Auditdienst Rijk
Ministerie van Financiën

Interim-auditrapport
2024

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Ministerie van Volkshuisvesting en Ruimtelijke Ordening

Gemeentefonds
Provinciefonds
BES-fonds

FEZ heeft blijvende aandacht voor verbeteren van het financieel beheer

Versterken risicomanagement financieel en IT-beheer

FEZ zet met het verstevigen van de financial control bij het kerndepartement stappen in het versterken van risicomanagement in het financieel en IT-beheer. Op basis van actuele procesbeschrijvingen heeft FEZ het voornemen om periodieke risicoanalyses uit te voeren.

Ook de uitvoeringsorganisaties zetten stappen in het versterken van het risicomanagement. Momenteel heeft FEZ inzicht in specifieke thema's zoals inkoop en betaaltermijnen, maar nog te weinig inzicht in de voortgang van risicomanagement en het bredere financieel en IT-beheerprocessen.

Bij drie van de vijf gewogen bevindingen uit 2023 hebben we een duidelijke vooruitgang waargenomen. In het IT-beheer zien we risico's bij IB governance en digitale weerbaarheid.

Dit betreft:

- Niet altijd sluitende PDCA-cyclus en bijbehorende actuele risicobeelden per IT-systeem;
- Niet alle agentschappen beschikken over een jaarkalender voor beveiligingsonderzoeken;
- Geen actuele centrale registratie van kritieke incidenten.

Wet deregulering beoordeling arbeidsrelaties (DBA)

Met de wet DBA beoogt de wetgever om schijnzelfstandigheid bij de inhuur van zelfstandigen (ZZP'ers) te voorkomen. BZK huurt, samen met haar uitvoeringsorganisaties, meer extern personeel waar onder zelfstandigen in dan de Roemer norm van 10% die daarvoor van toepassing is. Daardoor loopt BZK het risico van schijnzelfstandigheid en het niet voldoen aan de wet DBA.

Met een Taskforce Aanpak Schijnzelfstandigheid is BZK momenteel aan het inventariseren wat de situatie voor haar, inclusief de uitvoeringsorganisaties, precies is en in hoeverre welke organisaties risico's lopen met betrekking tot het naleven van de wet DBA vanaf 2025. Op basis van de uitkomsten zal de strategie worden bepaald om deze wet na te leven.

Externe inhuur
Het onderwerp externe inhuur zal geraakt worden door de taakstelling en de strakke hantering van de Roemer norm van 10% zoals afgesproken in het Hoofdlijnenakkoord.

Meerdere organisatieonderdelen van BZK en VRO hadden in 2023 een substantiële overschrijding van de Roemernorm.

Hoofdlijnenakkoord

Vervolg Wet DBA
Vanuit een interdepartementale werkgroep van DG DOO is recent een concept leidraad opgesteld, die organisaties binnen de Rijksoverheid moet helpen om schijnzelfstandigheid te voorkomen bij inhuur van zzp'ers. Deze leidraad en mogelijke vervolgacties worden door de betrokken partijen nog besproken.

Ontwikkelingen volgend uit hoofdlijnenakkoord

Het hoofdlijnenakkoord van 16 mei 2024 heeft geleid tot de vorming van drie nieuwe departementen, waaronder het Ministerie van Volkshuisvesting en Ruimtelijke Ordening (VRO). Hoewel dit ministerie formeel al op 2 juli is gecreëerd, vraagt het enige tijd om deze totstandkoming praktisch vorm te geven. Daarvoor wordt een overgangsperiode gehanteerd tot 1 januari 2025. Over 2024 zullen het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en Volkshuisvesting en Ruimtelijke Ordening één gecombineerde verantwoording opstellen.
Met betrekking tot het proces van departementale herschikking hebben de minister-president en de minister van BZK in het constituerend beraad van 5 juli meegegeven om als uitgangspunt 'minimale aanpassing op de bestaande situatie' te hanteren. Dit vanuit het oogpunt de herschikking zo efficiënt en doelmatig te laten plaatsvinden.

Daarnaast komen de volgende organisatieonderdelen over van het ministerie van Economische Zaken naar BZK en is het voornemen om de specifieke uitkeringen (SPUKS) terug te dringen en over te hevelen naar het Gemeentefonds:
- Directie Schadeherstel Groningen (en Gaswinning) en Directie Versterken en Perspectief Groningen (beleidsdirecties);
- Nationaal Coördinator Groningen (NCG);
- Adviescollege Veiligheid Groningen;
- Instituut Mijnbouwschade Groningen (IMG) (ZBO).

Ten tijde van het schrijven van dit interim-auditrapport moest een aantal belangrijke beslissingen nog genomen worden, onder andere met betrekking tot de bestuurlijke topstructuur en de organisatorische ophanging van de organisaties die naar BZK overkomen. BZK is al in een vroeg stadium gestart met het analyseren van de impact van deze wijzigingen voor de bedrijfsvoering, de administraties en IT-systemen, en de (financiële) verantwoording van 2024 en volgende jaren. Wij blijven de ontwikkelingen volgen om ook de implicaties voor de controle tijdig in beeld te hebben.

In december 2023 is in het SGO en in de ICBR afgesproken om binnen de Rijksoverheid mogelijke schijnzelfstandigheid te inventariseren en te komen tot een plan van aanpak om dit te beëindigen.

Samenvatting ontwikkelingen in het financieel en materieel beheer

OBF: Verbeteringen eCBF zichtbaar

- Risicoanalyses voor financieel beheerprocessen zijn geactualiseerd
- General IT controls voor kritieke applicaties van OBF zijn in kaart gebracht
- De betaalnorm van 95% betalen binnen 30 dagen wordt nog niet gehaald

Uitdagingen financieel beheer SSO-CN vergt tijd

- Door verschillende interne en externe uitdagingen is het verbeterplan nog niet conform planning uitgevoerd
- De interne beheersing van financieel en personeel beheerprocessen nog niet voldoende gewaarborgd

Prestatieonderbouwing BZK2 verdient aandacht

- De basishygiëne rond prestatieverklaringen is nog niet op orde

Inkoopbeheer inhuurkrachten SSC-ICT geborgd

- De risico's rondom verlengingsopties en knock-outcriteria zijn geborgd
- Het risico op eventueel verstrekken van tegenstrijdige informatie aan leveranciers is opgelost

RvIG

- De assurance audit voor IT beheer is gepland
- In de aanvullende werkzaamheden is voorzien voor het vaststellen van de volledigheid van de opbrengsten BRP

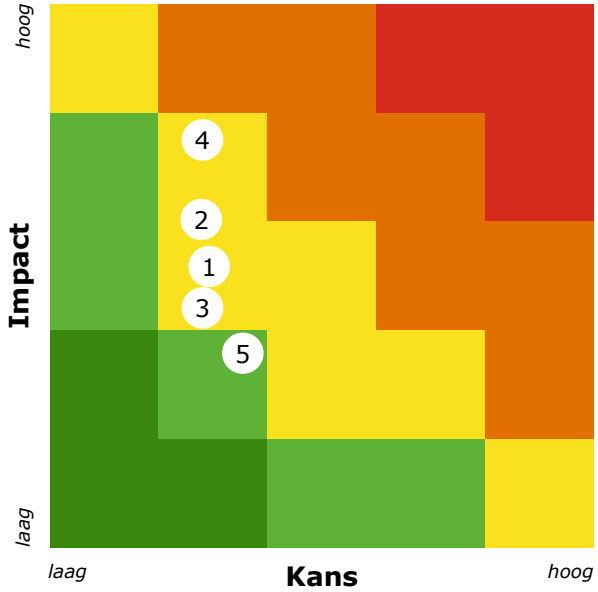
Overzicht voortgang bevindingen 2023

Financieel beheer en jaarrekening

1	Interne en externe uitdagingen in financieel beheer SSO-CN	=
2	Inkoopbeheer inhuurkrachten SSC-ICT nog niet geheel geborgd	↙
3	Prestatieonderbouwingen BZK2 niet in alle gevallen toereikend	=

IT Beheer

4	Werking interne beheersing eCBF heeft verbetering nodig	↙
5	Volledigheid opbrengsten RvIG aangetoond, na aanvullende werkzaamheden	↙



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

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 Binnenlandse Zaken en Koninkrijksrelaties (BZK), het ministerie van Volkshuisvesting en Ruimtelijke Ordening (VRO), het Gemeentefonds, het Provinciefonds en het BES-fonds. 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. Deze rapportage heeft het karakter van een 'early warning', zodat nog in 2024 maatregelen kunnen worden getroffen.

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 stand van zaken per 15 maart 2024 hebben wij de gewogen bevindingen uit ons auditrapport 2023 een prioritering meegegeven, die wij in dit interim-auditrapport presenteren volgens deze nieuwe rapportagewijze. Met symbolen is daarbij de voortgang ten opzichte van 15 maart 2024 geduid.

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.

1 Risicomanagement en frauderisicobeheersing

Stappen worden gezet in versterken risicomanagement financieel en IT-beheer

FEZ verstevigt momenteel de financial control bij het kerndepartement en heeft een goede start gemaakt met een presentatie voor alle financieel medewerkers van BZK over risicomanagement.

- Een speciaal gevormd team Financial Control en Management Informatie (FCMI) werkt projectmatig aan de invulling van deze rol. Onderdeel daarvan zijn interne controles naar de rechtmatigheid van verplichtingen en uitgaven die door de CDI-Office (inkopen) en het Expertise Centrum Subsidies (subsidies en bijdragen) worden uitgevoerd.
- FEZ is gestart met zogenaamde controlroom bijeenkomsten, waar de financial controllers op basis van data-analyse met elkaar vaststellen waar zich risico's kunnen voordoen in de financiële administratie en/of bedrijfsvoering.

- FEZ heeft een project opgestart voor het actualiseren van de procesbeschrijvingen en werkinstructies van de financiële processen. Het doel is om een systeem op te zetten met periodieke risicoanalyses op de processen en het actualiseren van de procesbeschrijvingen en werkinstructies op basis van de geldende regelgeving.

Uitvoeringsorganisaties

Bij de uitvoeringsorganisaties ligt de verantwoordelijkheid voor het risicomanagement bij het management van deze organisaties. De rapportage- en gesprekscyclus van de uitvoeringsorganisaties besteedt ook aandacht aan de kwaliteit van de bedrijfsvoering waaronder het financieel beheer en het IT-beheer.

Het valt ons op dat in de jaarplannen en de viermaands rapportages (VMR) relatief weinig wordt vermeld over het financieel beheer en het IT-beheer terwijl er bij alle uitvoeringsorganisaties op dat vlak nog werk te verzetten is en wordt verzet.

Nu komt het voor dat informatie over het financieel beheer achteraf via de derde lijn gevraagd wordt, in plaats via het toezicht.

Wij hebben vorig jaar FEZ geadviseerd om de regie te nemen en samen met de chief financial officers (CFO's) en chief information officers (CIO's) van de uitvoeringsorganisaties het risicomanagement in de financieel en de IT-beheerprocessen verder vorm te geven, wat BZK in staat stelt om waar nodig bij te sturen.

Dit kan door het opstellen van risicoanalyses, het treffen van beheersingsmaatregelen, het toetsen van de beheersingsmaatregelen om de werking daarvan vast te stellen en te bepalen welke acties nodig zijn om de doelen te bereiken, kansen te optimaliseren en risico's te beheersen.

Frauderisicobeheersing

De Organisatie Bedrijfsvoering en Financiën (OBF) heeft in de eerste VMR 2024 wel gerapporteerd omtrent het financieel beheer en aspecten van het IT- beheer. Het toetsen van de keycontrols in de IT-processen ontbreekt daarin. Mogelijk kan de VMR van OBF, aangevuld met toetsen van de keycontrols in de IT-processen, als voorbeeld dienen.

Handelingsperspectief
Wij adviseren FEZ om in samenwerking met de uitvoeringsorganisaties en Eigenaarsadvisering afspraken te maken om in de VMR's ook te laten rapporteren over het financieel beheer en het IT-beheer inclusief het risicomanagement die zij daarop uitvoeren.

Frauderisicobeheersing vordert langzaam
FEZ is sinds 2022 bezig met het opstellen van een BZK-brede controlmatrix frauderisicobeheersing. In de huidige versie (van 2024) zijn de frauderisico's en beheersingsmaatregelen van de agentschappen opgenomen. Wij missen daarin De Huurcommissie, de begrotingshoofdstukken en de Organisatie Bedrijfsvoering en Financiën (OBF), waar ook frauderisico's aanwezig zijn. Sommige frauderisico's komen bij alle organisatieonderdelen voor, maar in de huidige controlmatrix zien wij die risico's niet bij alle agentschappen terug.

Daarnaast heeft FEZ in 2024 een fraudeweerbaarheidskader opgesteld om het ministerie fraudebestendig te hebben en te houden. Dat kader biedt voldoende informatie om dit onderwerp in de organisatie te doen leven en moet nog worden afgestemd met de directies P&O en Mens en Middelen.

Verder heeft FEZ de intentie om nog een aantal van haar medewerkers de opleiding fraudepreventie van de RAFEB te laten volgen om kennis op dat vlak bij FEZ te vergroten.

Handelingsperspectief
Wij adviseren FEZ om de controlmatrix voor alle organisatieonderdelen volledig in te (laten) vullen zodat alle risico's en beheersingsmaatregelen inzichtelijk zijn. Verder adviseren wij om de getroffen beheersingsmaatregelen periodiek te laten toetsen en daarover te laten rapporteren aan FEZ. De agentschappen/uitvoeringsorganisaties kunnen dat via de viermaandsrapportages VMR's doen.

2 Follow-up bevindingen over 2023

OBF: Verbeteringen eCBF zichtbaar

Bevinding		Verantwoordelijke organisatieonderdeel	Weging 2022	Weging 2023	Prioritering 2023	Voortgang
1	Werking interne beheersing eCBF heeft verbetering nodig	OBF		●		↙

Bevinding

In 2024 is de Organisatie Bedrijfsvoering en Financiën (OBF) van de DG VBR doorgegaan met het verder optimaliseren van het Cifas systeem, dat het electronisch bestellen en factureren (eCBF) ondersteunt. Op het vlak van de interne beheersing heeft OBF haar risicoanalyses voor haar financieel beheerprocessen geactualiseerd en de general IT controls (GITC's) van kritieke applicaties in kaart gebracht. Zij heeft een interne controleplan opgesteld voor de oud-UBR organisaties en de eerste controles zijn al uitgevoerd.

Daarnaast voert zij verschillende controles en analyses uit voor haar ketenpartners om mogelijke fouten te signaleren en te rapporteren. Verder heeft zij een aantal application controls gewijzigd in blokkades in plaats van signaleringen zodat het proces geen doorgang vindt indien niet aan de in het systeem opgenomen (rechtmatigheids) criteria wordt voldaan. OBF is, conform ons advies van vorig jaar, voornemens om de interne controles die zij voor de oud-UBR onderdelen uitvoert uit te breiden voor haar andere afnemers, zodat de gehele keten wordt gecontroleerd, wat efficiënter is. Uit de gecontroleerde posten van OBF en van de ADR zijn tot nu toe geen onrechtmatigheden naar voren gekomen.

OBF: Verbeteringen eCBF zichtbaar (vervolg)

Bevinding (vervolg)	Het lukt nog niet om facturen tijdig te betalen, ondanks alle inspanningen van OBF en haar afnemers, die bepaalde processtappen in het betaalproces zelf uitvoeren. OBF heeft op dat vlak ook stagnatie ondervonden van het nieuw. inkoopsysteem DioR dat communicatieproblemen gaf met Cifas. De de gebruikers moesten hiermee nog leren werken. Daarnaast werkt OBF nog aan het ontsluiten van data uit Cifas om via de rapportagetool Clik Sense managementrapportages te faciliteren waaraan haar afnemers behoefte hebben ten behoeve van hun bedrijfsvoering. OBF werkt met haar stakeholders en ketenpartners samen aan verbeteringen met betrekking tot bovengenoemde punten.
Risico	Zowel OBF als haar afnemers kunnen hinder ondervinden door de nog niet optimaal functionerende systemen, onjuiste inkopen en bestellingen. Dit kan leiden tot inefficiënties en vertragingen in de verwerking van de facturen.
Handelingsperspectief	Het succes van het eCBF hangt af van het optimaal functioneren van Cifas. Wij adviseren de OBF om goed samen te werken met de ketenpartners en in overleg met haar prioriteiten te stellen in het optimaliseren van de systemen en de factuurverwerking.

Inkoopbeheer inhuurkrachten SSC-ICT geborgd

Bevinding		Verantwoordelijke organisatieonderdeel	Weging 2022	Weging 2023	Prioritering 2023	Voortgang
4	Inkoopbeheer inhuurkrachten SSC-ICT nog niet geheel geborgd	SSC-ICT	●	●		↙

Bevinding

In 2023 had SSC-ICT aanvullende beheersingsmaatregelen in het inkoopproces rond externe inhuur getroffen om tekortkomingen rond verlengingsopties en knock-outcriteria op te lossen. Zij heeft die maatregelen in 2024 gecontinueerd en de werking daarvan vastgesteld met interne controles. Van de uitgevoerde controles en conclusies van IAA heeft de ADR kennisgenomen. Uit de gecontroleerde posten van de ADR en IAA blijken geen rechtmatigheidsbevindingen over het eerste halfjaar van 2024. Daaruit blijkt dat het aantal bevindingen aangaande verlengingsopties en knock-outcriteria verder is verlaagd naar een beheersbaar niveau. Door de implementatie van DiOR door de Inhuurdesk, waarvan ook SSC-ICT gebruik maakt, is het risico dat voorheen werd gelopen op het eventueel verstrekken van tegenstrijdige informatie aan leveranciers, opgelost omdat het aanvraagformulier is komen te vervallen.

Weging: ● Licht ■ Gemiddeld ▲ Ernstig

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

RvIG: Aan IT-beheer basisregistratie persoonsgegevens (BRP) wordt nog gewerkt

Bevinding		Verantwoordelijke organisatieonderdeel	Weging 2022	Weging 2023	Prioritering 2023	Voortgang
5	volledigheid opbrengsten RvIG aangetoond, na aanvullende werkzaamheden	RvIG	●	●		↙

Bevinding

In 2023 kwamen tekortkomingen naar voren uit het onderzoek naar het IT-beheer van het systeem voor de BRP. Daardoor werden risico's gelopen met betrekking tot de betrouwbaarheid van het berichtenverkeer en de verantwoorde omzet van de BRP, die afhankelijk is van het aantal berichten. RvIG heeft toen met aanvullende gegevensgerichte werkzaamheden vastgesteld dat de risico's zich niet hebben voorgedaan en de verantwoorde omzet betrouwbaar was. RvIG laat ook in 2024 een assurance audit uitvoeren naar het IT-beheer rond de BRP en zal de uitkomsten daarvan analyseren en indien nodig evenals in 2023 met aanvullende (gegevensgerichte) werkzaamheden de betrouwbaarheid van de verantwoorde omzet vaststellen.

Weging: ● Licht ■ Gemiddeld ▲ Ernstig

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

SSO-CN: Uitdagingen in het financieel beheer verdient tijd

Bevinding		Verantwoordelijke organisatieonderdeel	Weging 2022	Weging 2023	Prioritering 2023	Voortgang
2	Interne en externe uitdagingen in het financieel beheer	SSO-CN		●		=

Bevinding

In 2023 hebben wij gerapporteerd dat het SSO-CN met verschillende interne en externe uitdagingen (werving MT-leden, implementatie OF-rapport en introductie KPM) te maken heeft waardoor het haar niet was gelukt om haar verbeterplan voor het financieel beheer conform planning uit te voeren. De interne beheersing in de financieel- en personeel beheerprocessen, die de rechtmatigheid, getrouwheid, ordelijkheid en controleerbaarheid van verplichtingen en uitgaven moet waarborgen was daardoor nog niet voldoende. Het opstellen en vaststellen van een betrouwbare financiële verantwoording vroeg veel inspanningen van SSO-CN, FEZ BZK en de ADR.

In juni 2024 heeft FEZ BZK een bezoek gebracht aan SSO-CN om na te gaan wat de uitdagingen en dilemma's zijn in het verbeteren van het financieel beheer en hoe FEZ daarin kan ondersteunen. Naar aanleiding van dit bezoek heeft FEZ (control en CDI) samen met SSO-CN een plan van aanpak opgesteld. Dit plan geeft inzicht in verschillende actiepunten en wordt binnenkort volledig vastgesteld. Deze actiepunten worden op initiatief van SSO-CN geprioriteerd waarbij SSO CN rekening houdt met de schaars beschikbare capaciteit. Het verplichtingenbeheer is een van de belangrijke punten binnen SSO-CN om verbeterslagen te maken. FEZ (control en CDI) faciliteren en adviseren bij de uitvoering van deze activiteiten, waarvan een aantal van de te nemen maatregelen reeds zijn opgestart. Een voorbeeld hiervan is een aanpak om bestaande onrechtmatige contracten te beëindigen en de opvolging van een aanbeveling uit het Verantwoordingsonderzoek van de Algemene Rekenkamer t.a.v. het inkoopbeheer. Daarnaast is er een opdracht geformuleerd om met een externe expert de verplichtingenadministratie op een duurzame wijze te verbeteren, onder andere door de rapportages te standaardiseren en actualiseren en het inrichten en beschrijven van de werkprocessen.

Weging: ● Licht ■ Gemiddeld ▲ Ernstig

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

SSO-CN: Uitdagingen in het financieel beheer verdient tijd (vervolg)

Risico	Ondanks de reeds lopende trajecten is er nog sprake van een verhoogd risico op onrechtmatigheden en getrouw beeld fouten in de verantwoorde verplichtingen en uitgaven.
Handelings-perspectief	Wij adviseren SSO-CN en FEZ om, zolang de interne beheersing niet voldoende is versterkt conform het plan van aanpak, met de door ons aanbevolen analyses en inventarisaties (gegevensgericht) vast te stellen dat de verantwoorde verplichtingen en uitgaven rechtmatig en getrouw zijn.

Prestatieonderbouwing BZK2 vergt aandacht

Bevinding		Verantwoordelijke organisatieonderdeel	Weging 2022	Weging 2023	Prioritering 2023	Voortgang
3	Prestatieonderbouwingen niet in alle gevallen toereikend	BZK2	●	●		=

Bevinding

Om onrechtmatige betalingen te voorkomen, is het essentieel dat BZK2 voorafgaand aan het betalen van een factuur verifieert of de levering van een product of dienst heeft plaatsgevonden zoals overeengekomen in het contract of de offerte, met betrekking tot hoeveelheden, tarieven en kwaliteit.

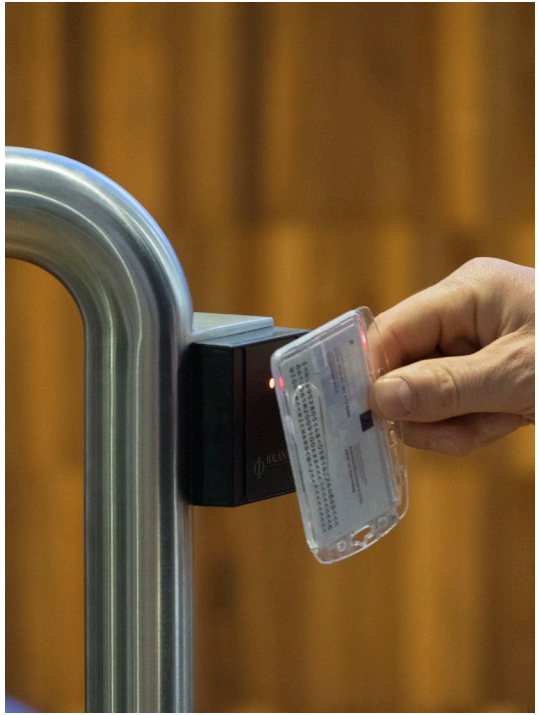
BZK2 heeft sindsdien verschillende maatregelen genomen om deze bevinding aan te pakken. Zo is in 2023 het proces rondom prestatieverklaringen beschreven. Verder zijn er vorig jaar binnen BZK2 meerdere 'roadshows' georganiseerd om het belang van prestatieverklaringen te benadrukken en het nalevingsgedrag te verbeteren. Uit onze controle over het eerste halfjaar 2024 blijken nog geen significante verbeteringen. Bij een aantal van de gecontroleerde transacties bleek de prestatieonderbouwing niet in de administratie aanwezig was en/of niet voldoen aan de kwaliteitseisen. Dit is een indicatie dat de administratieve basishygiëne rond prestatieverklaringen nog niet op orde is.

Weging: ● Licht ■ Gemiddeld ▲ Ernstig

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

Prestatieonderbouwing BZK2 vergt aandacht

Risico	Als de geleverde prestatie niet of onvoldoende wordt vastgesteld door BZK2, kan dit leiden tot onterechte betalingen en onrechtmatigheden. Verder raakt het niet archiveren van de prestatieonderbouwing in het betaaldossier de controleerbaarheid van de administratie.
Handelingsperspectief	We adviseren BZK2 om de prestatieverklaarders binnen de verschillende directies uitgebreid te informeren over het belang van het controleren van prestatieverklaringen en hoe zij deze controles duidelijk moeten documenteren. De verantwoordelijkheid voor een solide onderbouwing rust immers bij de prestatieverklaarders binnen de verschillende directies van BZK2.



3 Aandachtspunten en overige onderwerpen

Risico's in IT-Beheer: IB governance en Cloud

Inleiding

Goed IT-beheer is van cruciaal belang voor de uitvoering van de primaire processen en voor de bedrijfsvoering. Daarmee heeft IT-beheer ook consequenties voor de kwaliteit van het financieel beheer.

IB-Governance

IB-Governance is een cruciaal aspect binnen cybersecurity en informatiebeveiliging. Het verwijst naar het raamwerk van processen, regels, richtlijnen en verantwoordelijkheden die zijn vastgesteld om de informatiebeveiliging binnen een organisatie te beheren en te sturen. IB-Governance omvat onder andere het definiëren van beleid en procedures, het toewijzen van verantwoordelijkheden, het uitvoeren van risicobeoordelingen en audits, en het continu monitoren en verbeteren van informatiebeveiligingspraktijken binnen de organisatie.

Wij zien dat binnen BZK (inclusief agentschappen) aandacht is voor het treffen van IB-maatregelen. De te beschermen belangen (TBB's) zijn in beeld en daarover wordt ook gerapporteerd via de IBenP-beelden aan CIO Rijk.

Risico

Vooral agentschappen hebben een beperkte structurele inrichting van processen om (sturings)informatie op te leveren vanuit de eerste lijn, waardoor op dit moment niet altijd sprake is van een sluitende PDCA-cyclus en bijbehorende actuele risicobeelden per systeem. Dit is een risico.

Handelingsperspectief

Wij adviseren om de processen in de eerste lijn zodanig in te richten en uit te voeren dat een sluitende PDCA-cyclus wordt bereikt, teneinde de 2e en 3e lijn over actuele (sturings-) informatie beschikken.

Cloud

Met de introductie van het Rijksbrede (public) cloudbeleid medio 2022 is een verandering in gang gezet voor de informatievoorziening van de Rijksoverheid. BZK heeft een BZK-breed beleidskader Cloud opgesteld waarin onder andere afwegingscriteria zijn opgenomen voor het gebruik van cloud. Hiermee is een goede basis gelegd voor een verantwoord gebruik van cloud toepassingen.
Op basis van input van de onderdelen stelt BZK een centraal cloudregister samen dat centrale monitoring en sturing mogelijk maakt.

Risico’s in IT-Beheer: digitale weerbaarheid

Digitale weerbaarheid
Cyberdreigingen- en incidenten zijn dagelijks in het nieuws. Op het gebied van cybersecurity volgen ontwikkelingen elkaar snel op. De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) waarschuwt in haar cybersecuritybeeld voor de toegenomen dreigingen. Deze dreigingen zorgen ervoor dat organisaties ook digitaal weerbaarder moeten worden om hiertegen bestand te kunnen blijven.

Risico
BZK beschikt over een richtlijn ‘penetratie- en kwetsbaarheidstesten’ die kaders geeft voor de uitvoering en frequentie van beveiligingsonderzoeken. Van agentschappen wordt verwacht dat zij zelf een jaarkalender voor testen opstellen en hierover te rapporteren in het IBenP-beeld aan BZK.

Wij hebben vastgesteld dat nog niet alle agentschappen beschikken over een jaarkalender, waardoor onderzoeken mogelijk niet gestructureerd plaatsvinden.

Handelingsperspectief
Implementeer het proces van penetratie- en kwetsbaarheidstesten door alle onderdelen jaarkalenders te laten op stellen, zodat beveiligingsonderzoeken volgens een gestructureerde en gecontroleerde methode plaatsvinden.

Risico's in IT-beheer: awareness en inzicht

Awareness en inzicht

Voor digitale weerbaarheid is naast beveiligingsonderzoeken ook awareness en inzicht in en reageren op kritieke incidenten van belang. Wij zien dat binnen BZK en ook de agentschappen aandacht is voor awareness op het gebied van informatiebeveiliging en privacy. In de volle breedte vinden awareness-sessies plaats om begrip te creëren om veilig en bewust om te gaan met informatie.
De centrale registratie van kritieke incidenten is in 2024 niet actueel bijgewerkt. Om effectief risicomanagement te kunnen voeren is het van belang om inzicht te hebben in kritieke incidenten en de eventuele samenhang hiertussen. Daarnaast helpt een actuele centrale registratie ook in het juist en volledig kunnen informeren van de bestuurlijke en ambtelijke top.

Risico

Door het ontbreken van een actueel centraal overzicht van kritieke incidenten heeft BZK mogelijk blinde vlekken in het risicomanagement.
BZK kan daarmee niet voldoende effectief sturen op eventuele tekortkomingen om deze tijdig op te kunnen lossen.

Handelingsperspectief

Zorg ervoor dat de onderdelen beter aansluiten op de systematiek die BZK hiervoor heeft ingericht met de richtlijn 'incident management en afhandeling calamiteiten', zoals bijvoorbeeld SSC-ICT incidenten centraal rapporteert. Hierdoor zijn incidenten volgens een uniforme wijze centraal inzichtelijk en kan effectief risicomanagement worden gevoerd.
Dit is ook van belang voor NIS2 compliance.

Aandachtspunten bij financieel beheer: voorschotbetalingen agentschappen

Voorschot betalingen agentschappen via de bijdragen applicatie (DBA)

In 2024 is DBA in gebruik genomen om het bijdragenproces te ondersteunen. In het eerste halfjaar is een beperkt aantal bijdragen aan agentschappen via DBA verwerkt. Een aantal (rechtmatigheids) risico's zijn in DBA afgevangen met geprogrammeerde controles (application controls). Wij hebben die getoetst en de werking daarvan is voldoende. Een aantal controles worden in DBA handmatig uitgevoerd zoals het beoordelen van ingediende begrotingen en offertes. Daarvan hebben wij vastgesteld dat de controles niet zichtbaar worden uitgevoerd c.q. vastgelegd in DBA.

Voorbeeld niet zichtbare uitvoering van een controle

Er wordt met een vinkje aangegeven dat de controle is uitgevoerd, wat niet voldoende is om de rechtmatigheid vast te stellen.

Het risico bestaat dat een vinkje voor akkoord wordt gezet zonder dat de onderliggende controle is uitgevoerd, waardoor niet aan de rechtmatigheidseisen is voldaan.

DBA heeft als application controls ook verplichte velden voor het vastleggen van informatie over te verstrekken voorschotten en over (tussen)rapportages. Gezien het beperkt aantal bijdragen die in het eerste halfjaar via DBA zijn verwerkt, hebben wij nog niet kunnen vaststellen of de verplichte velden toereikend worden ingevuld. Dat gaan wij de komende periode onderzoeken.

Handelingsperspectief

Wij adviseren FEZ om in DBA verplichte velden te laten opnemen waarin duidelijk wordt vastgelegd hoe welke controles zijn uitgevoerd.

Aandachtspunten bij financieel beheer: implementatie systeem Digitale inhuur oplossing Rijk (DioR)

Implementatie DioR nog in doorontwikkeling

De Inhuurdesk (IHD) is verantwoordelijk voor de dienstverlening van de externe inhuur van verschillende departementen. Per begin mei 2024 is het inhuursysteem Digitale inhuur oplossing Rijk (DioR) live gegaan, waarbij het oude inhuursysteem Nétive Job is vervangen. De systemen blijven naast elkaar bestaan, omdat de IHD besloten heeft om voor DioR nieuwe stamdata te produceren en niet te migreren. DioR wordt gebruikt voor het gehele inhuurproces van externen van aanbesteding tot en met het geven van een prestatieverklaring. DioR genereert na het verlenen van de prestatieverklaring automatisch een factuur die ter betaling wordt aangeboden aan het FDC van SZW.

Medio juni 2024 heeft het FDC geconstateerd dat het systeem DioR een aantal facturen dubbel heeft verstuurd met een gewijzigd factuurnummer. Dit heeft in totaliteit geleid tot onrechtmatige betalingen voor €1.3mln voor de ministeries van BZK, FIN, SZW en VWS. De IHD heeft tijdig op het ontstane issue ingespeeld en een root-cause analyse laten uitvoeren door de IT-leverancier Nétive VMS. Er zijn inmiddels aanvullende maatregelen in het systeem doorgevoerd om dergelijke incidenten te voorkomen. Het testen van deze aanvullende maatregelen zal onderdeel uitmaken van ons onderzoek naar de general IT-controls GITC's).

We hebben geconstateerd dat IHD bezig is met het inrichten van Service Level Agreement Management, met afspraken over het volgen van het naleven van de contractuele afspraken en de wijze waarop de leverancier verantwoording aflegt over het beheer.

Wij constateren dat er geen koppeling is gerealiseerd tussen DioR en de ERP-systemen van de afnemende departementen. Dit leidt tot handmatige handelingen in het aanleverproces met een foutgevoelig karakter en er ontstaan verschillen in de informatie tussen de onderliggende administraties. Ook constateren wij dat de technische procesgang in DioR nog niet in voldoende mate functioneel is beschreven.

De ADR voert momenteel een verkennend GITC-onderzoek uit naar DioR. Hierbij nemen we tevens de onderstaande punten mee:

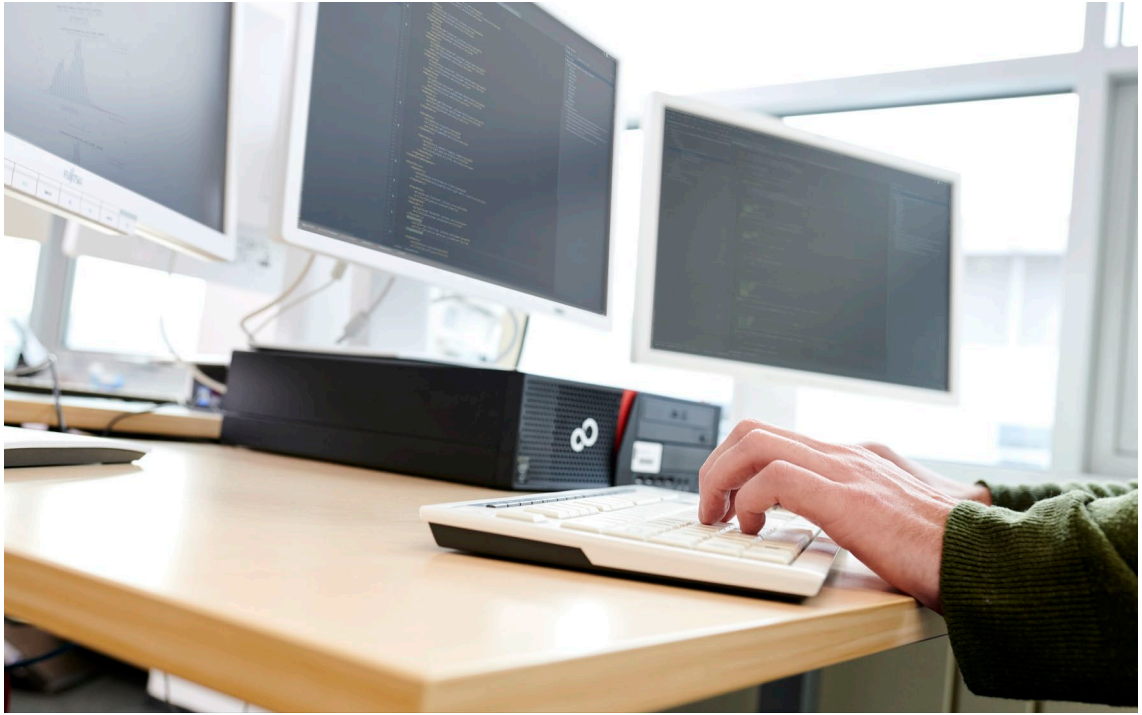
- Het testen van de aanvullende maatregelen ter voorkoming van dubbele facturen.
- De uitfasering van Nétive Job en de integriteit van de stambestanden.

Een volledig GITC-onderzoek is op dit moment niet opportuun, doordat het systeem nog in ontwikkeling is. We zullen gedurende dit controlejaar het ontwikkelproces blijven volgen.

Aandachtspunten bij implementatie systeem Digitale inhuur oplossing Rijk (DioR)

Handelingsperspectief
Ook adviseren wij de IHD om de werking van de general IT-controls te toetsen en de uitkomsten daarvan te delen met de afnemende departementen.

- Verder adviseren wij de IHD om met de afnemende departementen te verkennen of een koppeling kan worden gerealiseerd tussen DioR en de (financiële) ERP-systemen van de afnemers. Dat zou het voordeel geven dat dezelfde informatie in de systemen aanwezig is voor rapportage en analyse doeleinden, waardoor geen handmatige handelingen nodig zijn.



Aandachtspunten agentschappen: SSC-ICT (BZK)

Dossiers Financiële Afspraken SSC-ICT

Het Dossier Financiële Afspraken (DFA) beschrijft de financiële afspraken tussen SSC-ICT en afnemer voor de te leveren services die zijn vastgelegd in de Dienstverleningsafspraken (DVA). De afgelopen jaren was de doorlooptijd voor het ondertekenen van de DFA's lang waardoor er onduidelijkheid kon bestaan over de omvang van de geleverde diensten en de financiële afwikkeling daarvan.

SSC-ICT heeft de DFA-werkwijze in 2024 aangepast door het afsluiten van de DFA's, de facturatie en het afwikkelen van disputen als aparte processen in te richten. Dat heeft erin geresulteerd dat inmiddels 31 van de 37 DFA's al zijn geformaliseerd door de klanten.

Om dit probleem structureel op te lossen is SSC-ICT bezig om een nieuwe werkwijze op te zetten, waarbij de DFA wordt gekoppeld aan de begroting. In de nieuwe situatie zal niet de DFA, maar de DVA waarin de af te nemen dienst expliciet wordt gemaakt, leidend zijn.

Met de bovengenoemde acties lost SSC-ICT het probleem naar behoren op.

Terughalen oude devices SSC-ICT

Het inleverproces van oude devices (laptops, tablets en smartphones), als onderdeel van het Life Cycle Management, was door de situatie rond COVID verstoord, waardoor duizenden oude devices niet waren ingeleverd.

Omdat diverse zachte maatregelen geen significante resultaten opleverden is SSC-ICT sinds februari 2024 gestart met het resetten van de wachtwoorden van de accounts van medewerkers die, ondanks herhaaldelijke verzoeken de oude apparaten niet inleverden.

Het resultaat daarvan is zichtbaar in het inleverpercentage dat begin februari circa 40% bedroeg en ultimo augustus is gestegen tot circa 75%. Van de COVID-periode moesten ultimo 2023 circa 3.000 devices nog worden ingeleverd waarvan inmiddels 2.000 stuks zijn ingeleverd.

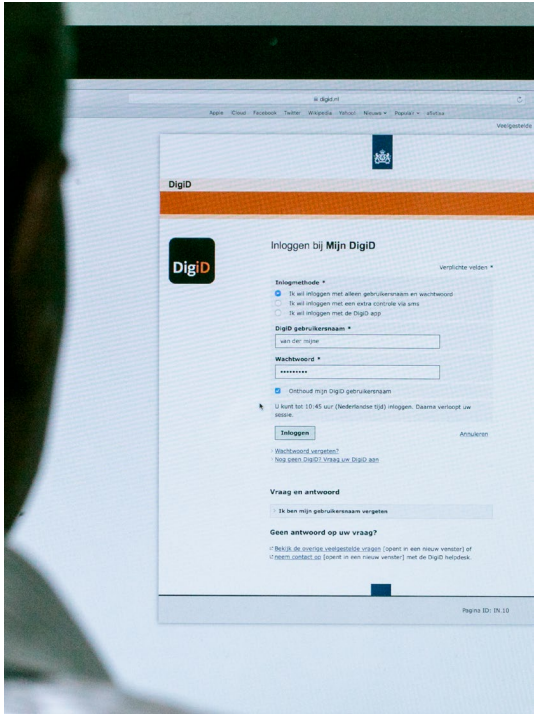
SSC-ICT gaat de komende periode op deze wijze door om oude devices terug te halen.

Aandachtspunten agentschappen: Logius (BZK)

Financieel beheer Logius
Het financieel beheer van Logius kwam de laatste jaren onder druk te staan mede vanwege groei van de organisatie, een hoog personeelsverloop bij de afdeling financiën en control en de leiding van de organisatie, de ingevoerde agile werkwijze en veel nieuwe ontwikkelingen (invoering Onventis, centrale financiering en overgang van KOOP). Daardoor kon een betrouwbare financiële verantwoording pas na veel handmatige werkzaamheden worden opgeleverd.

In 2023 heeft Logius door een externe partij een onderzoek laten uitvoeren om de knelpunten in het financieel beheer inzichtelijk te maken en adviezen ter verbetering te krijgen. Op basis daarvan heeft Logius een verbeterplan (programmaplan 'Bedrijfsvoering, basis op orde') opgesteld met een looptijd tot eind 2025. Daarmee wil Logius het financieel beheer structureel verbeteren.

Daarnaast heeft zij met prioriteit de administratie opgeschoond en als proef voor de financiële verantwoording een halfjaarafsluiting uitgevoerd. Op verzoek van Logius gaan wij de komende periode die tussentijdse afsluiting beoordelen en eventuele verbetervoorstellen doen zodat de financiële verantwoording zonder al te veel handmatige werkzaamheden op het laatste moment kan worden opgeleverd.



Aandachtspunten agentschappen RVB (VRO)

Gebruikersbeheer RVB verbeterd
RVB heeft verdere voortgang geboekt bij het oplossen van de issues in het gebruikersbeheer. Zo heeft RVB een autorisatiematrix en diverse procedures opgesteld en geaccordeerd of gaat een procedure op korte termijn accorderen. Deze procedures richten zich op:

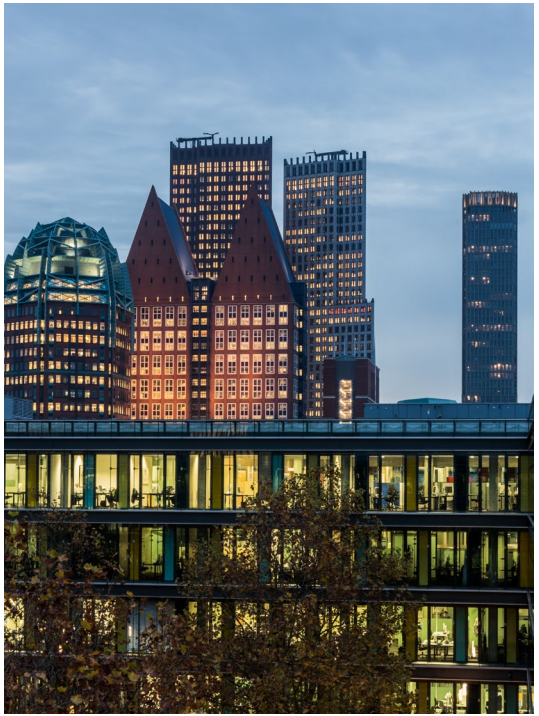
- het beheerst laten verlopen van aanpassingen in de matrix,
- het halfjaarlijks controleren van conflicterende autorisaties
- het intrekken en controleren van in het verleden ontstane conflicten.

In de komende periode zullen wij het bestaan en de werking van de procedures controleren.

Handelingsperspectief
Wij adviseren aandacht te blijven schenken aan het naleven van opgestelde procedures en interne controle te verfijnen op het inhoudelijk gebruik van de (tijdelijk) aanvullend en mogelijk conflicterende rechten van beheerders. Dit aan de hand van logging en andere soorten van vastleggingen en rapportages.

Verbeterde projectadministratie RVB nog niet kunnen onderzoeken
In ons auditrapport 2023 rapporteerden wij dat het RVB was gestart met de opschoning van de projectadministratie en het monitoren van de niet-opgeleverde projecten.

Wij hebben de voortgang daarvan in 2024 nog niet kunnen beoordelen omdat het RVB de daarvoor opgevraagde informatie nog niet heeft aangeleverd. Wij zullen de voortgang in het najaar beoordelen en daarover rapporteren in ons auditrapport.



Aandachtspunten agentschappen:de Huurcommissie (VRO)

DHC wordt toekomstbestendig gemaakt
Door verschillende wijzigingen op het beleidsterrein van De Huurcommissie (DHC) neemt haar werklast significant toe. Om de organisatie toekomstbestendig te maken en haar opdracht duurzaam naar behoren te kunnen uitvoeren, past DHC de organisatie aan en is zij bezig met het vullen van de organisatie. De benodigde (extra) financiering van DHC is nog niet structureel geborgd.

Om grote achterstanden te voorkomen, zet DHC ondertussen veel externe inhuurkrachten in. Desondanks is voor DHC moeilijk om de wettelijke termijnen met betrekking tot huurgeschillen (altijd) na te leven mede omdat dat ook te maken heeft met factoren die buiten de invloedsfeer van DHC liggen. DHC monitort dat en zoekt actief naar mogelijkheden om de prestaties op dat vlak te verhogen.

Mede door de hier genoemde ontwikkelingen die veel werklast opleveren is het DHC niet gelukt om de voorgenomen verbeteringen in de interne beheersing door te voeren en de PDCA-cyclus sluitend te maken met procesbeschrijvingen, het uitvoeren van een risicoanalyse op de financieel beheerprocessen en het periodiek toetsen van de beheersingsmaatregelen waarmee de onderkende risico’s worden afgedekt. Zij heeft wel de adviezen uit de audit op verzoek opgevolgd en een aantal andere activiteiten met betrekking tot het financieel beheer uitgevoerd zoals de vormgeving voor een integrale risicoanalyse en onderzoeken van de datakwaliteit om meer gebruik te maken van beschikbare data.

Aandachtspunten Herstel Veerkracht Plan

Drie mijlpalen voor tweede betaalverzoek HVP gehaald, één in bespreking

De Europese Herstel- en Veerkrachtfaciliteit is bedoeld om de Europese economie duurzamer, digitaler en veerkrachtiger te maken na de COVID-19 pandemie. In 2022 heeft de Raad van de Europese Unie (EU) de financiering van het Nederlandse Herstel- en Veerkrachtplan (HVP) voor duurzaam economisch herstel goedgekeurd. Momenteel bereiden de ministeries van BZK en Financiën het tweede betaalverzoek ad €1,19 miljard voor, dat uiterlijk 15 november 2024 door Financiën moet worden ingediend bij Europese Commissie.

Conform de eis van de EU heeft de ADR een onderzoek uitgevoerd naar de mijlpalen en de doelen van het tweede betaalverzoek en de financieel beheer maatregelen om fraude, corruptie, belangenverstrengeling en dubbele financiering te voorkomen.

Het ministerie van BZK heeft 2 maatregelen in betaalverzoek 2 met de volgende 4 mijlpalen:

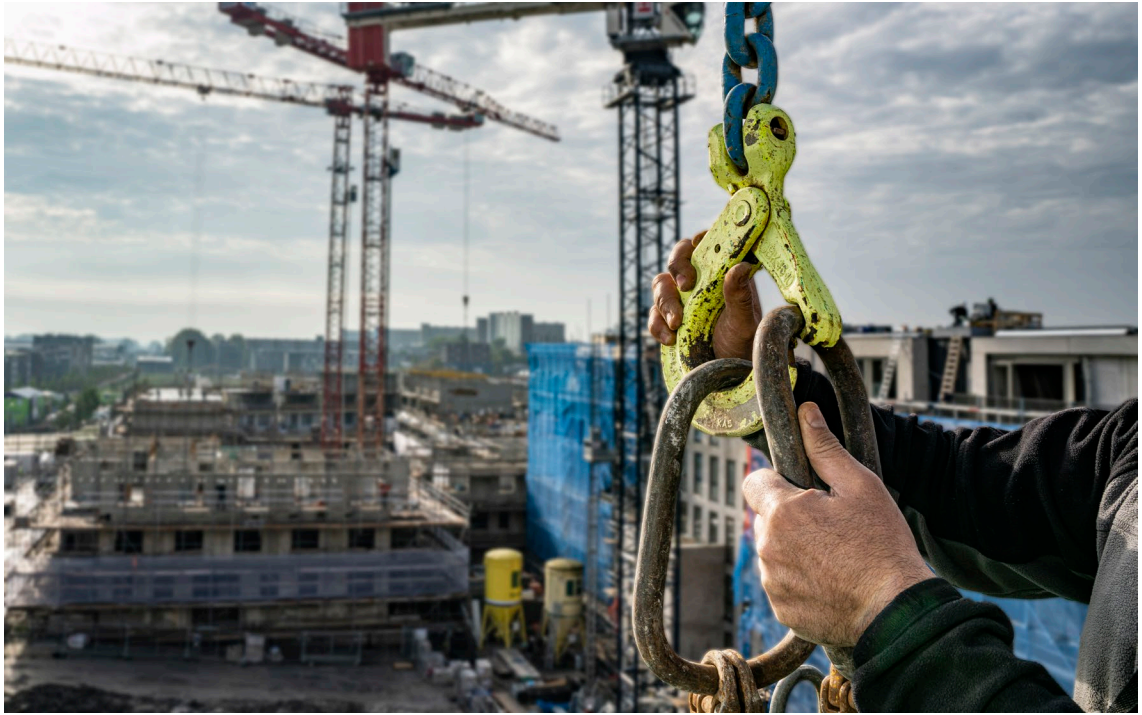
1. Maatregel 3.1 H-3: Regie op de aanbodzijde van de woningmarkt met de mijlpalen:
- 70: Overeenkomsten tussen provincies en gemeenten over de realisatie van 900.000 nieuwe woningen, waarvan 600.000 betaalbare woningen dienen te zijn.
- 71: Systeem voor monitoring van de uitvoering van overeenkomsten die met gemeenten zijn gelanceerd;
- 72: Inwerkingtreding van de wet tot verstelling van de aanvullende maatregelen van de staat om overeenkomsten inzake de bouw van nieuwe woningen te doen naleven.

2. Maatregel 3.1 H-5: Versnellen van proces en procedures bij realiseren woningbouw met de mijlpaal:
- 75: Acties om het planningsproces voor huisvestingsprojecten te versnellen.

Herstel Veerkracht Plan (vervolg)

Wij hebben geconstateerd dat de mijlpalen 70, 71 en 75 door BZK zijn gehaald. Daarbij past de aantekening dat in de plannen van mijlpaal 70 er 583.851 betaalbare woningen terug te vinden zijn in plaats van 600.000, die BZK ook minimaal denkt te realiseren.

Mijlpaal 72 is niet gehaald omdat BZK streeft naar een ambitieuzere wet waardoor het wetgevingstraject is vertraagd. BZK is daaromtrent samen met de programmadirectie HVP van het Ministerie van Financiën in overleg met de Europese Commissie. Zij zijn in overleg met de Europese Commissie om deze mijlpaal door te schuiven naar een volgend betaalverzoek.



Privacy en Algemene Verordening Gegevensbescherming

Rijksbreed AVG onderzoek bij BZK
De afgelopen jaren is het belang van privacy en gegevensbescherming steeds groter geworden. Europese wet- en regelgeving op dit gebied is stringenter geworden met als voornaamste voorbeeld de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) in 2018. Het is aan de Privacy Officer (PO) en Functionaris gegevensbescherming (FG) om afdoende controle en monitoringsactiviteiten uit te voeren teneinde het departement te laten voldoen aan de AVG.

Risico
BZK beschikt niet over een centraal overzicht van uitgevoerde DPIA's en de status van de uitvoering van de DPIA-maatregelen waardoor een risico ontstaat voor de kwaliteit van de (de)centrale aansturing op dit vlak. Wanneer een (recente) DPIA ontbreekt of een maatregel niet of niet volledig wordt uitgevoerd kan dit een mogelijk privacy risico zijn voor BZK, hierin is op dit moment geen volledige inzage.

Handelingsperspectief
Wij adviseren BZK om een centraal overzicht op te stellen met alle DPIA's dat inzicht dat inzicht geeft in de stand van zaken van alle DPIA's en in de kwaliteit van de decentrale aansturing op dit vlak.

Borg daarnaast dat er centraal inzage is in de mitigatie van geconstateerde privacyrisico's uit de DPIA's. BZK heeft aangegeven dat ze bezig is met een verbeterslag om departement-breed inzicht te verkrijgen. Beperkte privacy capaciteit maakt het nog niet mogelijk om een optimaal controle-en monitorstelsel in te richten. Aangegeven is dat de eerste lijn niet afdoende is bemenst waardoor de CISO en (plv.) CPO belast worden met eerstelijnstaken. Hierdoor komen zij minder toe aan advies- en toezichtstaken vanuit de tweede lijn bijvoorbeeld op het gebied van privacy by design en default.

BZK heeft het voornemen om privacyfunctionarissen te werven om de scheiding tussen eerste, tweede en derde lijn te borgen, zodat de CPO zich meer kan focussen op het aansturen van en zicht houden op de kwaliteit van de tweede lijn binnen BZK en het geven van tweedelijnsadviezen aan de beleidskern. Wij onderschrijven dit voornemen van BZK, en wijzen ook op het belang van privacy in het prioriteren van werkzaamheden.

Belangrijke ontwikkelingen in de Informatiebeveiliging en AI

NIS2

De Network and Information Security directive (NIS2-richtlijn) is de opvolger van de NIS-richtlijn. Deze is vastgesteld door de Europese Unie en bedoeld om de cyberbeveiliging en de weerbaarheid van essentiële diensten in EU-lidstaten te verbeteren. De NIS2-Richtlijn vergroot de reikwijdte van de eerste richtlijn door meer sectoren te omvatten. Daarnaast stelt de richtlijn strengere beveiligingsnormen en meldingsvereisten voor incidenten.

Wij constateren dat BZK de uitdagingen rondom NIS2 in beeld heeft. Er is een plan van aanpak aanwezig voor de implementatie van eventuele extra maatregelen. Dit plan is gebaseerd op de kennis over het implementeren van NIS2 in nationale wetgeving. Deze wetgeving dient nog definitief aangenomen te worden door de Tweede Kamer. Wij zullen deze ontwikkelingen blijven volgen.

Artificial Intelligence (AI)

Algoritmes en AI zijn volop in ontwikkeling en worden steeds vaker ingezet. Het gebruik van AI maakt het mogelijk om complexe processen te automatiseren en te sturen. Dit brengt nieuwe technische, maatschappelijke en ethische vraagstukken met zich mee. Tegelijkertijd is de regelgeving en het beheerstelsel rondom AI nog volop in ontwikkeling. Goede controle op AI is van groot belang voor een verantwoorde implementatie van AI-toepassingen.

De governance van AI verloopt nu volgens huidige IB-processen. Specifieke risico’s zoals ethische afwegingen zijn daardoor mogelijk niet volledig in beeld. BZK heeft hiertoe een concept richtlijn Generatieve AI opgesteld.

Wij volgen de ontwikkelingen op het gebied van governance rondom algoritmes en AI.

Duurzaamheidsverslaggeving en CSRD

Informatie over duurzaamheidsonderwerpen is verspreid over verschillende rapportages en gedeeltelijk te relateren aan Europese standaarden

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. In de 'Hoofdlijnennota rijksbreed beeld ADR 2023' hebben we aandacht gevraagd voor de duurzaamheidsverslaggeving binnen de Rijksoverheid. We merkten op dat de verantwoording over duurzaamheid onder andere in de jaarrapportage Bedrijfsvoering Rijk en de rapportage over de CO_2-prestatieladder, vrij divers is voor wat betreft onderwerpen, organisatie en verantwoordelijkheden en vorm en frequentie. Kortom, een breed speelveld waarin beperkt sprake is van centrale coördinatie en richtlijnen.

Handelingsperspectief

Ons advies was om meer regie en coördinatie te organiseren op de rijksbrede duurzaamheidsverslaggeving. Een noodzaak wanneer de CSRD- of vergelijkbare richtlijnen ook gaan gelden voor de rijksoverheid, maar ook om het risico te beperken van overlap, gebrek aan transparantie en inefficiënt gebruik van schaarse middelen.

Een complexiteit is dat de formulering van de ESRS-thema's, die ontworpen is voor bedrijven, niet altijd goed aansluit bij de terminologie die binnen de rijksoverheid wordt gehanteerd. 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 dit interim-auditrapport presenteren wij het eerste deel van het onderzoek: over welke duurzaamheidsonderwerpen momenteel reeds informatie wordt verschaft. In de komende maanden zullen we de werkwijze en organisatie van de duurzaamheidsinformatie in beeld brengen.

BZK

Er zijn per departement logischerwijs verschillen in de mate van aandacht voor de diverse thema's. BZK rapporteert grotendeels over de thema's:

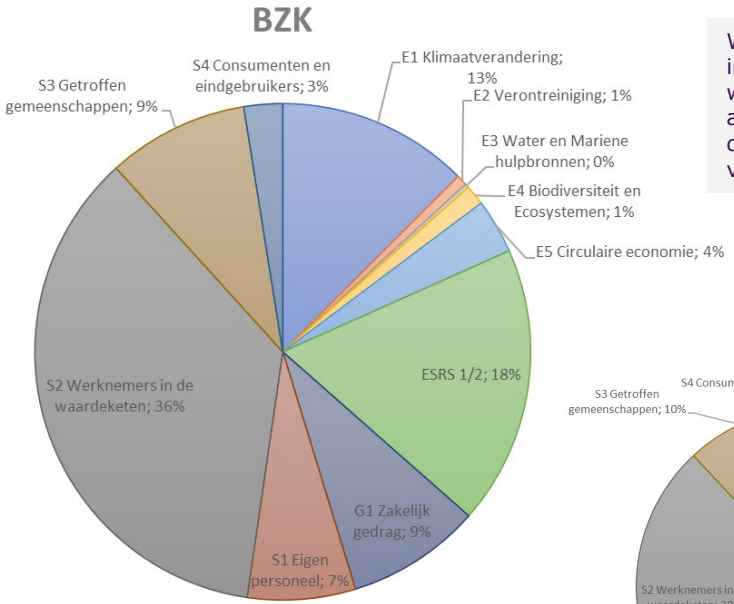
- Werknemers in de waardeketen (S2)
- Algemene vereisen en algemene toelichtingen (ESRS1/2)
- Klimaatverandering (E1).

Voorbeelden van thema's waar BZK minder prominent over rapporteert:

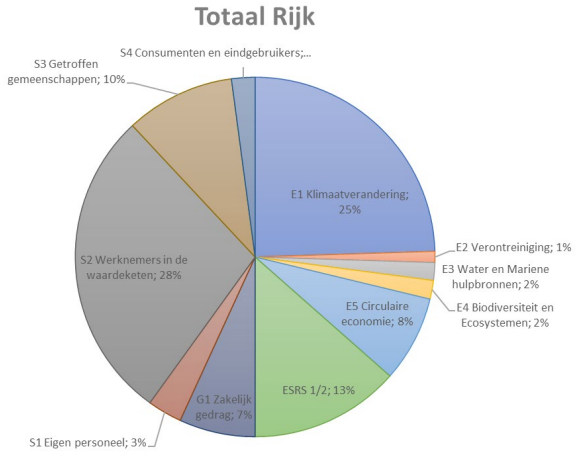
- Eigen personeel (S1)
- Circulaire economie (E5).

Relatieve verdeling van door BZK gerapporteerde duurzaamheidsinformatie

ESRS-thema	Toelichting
ESRS E1: Klimaatverandering	Broeikasgasemissies, risico's en kansen door klimaatverandering, reductiedoelstellingen.
ESRS E2: Verontreiniging	Maatregelen en emissies van verontreinigende stoffen, naleving van milieunormen.
ESRS E3: Water- en mariene hulpbronnen	Waterverbruik, impact op waterbronnen, maatregelen voor waterbeheer
ESRS E4: Biodiversiteit en ecosystemen	Bescherming van biodiversiteit, impact op ecosystemen, herstelmaatregelen.
ESRS E5: Materiaalgebruik en circulaire economie	Grondstofgebruik, afvalbeheer, circulaire economie initiatieven.
ESRS S1: Eigen personeel	Arbeidsomstandigheden, gezondheid en veiligheid, diversiteit en inclusie.
ESRS S2: Werknemers in de waardeketen	Arbeidsrechten, veiligheid, en gezondheid van werknemers in de waardeketen.
ESRS S3: Getroffen gemeenschappen	Impact op lokale gemeenschappen, betrokkenheid en rechten van inheemse volkeren.
ESRS S4: Consumenten en eindgebruikers	Productveiligheid, privacy, en consumentenrechten.
ESRS G1: Zakelijk gedrag, bestuur en organisatie	Structuur en functioneren van bestuur, ethisch beleid, compliance en anti-corruptiemaatregelen.



Wij adviseren BZK om met dit inzicht na te gaan of en zo ja welke mogelijke witte vlekken aanwezig zijn in de thema's die qua duurzaamheid van belang zijn voor BZK.



4 Rijksbrede bedrijfsvoering

Ontwikkelingen in de rijksbrede bedrijfsvoering

Risicomanagement voor digitale weerbaarheid van departement overstijgende ketens

In toenemende mate wordt er departement overstijgend in ketens samengewerkt aan de realisatie van gemeenschappelijke opgaven en ketendoelen. Daarbij zijn de betrokkenen partijen steeds meer afhankelijk van betrouwbare informatie. Die betrouwbaarheid staat voortdurend onder druk als gevolg van dreigingen op het digitale vlak die in aantal, complexiteit en professionaliteit steeds verder toenemen.

De Interdepartementale Commissie Bedrijfsvoering Rijksdienst (ICBR) heeft het CIO beraad opdracht gegeven tot rijksbrede inrichting van risicomanagement. Om hieraan gehoor te geven is er een project gestart waarvoor de CISO Rijk gedelegeerd opdrachtgever is. In 2022/2023 is de scope en reikwijdte van het project vastgesteld via afstemming met de dgDOO, de CIO Rijk, de CISO Rijk, de Stuurgroep Digitale Weerbaarheid, de CISO raad en het CIO beraad. Het CIO beraad heeft in 2023 het projectplan goedgekeurd waarna in januari 2024 het project officieel van start is gegaan. In eerste instantie is het niet gelukt om alle departementen de betrekken bij de uitvoer van het project, waardoor vertraging is opgelopen ten opzichte van de initiële planning. Op dit moment zijn alle departementen vertegenwoordigd in de projectgroep, in de klankbordgroep of op andere wijze bij het project betrokken en loopt het project volgens het herziene tijdspad. Het beleidsdocument voor risicomanagement en het implementatiekader van departement overstijgende ketens zijn in concept gereed.

De Stuurgroep Digitale Weerbaarheid heeft in juni 2024 gevraagd om de toegevoegde waarde van het beleid te valideren voorafgaand aan de doorgeleiding naar de CISO raad en het CIO beraad voor goedkeuring.

Wanneer binnen een departement overstijgende keten geen gezamenlijk geaccepteerd risicomanagementbeleid wordt toegepast en er geen gemeenschappelijke risicotaal wordt gesproken, kan het samenwerken in een departement overstijgende keten en het uitwisselen van informatie binnen de keten op zichzelf al een risicovolle aangelegenheid zijn.

Hierdoor wordt het mogelijk dat effecten van niet of onvolledig beheerste risico’s in de keten opnieuw optreden en de continuïteit van de dienstverlening in gevaar brengen met alle gevolgen van dien. Door het uitvoeren van het nieuwe risicomanagementbeleid voor digitale weerbaarheid van departement overstijgende ketens kunnen concentraties en stapelingen van risico’s worden herkend en kan risicobehandeling beter worden afgestemd.

Ontwikkelingen in de rijksbrede bedrijfsvoering (vervolg)

Hiernaast is ook beter inzicht in afhankelijkheden tussen ketenpartners en in de risico's op het gebied van de digitale weerbaarheid die gevolgen kunnen hebben voor de betrouwbaarheid van de voor de keten relevante informatie en voor het ongestoord functioneren, ofwel de continuïteit, van de departement overstijgende keten. Wij adviseren om dit beleid te effectueren wanneer de toegevoegde waarde hiervan is aangetoond.

Rijksbreed IT-beheer

DG DOO heeft op 12 juli 2024 het herziene plan van aanpak voor Rijksbreed IT beheer goedgekeurd. Dit project heeft als doel om te komen tot een PDCA-cyclus waarin departementen, agentschappen en ICT dienstverleners de CIO Rijk periodiek informeren over de wijze waarop zij hun IT beheren.

Begin mei 2024 is een koplopergroep geformeerd van vier departementen, waarmee in overleg het normenkader en de procesbeschrijving worden opgesteld. Het op te stellen kader dient rekening te houden met de bestaande en voorziene jaarlijkse uitvragen rond IT-beheer en informatieveiligheid. Overlap binnen de vraagstelling dient te worden vermeden en/of afgestemd te worden, zodat voor een onderdeel eenmalig informatie aangeleverd behoeft te worden.

Op dit moment heeft CIO Rijk geen actueel inzicht in de status van het Rijksbreed IT-beheer ten opzichte van al dan niet bestaande kaders, en hiermee kan het haar monitorende rol onvoldoende invullen. Hierdoor is geen volledig inzicht in risico's door tekortkomingen in het Rijksbreed IT-beheer buiten bestaande uitvragen zoals het Informatie Beveiligings Beeld (IBB). Hiervoor is een plan van aanpak opgesteld waarop wij op dit moment voldoende voortgang zien.

Wij adviseren CIO Rijk om de uitvoer van het plan van aanpak voort te zetten, teneinde een volledig inzicht te krijgen in het Rijksbrede IT-beheer.

Risico's bij het uitvoeren van het plan van aanpak liggen in een beperkte medewerking van de departementen, het niet beschikbaar zijn van de door CIO Rijk gevraagde informatie of onvoldoende capaciteit bij CIO Rijk om de resultaten te verwerken, waardoor uitvoer van het project in gevaar kan komen.

Om het risico voor de medewerking van departementen te mitigeren is de koplopergroep in het leven geroepen. Via de leden kunnen ook de bestaande kennis en best practices aanwezig bij de deelnemende departementen worden ingezet bij het opstellen van het normenkader en de methodiek van de uitvraag.

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 IV en VII, het Gemeentefonds, het Provinciefonds en het BES Fonds. 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 ministers, de staatssecretarissen en de secretarissen-generaal van de ministeries van Binnenlandse Zaken en Koninkrijksrelaties en Volkshuisvesting en Ruimtelijke Ordening 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 de ministeries van Binnenlandse Zaken en Koninkrijksrelaties en Volkshuisvesting en Ruimtelijke Ordening. 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: 11 oktober 2024

Handtekening:

Colofon

Interim-auditrapport 2024
ministerie van Binnenlandse Zaken en Koninkrijksrelaties
ministerie van Volkshuisvesting en Ruimtelijke Ordening

Datum
11-10-2024

Kenmerk
BZK-VRO 2024-0000461268

Auditdienst Rijk
Korte Voorhout 7
2511 CW Den Haag