAP-analyse is uitgevoerd om inzichtelijk te maken aan welke maatregelen wel of niet wordt voldaan, maar deze is niet specifieke toegespitst op NIS2; Algemene Zaken is momenteel bezig met een inventarisatie hiervan. Naar verwachting is deze in het eerste kwartaal van 2025 afgerond
- Het departement beschikt over een plan van aanpak, maar deze is niet specifiek gericht op de vereisten van de NIS2 richtlijn en nog niet alle plannen zijn bewerkstelligd. Zodra de in het vorige punt benoemde inventarisatie is afgerond, zal aansluitend een specifiek plan van aanpak worden opgesteld met betrekking tot de implementatie van de nog benodigde maatregelen in het kader van NIS2.
- Er is (nog) geen capaciteit of budget beschikbaar om de benodigde maatregelen vanuit de NIS2 richtlijn te implementeren aangezien de wetgeving nog niet van kracht is; Bij het opstellen van het plan van aanpak zal ook duidelijk worden hoeveel capaciteit/budget daarvoor nodig is.
- De NIS2 richtlijn wordt besproken op bestuursniveau.

Categoriemanagement Dienst Publiek en Communicatie (DPC)

Het managen van 22 onderkende inkoopcategorieën is in het Rijksinkoopstelsel belegd bij de verschillende ministeries. De DPC is binnen dit stelsel de categoriemanager voor de inkoopcategorie communicatie.

Het ministerie van Binnenlandse Zaken is verantwoordelijk voor de organisatie van dit stelsel. De ADR heeft voor vijf inkoopcategorieën onderzocht hoe het inkoopproces is georganiseerd, en welke overeenkomsten en verschillen zichtbaar zijn in de werkwijzen van de verschillende categoriemanagers. Daarnaast zijn wij nagegaan hoe de monitorings- en toezichtsrelatie met stakeholders in dit stelsel is ingericht.

Voor Algemene Zaken, valt op dat:

- DPC het inkoopproces grotendeels heeft overgedragen aan de Rijksinkoopsamenwerking (RIS). Hierdoor wordt gebruik gemaakt van schaalvoordelen en de expertise van deze organisatie waardoor de kans op onrechtmatigheden in het inkoop- en aanbestedingsproces afneemt.
- DPC is afhankelijk van informatie van de leveranciers voor wat betreft de monitoring van uitnutting van maximale waardes uit de raamovereenkomsten. DPC heeft geen mogelijkheid om de door de leveranciers aangeleverde gegevens te verifiëren.

Duurzaamheid

Op grond van de Corporate Sustainability Reporting Directive (CSRD) zijn vanaf 2024 steeds meer bedrijven verplicht te rapporteren over hun impact op mens en klimaat. De CSRD is niet verplicht voor de overheid.

Om meer zicht te krijgen op de huidige diversiteit in duurzaamheidsverslaggeving en een beter beeld te vormen over het benodigde ontwikkelpad naar effectieve en efficiënte duurzaamheidsverslaggeving binnen het rijk, voeren wij in 2024 een inventariserend onderzoek uit op basis van de gepubliceerde gegevens over 2023.

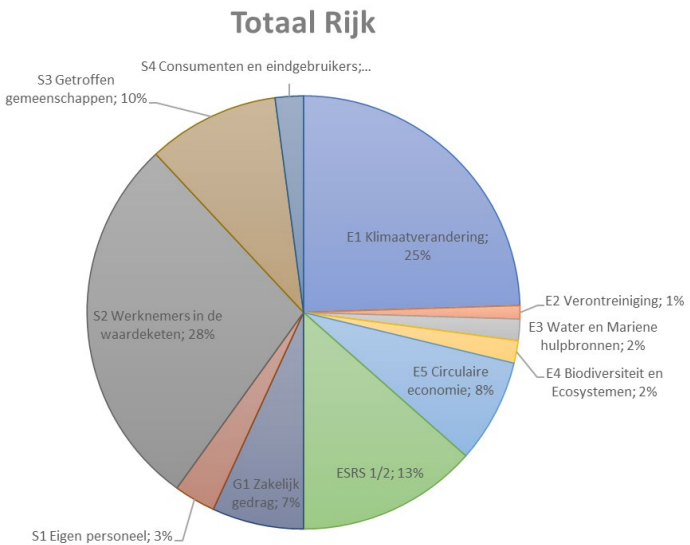
Uit onze inventarisatie komt naar voren dat over alle thema's uit de European Sustainability Reporting Standards (ESRS), die de kern vormen van de rapportageverplichtingen onder de CSRD, ergens vanuit de rijksoverheid gerapporteerd wordt. Er zijn wel duidelijke verschillen in de mate van aandacht voor de verschillende thema's. Zo wordt er bijvoorbeeld veel gerapporteerd over klimaatverandering en sociale aspecten, maar aanzienlijk minder over verontreiniging en biodiversiteit. Ook verschilt de aandacht per departement voor bepaalde thema's, afhankelijk van de beleidsmatige zwaartepunten van elk departement. Er zijn ook witte vlekken in de rapportages die niet verklaard kunnen worden vanuit het beleidsmatige karakter van de departementen.

De formulering van de ESRS-thema's, die ontworpen is voor bedrijven, sluit niet altijd goed aan bij de terminologie die binnen de rijksoverheid wordt gehanteerd. Mede hierdoor vinden we op ESRS gebaseerde zoektermen in onze data-analyse niet altijd terug in de onderzochte rapportages. De wél gevonden verslaggeving over duurzaamheid is verspreid over verschillende soorten rapportages.

Waar de CSRD zich vooral richt op het rapporteren van de negatieve impact van ondernemingen op duurzaamheid, richt het beleid van de rijksoverheid zich meer op het actief en positief beïnvloeden van duurzaamheidsthema's. Deze focus is niet onverenigbaar met de ESRS, maar vraagt wel een vertaling.

In grafieken op de volgende pagina staat de relatieve verdeling van de door het Rijk gerapporteerde informatie over de verschillende ESRS-thema's. Het beeld van AZ was niet representatief enerzijds omdat AZ een beleidsarm departement is met weinig ESRS thema's en anderzijds omdat we daar alleen de begroting en het jaarverslag in de analyse hebben meegenomen. AZ heeft inmiddels het certificaat voor de CO2-prestatieladder verkregen.

Duurzaamheid



Verantwoording interim-auditrapport

In dit rapport doen wij tussentijds verslag van de belangrijkste uitkomsten van de werkzaamheden van onze wettelijke taak over de eerste maanden van 2024 voor begrotingshoofdstuk III. Wij verrichten deze werkzaamheden als interne auditdienst van het Rijk conform artikel 6 van het Besluit ADR. Daarbij wordt aangetekend dat onze onderzoeken zich in wisselende stadia van uitvoering bevinden. Onze interim-bevindingen geven geen volledig tussentijds beeld van de stand van zaken, maar zijn afhankelijk van de bij elk departement passende mix van procesgerichte en cijfermatige controles voor zover deze op dit moment zijn uitgevoerd en geëvalueerd. Onze definitieve bevindingen, die in maart 2025 worden gerapporteerd in het auditrapport 2024, kunnen daarom afwijken van onze tussentijdse uitkomsten.

In dit interim-auditrapport willen wij met name bevindingen en risico's signaleren die de aandacht behoeven zodat in 2024 nog maatregelen ter verbetering kunnen worden getroffen. Wij focussen ons daarbij op de bevindingen in het beheer. In dit interim-auditrapport melden we ook eventuele significante tekortkomingen in de interne beheersing die wij tot dusverre op basis van onze controlewerkzaamheden hebben geïdentificeerd.

Onze controle is gericht op het verstrekken van een oordeel bij de financiële overzichten over het gehele jaar 2024. Wij betrekken hierbij de interne beheersing die voor het opstellen van de financiële overzichten van belang is. Wij geven geen oordeel over de effectiviteit van de interne beheersing.

Doel en doelgroepen

Dit interim-auditrapport is opgesteld voor de minister, de staatssecretaris en de secretaris-generaal van het ministerie van Algemene Zaken en wordt tevens verstrekt aan de leden van het audit committee, de directeur Financieel-Economische Zaken en de Algemene Rekenkamer.

De Auditdienst Rijk is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor het ministerie van Algemene Zaken. De voorschriften uit de Wet open overheid gelden voor openbaarmaking van dit rapport. De minister van Financiën stuurt elk halfjaar een overzicht naar de Tweede Kamer met de titels van door de Auditdienst Rijk uitgebrachte rapporten.

Ondertekening

Plaats: Den Haag

Datum: 2 december 2024

Handtekening:

Colofon

Interim-auditrapport 2024
ministerie van Algemene Zaken

Datum
2 december 2024

Kenmerk
2024-0000542953

Auditdienst Rijk
Korte Voorhout 7
2511 CW Den Haag