Auditdienst Rijk
Ministerie van Financiën

Interim-auditrapport 2022 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Definitief

Colofon

Titel	Interim-auditrapport 2022 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties Koninkrijksrelaties (IV), Binnenlandse Zaken en Koninkrijksrelaties (VII) en het Gemeentefonds (B), Provinciefonds (C) en het BES-fonds (H) en ter informatie: Staten Generaal (IIA), Overige Hoge Colleges van Staat en Kabinetten van de Gouverneurs (IIB)
Kenmerk	2022-0000255026
Inlichtingen	Auditdienst Rijk Korte Voorhout 7 2511 CW Den Haag

Inhoud

1 Inleiding

1.1 Algemeen

In dit rapport doen wij tussentijds verslag van de uitkomsten van de werkzaamheden die wij als interne auditdienst van het Rijk in het kader van onze wettelijke taak over het jaar 2022 bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties hebben verricht. Wij merken hierbij op dat dit rapport nog geen volledig beeld schetst over 2022. Onze definitieve bevindingen, die in maart 2023 worden gerapporteerd in het auditrapport 2022, 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 2022 nog maatregelen ter verbetering kunnen worden getroffen. Wij focussen ons daarbij op de bevindingen in het beheer.

1.2 Doel en doelgroepen

Het rapport is opgesteld voor de minister en de secretaris-generaal van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en wordt tevens verstrekt aan de leden van het audit committee, de directeur Financieel-Economische Zaken en de ambtelijke leiding van de Hoge Colleges van Staat.

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdrachten 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 de door de ADR uitgebrachte rapporten naar de Tweede Kamer.

1.3 Leeswijzer

Dit rapport is als volgt ingedeeld:

- De opvolging van de bevindingen 2021 uit het onderzoek naar het begrotingsbeheer, het financieel beheer, de materiële bedrijfsvoering en de daartoe bijgehouden administraties (hoofdstuk 1);
- Nieuwe bevindingen (hoofdstuk 2)
- Nieuwe ontwikkelingen in het beheer en overige onderwerpen (hoofdstuk 3).
- De opvolging van de bevindingen 2021 Staten Generaal (hoofstuk 4)

2 Follow-up bevindingen samenvattend auditrapport 2021

2.1 Inleiding

Als onderdeel van onze wettelijke taak onderzoeken wij of de door ons geselecteerde processen van financieel- en materieelbeheer voldoen aan de normen uit de comptabele wet- en regelgeving. Op het hoogste niveau geldt dat het financieel- en materieelbeheer voldoet aan de eisen van rechtmatigheid, ordelijkheid, controleerbaarheid en dat het beheer zo doelmatig mogelijk wordt ingericht. Deze eisen zijn verder uitgewerkt en samengevat in de baseline financieel beheer en materieelbeheer van het ministerie van Financiën.
Bij evaluatie van onze bevindingen hanteren wij drie categorieën: licht, gemiddeld en ernstig. Dit onderscheid geeft de impact van de bevinding weer op basis van gewicht en frequentie.

In dit hoofdstuk behandelen wij de follow-up van de bevindingen die wij medio maart 2021 hebben gerapporteerd in ons samenvattende auditrapport 2021.

Net als in 2021 heeft BZK in 2022 het verbetertraject verder doorgezet. Met hulp van de monitoringscommissie worden verbeterplannen ten uitvoer gebracht en krijgen de acties ook de aandacht die het nodig heeft.

2.2 Voortgang bevindingen in het beheer uit 2021

In onderstaande tabel wordt een overzicht gegeven van de bevindingen m.b.t. het financieel- en materieelbeheer ultimo 2021.

Figuur 1: overzicht bevindingen BZK per ultimo 2021

Bevinding	Verantwoordelijk organisatie-onderdeel	2020	2021	Ontwikkeling 2022
Zorgwekkende situatie over proces van informatiebeveiliging	SSO-CN	●	■	Informatiebeveiliging bij krijgt meer structuur en houvast
Juist, tijdig en volledig registreren van beschikkingen en opdrachten verbeterd, voorschottenbeheer nog aandachtspunt	BZK-Kern	■	●	Verbeteringen voorschottenbeheer voortvarend opgepakt
Interne controle financieel beheer schiet te kort	BZK 2		●	Let op voortgang verbeteracties interne controle
Structureel versterken IT beheer blijft noodzakelijk	SSC-ICT	●	●	Verbeteringen op gebied van beveiliging van componenten naar aanleiding van transitieplan zijn zichtbaar
Onzekerheid volledigheid opbrengsten BRP-berichtenverkeer blijft bestaan	RvIG		●	Volledigheid van opbrengsten is afhankelijk van uitkomsten assurance-onderzoek

● licht ■ gemiddeld ▲ ernstig √ opgelost

Wij zullen in de navolgende paragrafen per bevinding ingaan op de voortgang en de stand van zaken.

2.2.1 *SSO-CN Informatiebeveiliging krijgt meer structuur en houvast*

Over 2021 hebben wij een gemiddelde bevinding gerapporteerd inzake het proces van informatiebeveiliging. Wij constateren dat de verbeteractie in 2022 gedegen is opgepakt. Met het verbeteren van de benodigde IB-structuur en het opstellen van een informatiebeveiligingsjaarplan zijn door SSO-CN belangrijke mijlpalen behaald voor het realiseren van een toekomstig effectief functionerend proces van informatiebeveiliging. SSO-CN is onder leiding van een tijdelijk projectleider ICT volop gefocust op het oplossen van de IT-bevindingen uit 2021 aan de hand van het daartoe opgestelde 'Activiteitenplan IB op orde SSO-CN'.

Uit ons tussentijds IT-onderzoek blijkt dat door SSO-CN belangrijke stappen zijn gezet met het opzetten van de benodigde IB-structuur ter verbetering van de informatiebeveiliging. Zo heeft SSO-CN op basis van een risicoanalyse beheersingsmaatregelen in kaart gebracht, IB-processen beschreven en zijn de te treffen maatregelen geïmplementeerd in de generieke SSO-CN IT-beheerprocessen. Tegelijkertijd is binnen SSO-CN gewerkt aan het op niveau brengen van de security awareness en is vormgegeven aan het informatiebeveiligingsjaarplan.
Hiermee is de vereiste PDCA[1]-cyclus voor het proces van informatiebeveiliging in opzet (nagenoeg) gereed voor het in de praktijk operationaliseren en het frequent doorlopen van de Do, Check en Act-fasen van deze cyclus. Tijdens ons bezoek aan SSO-CN hebben wij het opstarten van de PDCA-cyclus van de IB waargenomen. De praktijk moet duidelijk maken of de in gang gezette verbetermaatregelen effect gaan ressorteren.

Een positieve ontwikkeling is de recente voltooiing van de migratie van de gemeenschappelijke SSO-CN IT-applicaties naar afname van IT-diensten uit de cloud, omdat dit de IT-capaciteit ontlast. Tegelijk is hiermee het dreigingsvlak van Cyber-risico's voor SSO-CN toegenomen en hebben de bedreigingen vanaf het internet naar SSO-CN een andere dimensie gekregen. Van belang is dat voldoende kennis en kunde aanwezig is om cloud-omgevingen in te richten, afspraken te maken met cloud providers en het gebruik en beveiliging stringent te bewaken en te monitoren.

Relatie tussen SSO CN als IT-dienstverlener en afnemers (RCN-organisaties) wordt aan gewerkt en besprekingen ter verbetering zijn gestart
Het SSO-CN heeft in 2022 richting de deelnemende klantorganisaties stappen gezet om de kwaliteit van het proces van *Demand and Supply* te verbeteren. De afnemende RCN-organisaties (de deelnemende klantorganisaties van SSO CN) zijn zelf verantwoordelijk voor de informatiebeveiliging van hun eigen specifieke IT-applicaties en hebben hun eigen IT-aspiraties voor het optimaliseren van de bedrijfsprocessen. De recent opgezette reguliere tafel-overleggen op strategisch-, tactisch- en operationeel niveau zijn een eerste aanzet voor de diverse geledingen om met elkaar in gesprek te gaan. Uit de door ons gevoerde interviews blijkt dat deze overleggen als positief worden ervaren.

Het moment komt voor SSO-CN, met het op orde brengen van het eigen IT-beheer, dan ook dichterbij om in gezamenlijkheid met de klantorganisaties meer concretere, klant-specifieke afspraken te maken over het aanbod aan IT-diensten (op het gebied van *IT infrastructure services* en *Application Hosting*) en over de kwaliteit van deze geleverde IT-diensten, inclusief het gewenste niveau van de IT-security. Het meedenken van SSO-CN over de IT-aspiraties van de afnemende

[1] Plan-do-check-act

klantorganisaties en het daarop vervolgens aansluiten op de ingezette IT-strategieën kan leiden tot een meer bestendige toekomstvisie en zo mogelijk tot betere onderlinge samenwerking. Een overkoepelend en open overleg, over het niveau van de IT-beveiliging ten behoeve van de eigen IT-infrastructuur, het gevoerde IT-beheer en over de eigen IT-applicaties van de deelnemende klantorganisaties, is door het organiseren van reguliere tafel-overleggen in 2022 opgestart. SSO-CN heeft in het verleden aangegeven over een geringe IT-capaciteit te beschikken en tevens over te weinig bevoegdheden jegens deelnemende klantorganisaties. Dit zijn complicerende factoren voor de effectiviteit van de samenwerking in de IT-dienstverlening.

2.2.2 BZK Kern: Verbeteringen voorschottenbeheer voortvarend opgepakt

BZK heeft de bevinding over de verlening van voorschotten aan de agentschappen voortvarend opgepakt. Het beleid is aangescherpt en er is een plan van aanpak opgesteld om de uitvoering daarvan te monitoren. Als onderdeel van dat laatste heeft zij onlangs een eerste toets op 24 dossiers uitgevoerd. De komende periode gaan wij de door BZK uitgevoerde maatregelen toetsen hierop.

In 2022 is BZK gestart met het bouwen van de subsidie-applicatie 'Digitale Subsidie Assistent' met geautomatiseerde controles. Momenteel wordt een pilot gedraaid met enkele subsidies. Wij hebben kennisgenomen van deze ontwikkeling en verwachten een verbetering ten opzichte van de huidige handmatige verwerking. Het is de bedoeling om later ook de verwerking van de bijdragen in een soortgelijke applicatie genaamd 'Digitale Bijdrage Assistent' te ondersteunen. Dit zal naar verwachting het voorschottenbeheer agentschappen ten goede komen.

2.2.3 BZK2: Let op voortgang verbeteracties interne controle

Wij hebben over 2021 gerapporteerd dat de interne controle van BZK2 tekortschoot op het gebied van ordelijkheid en controleerbaarheid van de financiële administratie en het IT-beheer van het financiële systeem. In reactie op onze bevindingen heeft BZK2 verbeteracties in gang gezet, die in opzet voldoende zijn.

Wij vragen aandacht voor de voortgang van de verbeteracties op de contractadministratie, gebruik van spendanalyses, onderbouwing prestatieverklaring en het IT beheer van het financieel systeem. Wij adviseren om deze eerder gerapporteerde onderwerpen, inhoudelijk en voor wat betreft voortgang ook proactief en expliciet in het bijpassende bestuurlijk niveau te bespreken met als doel in de praktijk adequate invulling te geven aan het interne financieel beheer bij BZK2.

2.2.4 SSC-ICT: Verbeteringen op gebied van beveiliging van componenten naar aanleiding van transitieplan zichtbaar

Afgelopen periode is door SSC-ICT een grootschalig en meerjarig transitieplan ten uitvoer gebracht om de bevinding inzake de 'beveiliging van componenten' op te lossen. Dit transitieplan is per april 2022 afgerond. Met het beëindigen van de transitie zijn de lopende projecten afgerond of verder belegd in de lijn. Nog niet alle projecten zijn momenteel afgerond en een aantal belangrijke mijlpalen moeten nog opgeleverd worden. Wij zien dat er in de afgelopen periode aantoonbaar stappen zijn gezet in het verbeteren van de interne beheersing en voortgang is geboekt met het wegnemen van de audit bevindingen. Zo zien we dat binnen SSC-ICT gedurende 2021 en 2022 de eerste lijn afdelingen verder ondersteund zijn bij het wegnemen van bevindingen door de inrichting van een tweede lijn (IB/IC teams). Daarnaast wordt de voortgang en inhoud bewaakt door een derde lijn (interne audit afdeling).

Een aantal belangrijke mijlpalen, waaronder implementatie van verschillende security baselines en implementatie van monitoring voortkomend uit het transitieplan moeten gedurende 2022 en begin 2023 nog verder geïmplementeerd dan wel opgeleverd worden. Dit is ook in lijn met de door ons tot zover uitgevoerde werkzaamheden. De eerder door ons geconstateerde tekortkoming op het gebied van 'beveiliging van componenten' is daarmee nog niet volledig opgelost.

Wij merken op dat bij de maatregelen voor het verbeteren van de interne beheersing de focus vooral heeft gelegen op de systemen die de ADR onderzocht heeft vanuit de wettelijke controletaak. SSC-ICT zal zelf in overleg met de eigenaren van de verschillende systemen een keuze moeten maken wat de belangrijkste systemen zijn die gemonitord moeten worden. Ook moet duidelijk zijn wat de eisen zijn aan deze monitoring. Daarbij is het van belang dat de tweede- en derde lijn afdelingen zich niet te veel beperken tot de door de ADR geconstateerde bevindingen, maar ook steeds meer zelf mogelijke bevindingen signaleert en tijdig opvolgt.

2.2.5 RvIG: volledigheid van opbrengsten is afhankelijk van uitkomsten assurance-onderzoeken

De opbrengsten van het agentschap Rijksdienst voor Identiteitsgegevens (RvIG) bestaan onder andere uit het verstrekken van reisdocumenten, het beheer van het Burgerservicenummer (BSN) en het berichtenverkeer met betrekking tot de Basisregistratie Personen (BRP). Voor de volledigheid van de BRP-opbrengsten is het nodig inzicht te verkrijgen in de werking in de bijbehorende IT-systemen. Een betrouwbare basis ontbrak voor het vaststellen van de volledigheid van de BRP-opbrengsten uit het berichtenverkeer.

Om de onzekerheid over de volledigheid van de BRP-opbrengsten weg te nemen heeft RvIG met partij 1 en partij 2 afspraken gemaakt. Vervolgens is de afspraak gemaakt om jaarlijks onderzoek te doen naar de opzet, het bestaan en de werking van de interne beheersing. Ten behoeve van het systeem bij zowel partij 1 als partij 2 constateren wij dat RvIG stappen heeft gezet met de bedoeling om met een assurance rapport inzicht over de betrouwbaarheid van het systeem te krijgen. Tevens is het van belang dat het functioneel beheer van Gemeentelijke Basisadministratie Persoonsgegevens Verstrekkingsvoorziening (GBA-V) door RvIG voldoet aan het GITC normenkader, waarmee afdoende maatregelen zijn getroffen voor adequaat functioneel beheer.

De snelheid waarmee deze assurance-onderzoeken plaats gaan vinden en de eerste resultaten van deze onderzoeken zullen bepalen of de onzekerheid weggenomen kan worden en/of de bevinding over 2022 niet langer van toepassing zal zijn.

3 Nieuwe bevindingen

3.1 Inleiding

In dit hoofdstuk behandelen wij de belangrijkste nieuwe bevindingen van onze onderzoeken naar het financieel- en materieelbeheer. Daarbij wordt aangetekend dat onze onderzoeken zich in wisselende stadia van uitvoering bevinden. Sommige onderzoeken zijn al uitgevoerd, sommige onderzoeken zijn halverwege dan wel recent opgestart en bepaalde geplande onderzoeken moeten nog worden uitgevoerd. Onze definitieve bevindingen over het financieel- en materieelbeheer, die in maart 2023 worden gerapporteerd in ons samenvattende auditrapport 2022 kunnen daarom afwijken van onze tussentijdse uitkomsten.

Deze nieuwe bevindingen gaan over de positionering van de CIO BZK en over de uitfasering van het bestelsysteem Digi Inkoop. Wij rapporteren deze bevindingen en geven handelingsperspectief om dit op te lossen.

Bevinding	Verantwoordelijk organisatieonderdeel
Positionering CIO niet meer in lijn met Besluit CIO-stelsel Rijksdienst	CIO BZK
Risico op problematische migratie bestelsysteem vanwege vertraging in de voorbereiding	UBR en SSC-ICT

Figuur 2: nieuwe bevindingen 2022

3.2 CIO BZK: Positionering CIO BZK niet meer in lijn met Besluit CIO-stelsel Rijksdienst

Op 23 maart 2022 heeft de SG van BZK een formeel besluit aangenomen dat de topstructuur van het ministerie verandert. Vanwege deze verandering, hebben wij de invulling van het Besluit CIO-stelsel Rijksdienst voor BZK opnieuw bekeken. In dit besluit, is onder meer opgenomen dat de CIO organisatorisch onder de SG dient te worden geplaatst (artikel 3.1. Besluit CIO-stelsel) en dat de CIO lid moet zijn van de Bestuursraad (artikel 3.4. Besluit CIO-stelsel). Aan deze punten wordt momenteel niet voldaan. Zo is de CIO BZK niet meer rechtstreeks onder de SG geplaatst en heeft de CIO BZK niet langer zitting in de Bestuursraad, maar heeft een staande uitnodiging gekregen. Hiermee ontstaat een mogelijk risico dat de in het Besluit gewenste strategische positie van de CIO ("de CIO als digitaal leider") en de beschreven taken en bevoegdheden van de CIO onvoldoende tot uiting komen. Overigens biedt artikel 17 Besluit CIO-stelsel de ruimte om gemotiveerd af te wijken indien dit de effectiviteit van de met dit besluit beoogde doelen ten goede komt.

We constateren dat de CIO Rijk destijds in overleg met de CIO BZK en de SG heeft ingestemd met een werkwijze waarbij de CIO een staande uitnodiging heeft tot bestuursraad kern en de bestuursraad breed en een evaluatiemoment inzake deze nieuwe positionering CIO BZK later gaat plaatsvinden. In deze nieuwe positionering is meegenomen dat de CIO BZK zitting heeft in bijvoorbeeld de BR bedrijfsvoering waarin veel onderwerpen worden besproken die te maken hebben met informatievoorziening.

Wij adviseren om in de genoemde evaluatie de impact van de huidige strategische positie van de CIO-BZK expliciet te analyseren in het licht van het besluit CIO-

stelsel Rijksdienst en de bedoeling daarvan. Voorts zal de impact van de huidige praktijk worden meegenomen in het ADR rijksbrede vervolgonderzoek naar het besluit CIO-stelsel dat gepland staat voor 2023.

3.3 UBR en SSC-ICT: Risico op problematische migratie naar het elektronisch Contracten, Bestellen en Factureren (eCBF)

In 2019 heeft de Interdepartementale Commissie Bedrijfsvoering Rijk (ICBR) besloten om het rijksbrede inkoopsysteem DigiInkoop te vervangen. In juli 2023 loopt de overeenkomst voor het beheer van DigiInkoop af. Binnen BZK is voor de vervanging van DigiInkoop onder andere het project elektronisch Contracteren, Bestellen en Factureren (eCBF) als onderdeel van het rijksbrede programma ‘’Vernieuwing Corporate Services’’ binnen BZK geïnitieerd. Voor UBR, SSC-ICT, FMH en P-direkt is het project eCBF opgezet om de functionaliteit van DigiInkoop te vervangen en een alternatief te bieden voor de ondersteuning van contractmanagement en de processen rondom bestellen, ontvangen en factureren van goederen en diensten.

Zowel bij UBR als SSC-ICT hebben wij onze zorgen geuit over de tijdigheid van de voorbereidingen omtrent de vervanging van DigiInkoop. Meer specifiek is de bestelmodule in CIFAS voor bestellen, ontvangen en factuurafhandeling een aandachtspunt. Inhoudelijke problemen en capaciteitstekorten bij het project, de leverancier en de deelnemers maken dat de planning van dit project naar achteren is verschoven. Met de gestelde interne deadlines zien wij een verhoogd risico op ondoelmatige, onjuiste en/of onrechtmatige inkooptransacties na migratie. Daarbij is het invoeren van nieuwe contracten *én bestaande* contracten in het nieuwe systeem een belangrijk aandachtspunt.

Overweeg om in overleg met DGDOO te komen tot alternatieve scenario’s, waaronder uitstel van migratie als laatste redmiddel, om een zorgvuldig voorbereide migratie uit te voeren. Wij benadrukken het belang van het onderkennen van potentiële risico’s bij een kwetsbaar migratieproces.

4 Overige onderwerpen

4.1 Inleiding

In dit hoofdstuk behandelen wij de belangrijkste ontwikkelingen die ook kunnen leiden tot nieuwe beheerbevindingen vanuit onze wettelijke controletaak. Ook gaan wij in op overige onderwerpen die van belang zijn voor een goede bedrijfsvoering. Daarbij wordt aangetekend dat onze onderzoeken zich in wisselende stadia van uitvoering bevinden. Sommige onderzoeken zijn al uitgevoerd, sommige onderzoeken zijn halverwege dan wel recent opgestart en bepaalde geplande onderzoeken moeten nog worden uitgevoerd. Onze definitieve bevindingen over het beheer, die in maart 2023 worden gerapporteerd in ons auditrapport 2022 kunnen daarom afwijken van onze tussentijdse bevindingen.

4.2 Monitoringscommissie BZK is effectief, blijf duiding geven aan "nut en noodzaak"

De monitoringscommissie is in 2021 opgericht met als doel te monitoren op welke wijze onvolkomenheden (AR), bevindingen (ADR) en aandachtspunten worden opgepakt door de verschillende organisatieonderdelen. De inrichting van de monitoringscommissie per 2021 is effectief gebleken. De voortgang en de opvolging van de bevindingen, onvolkomenheden en overige verbetertrajecten zijn kwalitatief toegenomen.

Ook dit jaar monitort de commissie de voortgang en waar nodig zullen er concrete stappen gezet worden om de bevindingen weg te nemen. Een goede samenwerking en communicatie speelt hierbij een essentiële rol om te komen tot een kwalitatief goede en effectieve bijdrage aan het financieel beheer. Tegelijk blijven wij aandacht vragen voor het expliciet maken van de nut en noodzaak om het verbetertraject in te zetten. Dit wordt namelijk niet als zodanig in het verbeterplan afgedwongen. Wanneer de nut en noodzaak niet op alle niveaus in de organisatie wordt onderkend, bestaat het risico dat de activiteiten gericht zullen worden op het wegwerken van de bevinding zonder de oorzaak hiervan te adresseren. Dit leidt dan meer tot symptoombestrijding, dan een structurele oplossing.

4.3 UBR: Doorontwikkeling UBR zorgvuldig bestuurlijk proces en impact op "soft controls"

Met de ondertekening van het convenant door de bestuurder van UBR, de DG Vastgoed en Bedrijfsvoering (VBR) en de ondernemingsraad (OR) kunnen de transitieplannen voor de diverse onderdelen van UBR ten uitvoer worden gebracht en worden alle bestaande UBR-onderdelen per 1 januari 2023 ondergebracht in 5 nieuwe dienstonderdelen direct onder DG VBR.

In het convenant zijn aanvullende afspraken bovenop het Voorgenomen Organisatiebesluit UBR (VOB) en het Organisatiebesluit UBR (OB) opgenomen. Deze extra afspraken gaan over zekerheid en duidelijkheid voor medewerkers en voor organisatieonderdelen.

Aan de hand van het convenant en gesprekken met UBR stellen wij vast dat er sprake is van een zorgvuldig bestuurlijk proces vanaf het opstellen van het VOB, het inwinnen van advies bij de OR, het nemen van het OB door de bestuurder, tot aan intensief overleg en afstemming over uitgangspunten en afspraken zoals vastgelegd in het convenant. Op dit moment is UBR bezig met het beschrijven van de wijzigingen in de topstructuur, het benoemen van (nieuwe) directeuren in de nieuwe organisatie en het uitwerken van medezeggenschap binnen de nieuwe organisatie.

Gezien de naderende datum van 1 januari 2023 is het zaak de voortgang te bewaken van deze laatste fase van de transitie. Naast aandacht voor het ontwikkelen/aanpassen van bestaande financiële processen benadrukken wij het belang van het goed inschatten van de organisatiecultuur, zoals het analyseren van resultaten van het Werk Omgeving Beleving Onderzoek (WOBO) en te blijven investeren in communicatie op alle niveaus. Ook de zogenaamde 'soft controls' benodigd voor adequaat financieel beheer zijn nauw verbonden met de organisatiecultuur en de turbulentie die een reorganisatie met zich meebrengt.

4.4 BZK FEZ: doorontwikkeling FEZ

In 2022 is BZK gestart met de doorontwikkeling van FEZ om de uitvoering van die taak te versterken. Daarvoor wordt de rol van FEZ duidelijker afgebakend, worden processen geoptimaliseerd en worden de belegging van taken en de ondersteuning door systemen en tools onder de loep genomen. Wij vinden dat een goed initiatief en hebben een positief beeld over de aanpak daarvan tot nu toe.

Producten, diensten en knelpunten van alle afdelingen zijn in kaart gebracht. Onder leiding van FEZ zijn de eerste 5 verbeterpunten in gang gezet, te weten:

1. Financial Control met filosofie "single point of truth"
2. (on)mogelijkheden Digidoc en het financiële proces, met aandacht voor betere workflow ondersteuning
3. Verantwoordelijkheid nemen op inhoud en geld, wie is verantwoordelijk voor welk (financieel) proces?
4. Coördinatie, regie en escalatie, hoe wordt dit toegepast?
5. Aanschrijvingen en werkinstructies, kan dit ook eenvoudiger?

Wij onderschrijven het belang van bovengenoemde 5 punten en verwachten dat deze actiepunten de doelmatigheid van de financiële functie ten goede zullen komen. Wij zullen de uitvoering van deze verbeteracties met belangstelling blijven volgen.

4.5 Huurtoeslag: voorstel hersteloperatie toeslagen nog niet goedgekeurd

In juni 2022 heeft de staatssecretaris van Financiën het wetsvoorstel "Wet hersteloperatie Toeslagen" bij de Tweede kamer ingediend. Momenteel is het wetsvoorstel nog niet goedgekeurd door het parlement. Wij willen erop wijzen dat pas wanneer de Wet hersteloperatie Toeslagen formeel aangenomen is, er een wettelijke grondslag is voor deze kwijtschelding, die tot nu toe heeft plaatsgevonden op basis van beleidsbesluiten.

Wij willen u wijzen op de risico's die samenhangen met het gebruik van beleidsbesluiten en benadrukken dat wanneer de genomen beleidsbesluiten niet in de volle omvang en met terugwerkende kracht bij wet worden geformaliseerd dit er toe kan leiden dat verplichtingen, uitgaven en kwijtscheldingen onrechtmatig zijn wegens het ontbreken van een wettelijke grondslag.

4.6 BZK kern: verantwoording en controle herstel- en veerkrachtplan (HVP) nog onduidelijk

Op 8 september heeft de Europese Commissie (EC) het door Nederland ingediende HVP bij het ministerie van Financiën goedgekeurd. De opgenomen maatregelen en doelen worden momenteel door de beleidsdirectie HVP in overleg met de EC concreet gemaakt.

De hiermee verband houdende activiteiten en uitgaven vinden reeds plaats bij BZK. Het is van belang om duidelijkheid te verkrijgen in de afspraken over de wijze van verantwoorden en accountantscontrole. Houd er rekening mee dat aantoonbaarheid van departementale risicoanalyses inclusief fraude en corruptie en het tegengaan van dubbele financiering belangrijke elementen zijn. Tevens is een belangrijk aspect inzichtelijk te maken hoe binnen BZK de relatie met de eindbegunstigde is ingeregeld. Het is voor BZK de uitdaging om zoveel mogelijk gebruik te maken van

de huidige praktijk van verantwoorden en beheersing. Tijdigheid van afspraken zijn cruciaal om de nodige voorbereidingen te kunnen treffen en om daarmee een doelmatig verantwoordings- en controleproces uit te kunnen voeren. BZK blijft wel afhankelijk van de beleidsdirectie HVP die hier een leidende rol in heeft.

4.7 BZK kern: overkoepelend inzicht BZK fraudebeheersing in ontwikkeling

In 2022 investeert BZK in het opstellen van een overkoepelende frauderisicoanalyse. Dit geeft BZK vorm door het risicoprofiel per onderdeel in kaart te brengen, een overzicht te maken van de belangrijkste frauderisico's en best practices te benoemen. FEZ organiseert in samenwerking met de RAFEB een tweedaagse opleiding voor de controllers van de uitvoeringsorganisaties van BZK en de collega's binnen FEZ. Het structureel inregelen van frauderisicobeheersing zal later plaatsvinden. We vragen aandacht voor het op langere termijn 'levend' houden van dit onderwerp en voor het agenderen daarvan in de bestuursraad en de verschillende managementteams. Dat zal het belang van "tone at the top" benadrukken waar een voorbeeldfunctie van uitgaat. Laat ook op dit niveau een kwalitatieve analyse plaatsvinden door bijvoorbeeld de zogenaamde fraudedriehoek voor BZK te bespreken.

4.8 BZK Kern: versterking begrotingsbeheer

Vorig jaar heeft BZK na het uitgaan van de zogenaamde veegbrief ontdekt dat de daarin opgenomen verplichtingenstand van artikel 10, niet juist was. Dat betekende dat de Tweede Kamer op dat moment met betrekking tot die verplichtingen niet juist was geïnformeerd. Om mogelijke herhaling te voorkomen heeft BZK een plan van aanpak met verbetermaatregelen opgesteld. Wij hebben die maatregelen in opzet beoordeeld en achten deze (in opzet) toereikend. De werking daarvan zullen wij later in het jaar toetsen wanneer de maatregelen zijn geïmplementeerd.

4.9 CIO BZK: BZK blijft op centraal niveau werken aan verdere verbetering van informatiebeveiliging

Over 2021 concludeerden wij dat BZK stappen heeft gezet om de volwassenheid op het gebied van centrale beheersing van informatiebeveiliging te verhogen. Wel gaven wij een aantal aandachtspunten mee:

- Blijf actief sturen op de volledigheid van de informatiebeveiligingsrapportages vanuit de dienstonderdelen om daarmee inzicht te houden in onder meer de lopende acties;
- Stuur (blijf) actief (sturen) op de decentrale invulling van het informatiebeveiligingsbeleid, bijvoorbeeld met de voorgenomen rapportage op Key Performance Indicators (KPI's) vanuit de onderdelen.
- Geef prioriteit aan het ontwikkelen van een awareness-plan;
- Inventariseer de weerbaarheid tegen ransomware aanvallen en bepaal waar aanvullende maatregelen nodig zijn.

BZK heeft hier in 2022 op de volgende wijze invulling aangegeven:
Op centraal niveau wordt actief gestuurd op de volledigheid van de informatiebeveiligings- en privacy rapportages door onder meer feedback te geven op de ontvangen rapportages. Ook is er een checklist 'beschikbaar' die beschrijft welke onderwerpen terug moeten komen in deze rapportages. Vanaf het tweede tertaal moeten de onderdelen ook rapporteren over de KPI's met betrekking tot informatiebeveiliging en privacy. Hoewel de kwaliteit en diepgang van de verschillende rapportages nog divers is, krijgt BZK op centraal niveau steeds meer zicht op de decentrale naleving van het informatiebeveiligingsbeleid, belangrijkste ontwikkelingen en risico's. Om voldoende capaciteit voor deze werkzaamheden op centraal niveau te behouden, wordt een aparte BZK Privacy Officer geworven. Een taak die tot nu toe belegd was bij CISO BZK.

BZK heeft dit jaar een Awareness-strategie voor bewustwordingsactiviteiten op het gebied van informatiebeveiliging en privacybescherming vastgesteld voor de periode 2022 en 2023. Deze strategie kent een gemeenschappelijk deel die wordt gefaciliteerd door de centrale staf en specifieke activiteiten bij organisaties of voor

specifieke functies. In dit plan zijn diverse meer generieke activiteiten benoemd. Hoewel diverse activiteiten op het gebied van awareness doorgang vinden, ontbreekt momenteel nog een nadere analyse van de noodzakelijke activiteiten en de daarbij behorende uitwerking. Het is van belang om hier de komende tijd verder invulling aan te gaan geven.

Een project dat meer inzicht moet bieden in de weerbaarheid tegen ransomware-aanvallen is recentelijk gestart. Hierbij wordt gestart bij drie onderdelen van BZK met een belangrijk I-component.

4.10 CIO Rijk: aandachtspunten

4.10.1 Meer aandacht voor feitelijke veiligheid

In ons rapport over 2021 constateerden we een lichte verbetering ten aanzien van de governance en beheersing van informatiebeveiliging bij de departementen op departementaal niveau. Tegelijkertijd spraken wij onze zorg uit over de feitelijke veiligheid en adviseerden wij om te bezien op welke wijze BZK/CIO-Rijk de departementen kan ondersteunen in verkrijgen van inzicht en waar mogelijk het verbeteren van de feitelijk veiligheid, bijvoorbeeld door middel van red-teaming activiteiten.

De afgelopen periode is een routekaart Digitale Weerbaarheid opgesteld en goedgekeurd in het CIO-beraad. Deze routekaart beschrijft een aantal speerpunten die invulling geven aan het thema Weerbaarheid uit de vorig jaar vastgestelde I-strategie.

De CIO Rijk heeft in 2022 samen met de departementale CISO's onderzoek uitgevoerd naar de toepasbaarheid van TIBER (Rijksbreed IB-Beeld 2021) om daarmee, in lijn met de I-strategie 2021-2025, te komen tot een rijksbreed testprogramma voor de periode 2022-2026. Aan de Tweede Kamer is toegezegd dit plan ten uitvoer te brengen. Dit is een positieve ontwikkeling, omdat uit onze eerdere rode-draden analyse op ADR-onderzoeken naar informatiebeveiliging is gebleken dat het laten toetsen van de beveiliging een wezenlijke bijdrage kan leveren aan de beveiliging van de onderzochte systemen. Wij zijn betrokken bij de nadere uitwerking van het rijksbreed testprogramma.

Wij zullen in ons rijksbrede onderzoek naar informatiebeveiliging, in opdracht van de CIO-Rijk als voorzitter van het CIO-beraad, ook in de komende periode onze aandacht verleggen van governance en sturing op informatiebeveiliging naar het testen van de feitelijk veiligheid. De opdracht hiervoor wordt momenteel nader uitgewerkt. Voor de volledigheid merken wij op dat audits, pentesten en red-teaming activiteiten een sluitstuk vormen en de maatregelen die getroffen moeten worden in de eerste en tweede lijn niet vervangt. Ook is er een plan van aanpak 'Versterkt SOC Stelsel Rijk en Projectbrief Verplichte basistraining Digitale weerbaarheid' opgesteld.

Voorts is als reactie op het Rijksbrede IB-beeld over 2021, door het ICBR besloten tot het opstellen en introduceren van een rijksbreed kader en beleid voor risicomanagement om daarmee risicogerichte sturing op informatiebeveiliging te verbeteren. Wij onderschrijven het belang van risico-gerichte sturing om daarmee beter zicht te krijgen op de belangrijkste rijksbrede risico's. Een project om dit kader en beleid vorm te geven wordt momenteel opgestart.

4.10.2 CIO Rijk: Monitoring Rijksbreed IT-beheer blijft aandachtpunt

BZK/CIO-Rijk heeft in 2022 een plan van aanpak opgesteld dat nadere invulling geeft aan de opvolging van de onvolkomenheid van de Algemene Rekenkamer met betrekking tot het monitoren van Rijksbreed IT-beheer. Dit plan gaat in op het verkrijgen van inzicht in de beheerdomeinen autorisatiebeheer, wijzigingsbeheer, beveiliging van componenten en backup- en recovery bij de departementen, het

verkrijgen van inzicht in de effectiviteit van bestaande goedgekeurde kaders, het waar nodig vernieuwen of, het maken van nieuwe kaders en afspraken en het inrichten van monitoring op de status van Rijksbreed IT-Beheer. Het uitvoeren van het plan wordt op dit moment opgestart. Zo is hier recent een projectleider voor benoemd.

BZK/CIO-Rijk lijkt vooralsnog aan de departementen over te laten over welke belangrijke IT-systemen het departement zal rapporteren en daarmee in de monitoring van BZK zal vallen. Wij adviseren DGDOO duidelijke criteria te definiëren welke systemen wel of niet binnen de scope van het project vallen. Het is van belang om een volledig en actueel beeld te hebben van de in gebruik zijnde systemen zodat risicomanagement effectief kan plaatsvinden.

Het plan voorziet verder in de mogelijkheid tot het definiëren van nieuwe kaders. Wij adviseren zo veel mogelijk aan te haken bij de reeds bestaande (normen)kaders, zoals de Baseline Informatiebeveiliging Overheid (BIO) of het veel gehanteerde General IT-control normenkader.

4.10.3 CIO-Rijk: cloudbeleid geformaliseerd, aandachtspunten blijven

Recentelijk is het rijksbrede cloudbeleid 2022 geformaliseerd en uitgebracht. Dit cloudbeleid bevat een uitwerking van de nieuwe visie op het gebruik van publieke clouddiensten door de Rijksoverheid. Het is positief dat nu uitgangspunten zijn geformuleerd. Tegelijkertijd constateren wij dat een deel van de in onze rapportage 2021 genoemde vragen en zorgen nog niet zijn geadresseerd. Wij noemen hierbij bijvoorbeeld:

- het op peil brengen en aanhouden van voldoende kennis binnen de Rijksoverheid voor de inrichting en aansturing van (respectievelijk functioneel en technisch personeel) cloudproviders,
- het marktconcentratierisico van grote public cloud providers en in samenhang hiermee de invulling van de regiefunctie van BZK ten aanzien van cloudgebruik.

Wij adviseren dergelijke punten de komende tijd mee te nemen in de nadere uitwerking van het cloudbeleid (implementatie richtlijn) en waar nodig mee te nemen in de (jaarlijkse) evaluatie van het cloudbeleid.

5 Specifiek Staten-Generaal: Let op de voortgang van verbeteracties

Voor begrotingshoofdstuk IIA Staten-Generaal en begrotingshoofdstuk IIB Overige Hoge Colleges van Staat en Kabinetten van de Gouverneurs en de Kiesraad geldt dat zij staatsrechtelijk de vrijheid hebben om het financieel beheer (van de begroting) zelf in te richten binnen de kaders van de Comptabiliteitswet 2016. De stand van zaken inzake de follow-up van de bevindingen van 2022 staat ter informatie in dit interim rapport gericht aan de minister van Binnenlandse Zaken en Koninkrijksrelaties opgenomen vanwege de begrotingsverantwoordelijkheid van deze minister.

Hieronder staan de bevindingen, zoals op 15 maart 2022 gerapporteerd over 2021. Initiatief tot verbetering is op alle fronten genomen. Wij hebben de leiding van de Staten-Generaal geadviseerd om de voortgang van de verbeteracties te concretiseren, duidelijke mijlpalen te formuleren en de voortgang goed te blijven volgen en bij te sturen om zodoende verbetering ook in 2022 (op onderdelen) als gerealiseerd te kunnen gaan beschouwen.

Figuur 2: overzicht bevindingen Staten-Generaal per ultimo 2021

Bevinding	Verantwoordelijk organisatie-onderdeel	2020	2021	Ontwikkeling 2022
Administratieve verwerking verplichtingen en voorschotten niet op orde	Tweede Kamer der Staten-Generaal		■	Versterking administratieve verwerking verplichtingen en voorschotten in gang gezet
Registratie kunstwerken verbeteringen noodzakelijk	Eerste Kamer der Staten-Generaal, en Tweede Kamer der Staten-Generaal		■	Verbeteringen in het beheer kunstwerken onder handen werk
Onderbouwing prestatielevering niet altijd snel aantoonbaar	Tweede Kamer der Staten-Generaal		●	Overweeg three-way-match in financieel systeem
Nog geen (aantoonbare) effectieve werking IT-beheer	Tweede Kamer der Staten-Generaal		●	Let op GITC van uitbestede IT diensten

● licht ■ gemiddeld ▲ ernstig √ opgelost

Nadere toelichting:
De Tweede Kamer heeft ten aanzien van het financieel beheer versterking geregeld en heeft interne checklists onder handen genomen. Tevens hebben de bevindingen van vorig jaar van de ADR aan een stuk bewustwording bijgedragen.

Zowel de Eerste Kamer als de Tweede Kamer hebben inventarisaties uitgevoerd van de kunstwerken en zijn bezig met een professionaliseringsslag plaats ten aanzien van het beheer en de registraties van de kunstwerken. Op dit moment is dit onderhanden werk, waardoor we nog niet kunnen vaststellen dat onze bevinding over 2022 weggenomen gaat worden.

De aantoonbaarheid van de prestatieonderbouwing was vorig jaar een bevinding. Er zijn door de Tweede Kamer verbeteracties in gang gezet. Komende periode zal uitwijzen welke resultaten de verbeteracties opgeleverd hebben. De verwachting is dat dit voor 2022 nog steeds een aandachtspunt zal blijven. Door de Tweede Kamer wordt verkend of met een in de financiële administratie digitaal ingeregelde three-way-match de prestatieonderbouwing gerelateerd zou kunnen worden aan de ontvangen factuur en de opdrachtverstrekking.

De aantoonbaarheid van de general IT controls van het *financieel pakket* is verbeterd, zoals wij dat in opzet hebben beoordeeld. Een deel van het beheer is uitbesteed aan externe beheerorganisaties. Er is gebleken dat het wachtwoordbeheer en gebruikersbeheer die bij deze partijen is belegd, niet (zichtbaar) effectief zijn ingericht. Wij adviseren de Tweede Kamer haar inzicht te vergroten rondom de general IT controls die ingeregeld zijn bij uitbestede diensten.

6 Ondertekening

Den Haag, 12 oktober 2022

Auditdienst Rijk

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(