Auditdienst Rijk
Ministerie van Financiën

Interim-auditrapport 2022 ministerie van Buitenlandse Zaken (V) en Buitenlandse Handel en Ontwikkelingssamenwerking (XVII)

Colofon

Titel	Interim-auditrapport 2022 ministerie van Buitenlandse Zaken (V) en Buitenlandse Handel en Ontwikkelingssamenwerking (XVII)
Kenmerk	2022-0000263830
Inlichtingen	Auditdienst Rijk Korte Voorhout 7 2511 CW Den Haag

Inhoud

1 Inleiding—4
1.1 Algemeen—4
1.2 Doel en doelgroepen—4
1.3 Leeswijzer—4

2 BZ op weg naar 'in control'—5
2.1 Opvolging bevindingen auditrapport 2021—5
2.2 Overige onderwerpen en ontwikkelingen—5

3 Financieel beheer richting een hoger niveau—7
3.1 Inleiding—7
3.2 Voortgang bevindingen in het beheer uit 2021—7
3.3 Regie op informatiebeveiliging verschuift naar lijnorganisatie—7
3.4 Voortgang opvolging overige bevindingen in het beheer—10
3.4.1 Voortgang plan van aanpak 'Versterking BZ in control'—10
3.4.2 Risicoparagraaf in bemo's—12
3.4.3 Spendanalyse bij inkopen—12
3.4.4 Payment Factory ondersteunt het betaalproces—12
3.4.5 Eindejaarsdruk—13

4 Overige onderwerpen en ontwikkelingen—14
4.1 Inleiding—14
4.2 Verwerkingsregister onderhanden en afhandeling inzageverzoeken verbeterd—14
4.3 Beperkte speelruimte in de planning van nieuwe IT-systemen; implementatie is haalbaar mits geen nieuwe tegenslagen—15
4.4 Juiste registratie verplichtingen is een aandachtspunt—16
4.5 Ontwikkelingen Invest International BV—16

5 Ondertekening—17

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 2022 bij ministerie van Buitenlandse Zaken (V) en Buitenlandse Handel en Ontwikkelingssamenwerking (XVII), in het vervolg aangeduid als 'BZ' hebben verricht. Daarbij wordt aangetekend dat onze onderzoeken zich in wisselende stadia van uitvoering bevinden. 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

Dit rapport is opgesteld voor de ministers en de secretaris-generaal en wordt tevens verstrekt aan de leden van het Audit Committee, de Managementraad, de directeur Financieel-Economische Zaken en de Algemene Rekenkamer.

De minister van Buitenlandse Zaken (BZ) en de minister voor Buitenlandse Handel en Ontwikkelingssamenwerking (BHOS) zijn een ieder verantwoordelijk voor hun eigen begroting en stellen daarom ieder een jaarverslag op. De organisatie van de bedrijfsvoering van het ministerie is niet gesplitst. Beide ministers maken gebruik van hetzelfde apparaat en hebben de verdeling van de verantwoordelijkheid voor de bedrijfsvoering expliciet vastgelegd. De minister van Buitenlandse Zaken is verantwoordelijk voor de integrale bedrijfsvoering, met uitzondering van de procesmatige beheersing van de activiteitencyclus. De minister voor Buitenlandse Handel en Ontwikkelingssamenwerking is verantwoordelijk voor de opzet en werking van het proces van het activiteitenbeheer, inclusief het bijbehorende voorschottenbeleid en -beheer.

De ADR is de interne auditdienst van het Rijk. Voor openbaarmaking van de door de ADR aan BZ uitgebrachte rapporten gelden de voorschriften uit de Wet open overheid. De minister van Financiën stuurt elk halfjaar een overzicht van door de ADR uitgebrachte rapporten naar de Tweede Kamer.

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 2);
- overige onderwerpen en ontwikkelingen (hoofdstuk 3).

2 BZ op weg naar 'in control'

In dit hoofdstuk geven wij een samenvatting van de voortgang op de bevindingen uit het auditrapport 2021. Daarnaast behandelen wij de belangrijkste ontwikkelingen in 2022, die kunnen leiden tot nieuwe beheerbevindingen vanuit onze wettelijke controletaak. Ook eventuele overige onderwerpen die van belang zijn voor een goede bedrijfsvoering zullen wij hier benoemen.

2.1 Opvolging bevindingen auditrapport 2021

BZ heeft dit jaar met de nodige uitdagingen te kampen. De effecten van COVID-19 op de organisatie zijn steeds weliswaar minder zichtbaar, echter de nasleep van Afghanistan crisis loopt nog en de oorlog in Oekraïne, die inmiddels een halfjaar gaande is, vergt de nodige inspanningen. Deze uitdagingen leggen druk op de bedrijfsvoering van BZ. Desondanks heeft BZ weer stappen gezet om het financieel beheer verder te verbeteren.

Voor onze over 2021 gerapporteerde lichte bevinding op *regie op informatiebeveiliging* zien wij, mede door het project Olympia, verbeteringen ten aanzien van incidentmanagement, de accreditaties van systemen, bewustwording van medewerkers en borging van sturing en monitoring op de verbeteringen op organisatieniveau. Eind 2022 zal dit project aan de Managementraad decharge vragen. De regie op informatiebeveiliging verschuift dan naar de lijnorganisatie. Bij de accreditaties van niet-BZ systemen, soms al jarenlange trajecten, zien wij nog weinig voortgang en zijn acties op bestuurlijk niveau nodig. Op onderdeel toegangsbeveiliging, bij de implementatie van het 'gesloten tenzij'- beleid, wordt een meerjarenprogramma gestart, dat alleen met commitment van de lijnorganisatie succesvol kan zijn.

BZ heeft een overkoepelend plan van aanpak '*Versterking BZ in control*' opgesteld. Dit plan bevat een drietal pijlers: oplossen van (oorzaken) van herhalende fouten, versterking interne beheersing en versterking toezicht. Alle pijlers bevatten onderliggende deelprojecten met acties op continue, korte, middellange en lange termijn. De termijn is mede afhankelijk van de complexiteit en afhankelijkheid van de implementatie van nieuwe systemen zoals IMPACT. Het is een veelomvattend plan, waar naast de inzet van FEZ, veel commitment vanuit de lijnorganisatie nodig is. Wij zien dat voortgang is geboekt op nagenoeg alle deelprojecten en wij verwachten dat concrete verbeteringen vanaf 2023 merkbaar zullen zijn.

Verder is bij *betalingsorganisatie* bij een deel van de banken de Payment Factory uitgerold, met aandacht voor toereikende beheersmaatregelen. Is de spendanalyse verder doorontwikkeld, maar nog niet geschikt om als borging van de rechtmatigheid te dienen en tot slot zien wij ontwikkelingen op de aanpak van de *eindejaarsdruk*.

2.2 Overige onderwerpen en ontwikkelingen

BZ was eind 2021 nog niet AVG-compliant onder meer op de onderdelen verwerkingenregister en procedure afhandeling inzageverzoeken. De functionaliteit van het verwerkingsregister is nog niet op orde. BZ werkt aan het verbeteren daarvan. Wel zien wij positieve ontwikkelingen in de afhandeling van inzageverzoeken, die binnen de wettelijke termijn zijn afgewikkeld.
De AP heeft BZ in februari 2022 een boete en last onder dwangsom gegeven wegens het ontoereikend informeren van betrokkenen en het onvoldoende waarborgen van de beveiliging van de verwerking van persoonsgegeven in de visumapplicatie NVIS. Nog niet alle verbeteringen zijn doorgevoerd; het is nog niet duidelijk of dit haalbaar is binnen de door de AP gestelde termijn.

BZ koerst vooralsnog af op implementatie per 1 januari 2023 van het nieuwe bedrijfsvoeringssysteem (SAP en BMS) en de activiteitenapplicatie (IMPACT). Ook het managementinformatiesysteem (MI BZ) moet worden aangepast bij implementatie van deze nieuwe systemen en speelt een belangrijke rol bij de dataconversie. Het tijdspad is erg krap, mogelijke tegenvallers kunnen leiden tot een latere implementatie en gevolgen hebben voor de afhankelijke systemen. Het is van belang de samenhang van de tijdpaden en (alternatieve) scenario's te blijven bewaken en integrale scenario's te overwegen. Het ultieme fallbackscenario is voorlopig continueren van de huidige situatie, waarbij IMPACT alleen het eerste deel van de activiteitencyclus ondersteunt als stand-alone systeem en SAP en MI BZ in hun huidige vorm operationeel blijven.

3 Financieel beheer richting een hoger niveau

3.1 Inleiding

Als onderdeel van onze wettelijke taak onderzoeken wij of de door ons geselecteerde processen van het beheer voldoen aan de normen uit de comptabele wet- en regelgeving. Onder beheer verstaan we het begrotingsbeheer, financieel beheer, materiële bedrijfsvoering en de daartoe bijgehouden administraties. Deze eisen zijn verder uitgewerkt en samengevat in de Regeling financieel beheer van het Rijk.

In dit hoofdstuk behandelen wij de follow-up van de bevindingen die wij medio maart 2022 hebben gerapporteerd in ons auditrapport 2021.

3.2 Voortgang bevindingen in het beheer uit 2021

In onderstaande tabel wordt een overzicht gegeven van de bevindingen in het beheer ultimo 2021. Selectie vindt plaats op basis van het belang van de processen en de in die processen onderkende risico's. 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. Daarnaast is sprake van overige bevindingen in het beheer, deze bevindingen kunnen, bij onvoldoende voortgang, alsnog leiden tot een bevinding met een weging.

Figuur 1: overzicht bevindingen ultimo 2021

Bevinding	**Verantwoordelijk organisatieonderdeel**	**2018**	**2019**	**2020**	**2021**
Fraude- en corruptierisico's	OS-directies en posten	■	■	▲	✓
Regie op informatiebeveiliging	IDI	■	■	■	▲

▲ licht ■ gemiddeld • ernstig √ opgelost

In de navolgende paragraaf zullen wij voor de lichte bevinding op 'regie op informatiebeveiliging' ingaan op de stand van zaken. In paragraaf 3.4. zullen wij de voortgang van de overige bevindingen uit het auditrapport 2021 nader toelichten en in hoofdstuk 4 de overige onderwerpen. In dit interim-auditrapport vindt geen nieuwe weging plaats.

3.3 Regie op informatiebeveiliging verschuift naar lijnorganisatie

De afgelopen jaren hebben wij consequent aandacht gevraagd voor diverse aspecten van de informatiebeveiliging (IB). In ons auditrapport 2021 noteerden wij een lichte bevinding inzake dit onderwerp. Wij vroegen met name aandacht voor de volledige accreditatie van systemen, het blijven werken aan het wegnemen van de resterende kwetsbaarheden en borging van sturing en monitoring op de verbeteringen op organisatieniveau. Mede door het project Olympia zien we verbetering op deze gebieden.

Plan van aanpak Olympia fase 3

In 2022 is het project Olympia fase 3 gestart om opvolging te geven aan de aanbevelingen van de Algemene Rekenkamer (AR) in het Verantwoordingsonderzoek 2021 (VO 2021) en die van ons, zoals aangegeven in het Auditrapport 2021. Onze verbeterpunten zijn voldoende geadresseerd in het Plan van Aanpak (PvA). Activiteiten zijn langs vijf sporen gepland tot en met december 2022. Dan moet de projectmatige sturing en monitoring vanuit het Olympia project zijn ondergebracht in de lijnorganisatie. Eind 2022 zal decharge worden gevraagd aan de Managementraad. Wij hebben de voortgang van de realisatie van het PvA

voor Olympia Fase 3 getoetst als onderdeel van de interimcontrole. Wij zien dat activiteiten goed zijn opgepakt en dat verbetering is gerealiseerd ten aanzien van incidentmanagement, accreditaties van systemen, bewustwording van medewerkers en borging van sturing en monitoring op de verbeteringen op organisatieniveau. Aandacht is nodig voor de volledige accreditatie van BZ-systemen en voor de accreditatie van niet-BZ systemen. Voor de implementatie van het 'gesloten tenzij'-beleid wordt een meerjarenprogramma gestart, dat alleen met commitment van de lijnorganisatie succesvol kan zijn.

Spoor 1 Governance en spoor 4 Incidentmanagement
De evaluatie van het incidentmanagementproces heeft in maart 2022 geleid tot een aangepaste procesbeschrijving met bijgewerkte impact- en urgentietabellen om de ernst van een informatiebeveiligingsincident of datalek te bepalen op een vijfpuntsschaal. De ernst is bepalend voor de verdere communicatie en verantwoordelijkheid voor de afhandeling. Daarmee is invulling gegeven aan ons advies om eenduidige escalatiecriteria te definiëren, zodat duidelijk wordt bij welk soort incidenten wanneer dient te worden geëscaleerd in de lijn.
Bij evaluatie van het incidentmanagementproces in 2020 is de noodzaak voor de automatisering van het incidentmanagementproces onderkend. Volgens planning wordt in oktober 2022 een generieke tool (app) binnen Sharepoint in gebruik genomen voor de registratie en afhandeling van informatiebeveiligingsincidenten. De evaluatie van de overige drie beleids- en procesdocumenten, met mijlpalen in december 2022, is reeds opgestart.

Spoor 2 Risicomanagement en accreditaties
Accreditaties
Een informatiesysteem is accreditatiewaardig (plichtig) als het gerubriceerde gegevens verwerkt. Voor negen van de vijftien accreditatiewaardige BZ-systemen is een volledige accreditatie door middel van een FATO (Full Approval to Operate) verleend. Voor vijf accreditatiewaardige operationele BZ-systemen is nog sprake van een tijdelijke accreditatie middels een IATO (Interim Approval te Operate). Voor één operationeel accreditatiewaardig systeem worden de voorbereidende werkzaamheden voor een IATO-aanvraag uitgevoerd; wij merken daarbij op dat BZ hiervoor afhankelijk is van andere ministeries. BZ maakt ook gebruik van accreditatiewaardige niet-BZ-systemen. De drie EU-systemen zijn voorzien van een Statement of Compliance, waarbij aandacht is voor tijdige verlenging. Over de accreditatie van de overige zes niet-BZ-systemen wordt overleg gevoerd met andere ministeries. Deze trajecten zijn al enige jaren geleden in gang gezet. Wij zien nagenoeg geen voortgang op deze dossiers.
Wij benadrukken nogmaals het belang om naar een volledig duurzame accreditatie door middel van FATO's toe te werken. Voor de eigen systemen heeft BZ hier een verbetering laten zien, maar er zijn nog vijf BZ-systemen met een tijdelijke accreditatie. Voor accreditatie van zes niet-BZ-systemen is meer urgentie en inspanning bij andere ministeries nodig. Wij adviseren BZ hiervoor meer aandacht te vragen op bestuurlijk niveau.

Implementatie specifieke hoofdstukken BZ Baseline Informatiebeveiliging
De directie Veiligheid, Crisiscoördinatie en Integriteit (VCI) en directie Informatievoorziening en Digitale Innovatie (IDI) hebben ieder een inventarisatie gemaakt van de implementatie van beveiligingsnormen uit de vernieuwde Baseline Informatiebeveiliging BZ. De inventarisatie van VCI geeft een goed beeld van de invulling van beveiligingsnormen uit de hoofdstukken SG, BVA, DHF en HDPO. In een memo is samenvattend weergegeven waar verbetering nodig is. In het evaluatiedocument van IDI-Information Security Centre (IDI-ISC) blijkt niet voor alle beveiligingsnormen uit de hoofdstukken CIO en CISO duidelijk wat de bevindingen van de inventarisatie zijn. Daarnaast kunnen we geen 1-op-1 aansluiting maken tussen de inventarisatie en het plan voor implementatie. Als gevolg daarvan worden mogelijk niet alle minimale beveiligingsnormen uit de hoofdstukken IDI en CISO ingericht.

Wij vragen IDI-ISC deze 1-op-1 aansluiting te maken en zullen hierop terugkomen bij de eindcontrole.

Opvolging maatregelenplannen kritieke systemen
De systeemeigenaren zijn verantwoordelijk voor de opvolging van de maatregelen zoals opgenomen in de maatregelenplannen. Zij worden hierbij ondersteund door het IDI-ISC, dat gebruik gaat maken van een nieuw Informatiebeveiliging & Privacy Dashboard. Het Dashboard is in september besproken in de Managementraad en zal periodiek worden geagendeerd om de voortgang te monitoren, zoals vermeld bij spoor 5.

Spoor 3 Toegangsbeveiliging
Implementatie 'gesloten tenzij'-beleid
BZ is overgegaan van een 'open tenzij'-beleid naar toegang tot informatie op basis van 'need-to-know'. Het beleid 'Toegang tot BZ-informatie' en het 'implementatieplan op hoofdlijnen' zijn goedgekeurd door de Managementraad. Het implementatieplan is verder uitgewerkt de Programmabrief 'Toegang tot BZ-informatie'. Op basis daarvan heeft de Managementraad besloten een externe programmamanager onder IDI aan te stellen voor de nadere uitwerking in een plan van aanpak. In de Programmabrief is vermeld dat voor de uitvoering van dit programma met name capaciteit nodig is van IDI, voor alle technische maatregelen en voor de lead in de uitvoering van het programma. Uitgangspunt is dat de lijnorganisatie zo min mogelijk wordt belast. Het programma betreft alle BZ-informatie, alle BZ-informatiesystemen en alle gebruikers van die informatie(systemen).
Wij merken daarbij op dat dit een omvangrijk, complex, meerjarig programma is met veel afhankelijkheden met lopende trajecten/IT-ontwikkelingen. Wij begrijpen dat IDI de lead neemt en dat het voor de lijnorganisatie wenselijk is zo min mogelijk te worden belast, echter het programma kan alleen succesvol kan zijn met draagvlak, kennis, capaciteit en inspanning van de lijnorganisatie. Het is aan te bevelen daar – parallel aan het opstellen van een plan van aanpak - in de jaarplannen 2023 aandacht aan te besteden.

Bewustwording medewerkers
In het eerste halfjaar is veel aandacht besteed aan awareness-trainingen op gebied van informatiebeveiliging en AVG. Deze activiteiten volgen uit het 'Plan van Aanpak verdere ontwikkeling informatieveiligheid en privacy BZ 2021-2023' en werkplannen die twee keer per jaar worden vastgesteld. Er is een trainingsprogramma met daarin extra aandacht voor diverse doelgroepen binnen BZ, zoals IB-coördinatoren, nieuwe medewerkers en posten. Ook heeft een gesprek plaatsgevonden met de nieuwe bewindslieden en de informatiebeveiliging daaromtrent. Verder worden op intranet regelmatig artikelen geplaatst om het beveiligingsbewustzijn van de medewerkers te vergroten. Om het niveau van kennis te meten en te bepalen welke volgende activiteiten prioriteit behoeven, speelt BZ meerdere keren de serious game 'Are You Secure'. In het voorjaar van 2022 heeft de tweede ronde plaatsgevonden, de derde ronde vindt plaats in het najaar.

Spoor 5 Inbedding in de organisatie
Het project Olympia voorziet in een centrale sturing en monitoring van het oplossen van de bevindingen. BZ is reeds gestart met het maken van afspraken om de activiteiten van het project Olympia onder te brengen in de bestaande lijnorganisatie. Zo wordt de coördinatie van accreditatieonderzoeken belegd bij de Compliance Officer en wordt de review op kritieke en niet-kritieke systemen belegd bij het Risicomanagementteam van IDI-ISC.
BZ heeft een PDCA-cyclus ingericht om de naleving van informatiebeveiliging en AVG te monitoren en waar nodig verbeteringen door te voeren. Het Informatiebeveiliging & Privacy Dashboard is een hulpmiddel dat inzicht geeft in de status van kritieke systemen die in productie zijn en de gegevensbescherming van hoog risico verwerkingen. Het Dashboard is een Exceldocument dat handmatig wordt samengesteld op basis van informatie uit verschillende bronnen. Het is de

bedoeling dat alle IB-bronnen in de nieuwe GRC-tool worden opgenomen. Het IB & Privacy Dashboard en begeleidend memo zijn op 21 september jl. in de Managementraad besproken. De systeemeigenaren pakken de oranje en rood gemarkeerde zaken op met ondersteuning van IDI-ISC. Het Dashboard zal periodiek in de Managementraad worden besproken.
Het is van belang ook sturing en monitoring op verbeteringen op organisatieniveau te borgen. Na decharge van het project zal de stuurgroep Olympia worden ontbonden en zullen de IB-gerelateerde activiteiten worden aangestuurd via een in te richten IB-Managementoverleg, naar voorbeeld van het AVG-Managementoverleg. De kandidaat-leden van het IB-Managementoverleg zijn de BVA, CIO en CISO. BZ heeft aangegeven dat de Compliance Officer eerste aanspreekpunt is voor de onderzoeken van AR en ADR en dat de opvolging van toekomstige aanbevelingen wordt aangestuurd en bewaakt in het IB-Managementoverleg.

<u>BZ Vragenlijsten Informatiebeveiliging & Privacy</u>
BZ is in 2020 gestart met uitvragen van de volwassenheid op het gebied van informatiebeveiliging en privacy bij de directies en posten aan de hand van self assessment vragenlijsten. Dit is weliswaar een momentopname, maar heeft wel geleid tot een bruikbaar inzicht in de volwassenheid.
De evaluatie over 2020-2021 heeft geleid tot een vernieuwde aanpak, met de inrichting van informatiepagina's, de ontwikkeling van kennisproducten en betere positionering van directe contactpersonen (DCR) bij IDI-ISC en IMB-ers in de regio's. De BZ vragenlijst zal op 16 september 2022 worden verstuurd naar de 'jaarlijkse' groep, bestaande uit 18 directies met kritische systemen en/of hoog-risicovolle verwerkingen van persoonsgegevens en 71 posten met hoog risico postendreiging en/of meer dan veertig medewerkers. Tevens worden de non-responses van 2020-2021 aangeschreven. De dienstonderdelen krijgen tot en met 14 oktober de tijd om deze in te vullen. In Q4 2022 zullen de rapportages worden opgesteld door Team Vragenlijsten van IDI-ISC.
Bij de eindcontrole zullen wij de ingevulde BZ vragenlijsten, de validatie door IDI-ISC en rapportages nader bekijken.

3.4 Voortgang opvolging overige bevindingen in het beheer

In deze paragraaf behandelen wij de voortgang van onze overige bevindingen in het beheer, zoals gerapporteerd in ons auditrapport 2021. Deze bevindingen kunnen, bij onvoldoende voortgang, mogelijk leiden tot beheerbevindingen met een weging in ons auditrapport 2022. 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.

3.4.1 Voortgang plan van aanpak 'Versterking BZ in control'

In ons auditrapport 2021 vroegen wij BZ extra inspanningen te leveren om het aantal hardnekkige fouten, die zich vooral voordoen op het OS-domein, terug te brengen. Immers eerdere inspanningen, zoals het organiseren van leersessies en het opleiden van (nieuwe) medewerkers, hebben niet geleid tot een foutenreductie. Voornoemde hangt ook samen met de inrichting van het toezichtsmodel bij BZ, waar wij eind 2020/begin 2021 een vraaggestuurd onderzoek naar hebben verricht. Dit onderzoek heeft geleid tot een aantal aanbevelingen, die in 2021 door BZ verder in kaart zijn gebracht. Begin 2022 is onder regie van FEZ een voorstel tot doorontwikkeling van het toezichtsmodel in de Managementraad besproken.

Dit voorstel heeft in 2022 tot meerdere initiatieven geleid, die zijn samengebracht in het overkoepelend plan van aanpak 'Versterking BZ in control'. Dit plan bestaat uit een drietal pijlers met onderliggende deelprojecten:

1. Oplossen van (oorzaken van) herhalende fouten:

- fouten oplossen, voorkomen en signaleren (FOVOS) en leren van fouten inclusief presentaties beeld ADR en FEZ bij de MT's van de themadirecties (inclusief meerjarige analyse van fouten).

2. Versterking interne beheersing:
    - verantwoordelijkheden binnen het three lines model;
    - visie op 'in control' zijn (vooruitkomdagen met thema 'de dynamiek van 'in control' zijn' en 'visie op 'in control' zijn');
    - versterking instrumenten van de interne beheersing (jaarplannen, risicoanalyse/interne beheersingsplannen, controlewerkzaamheden verbijzonderde interne controle werkzaamheden (VIC's), peerreview bij ODA-posten, werkprogramma's ODA), risk control framework (RCF), kritische prestatie indicatoren (KPI's) en kwartaalrapportages);
    - modernisering interne beheersing (modernisering activiteiten cyclus; IMPACT en Governance, Risk and Compliance Tooling (GRC)).
3. Versterking toezicht:
    - werking van het toezichtmodel;
    - rollen, taken en verantwoordelijkheden (toezicht op de bedrijfsvoeringsdirecties, toezicht op de ODA-directies; toezicht op de ODA-posten, toezicht op de overige beleidsdirecties, regiodirecties en non-ODA posten);
    - toezichtkalender;
    - toezichtarrangement;
    - staat van toezicht en inzicht;
    - samenwerking met derdelijnsfuncties (samenwerking met ADR en samenwerking met BVA, de FG en ISB);
    - modernisering van het toezicht (datagedreven toezicht).

In dit plan van aanpak zijn acties op continue, korte, middellange en lange termijn benoemd. De termijn is mede afhankelijk van de complexiteit en afhankelijkheid van de implementatie van nieuwe systemen zoals IMPACT. Medio september is door FEZ over de voortgang gerapporteerd inclusief onderbouwende documentatie. Hierbij valt het volgende op:

- Op nagenoeg alle deelprojecten is sprake van voortgang. Uit bestudering van deze voortgang verwachten wij dat de gewenste resultaten vanaf 2023 merkbaar zullen zijn. Veel initiatieven zijn nog onderhanden, wat overigens ook passend is bij de termijn die aan een deelproject gekoppeld is.
- De korte termijn acties zijn vooral gericht op pijler 1: de implementatie van beheersmaatregelen op het voorkomen, tijdig signaleren en oplossen van veel voorkomende fouten, gebaseerd op een oorzakenanalyse (project FOVOS). De oorzakenanalyse is inmiddels afgerond, vanaf september gaan twee werkgroepen (voor betalingen en verantwoordingen) de aangedragen oorzaken prioriteren en vervolgens de oplossingsrichtingen in kaart brengen en implementeren.
- Voor het slagen van dit overkoepelend plan is succes op alle drie de pijlers een randvoorwaarde. Immers een toereikende interne beheersing en toezicht leiden tot het voorkomen en vroegtijdig signaleren van fouten. Wij zien bij pijlers 2 en 3 vooral de structurele verbetermogelijkheden en bij pijler 1 vooral het incidentele karakter. Acties op pijlers 2 en 3 zijn naar onze mening daarom nodig voor een duurzame verbetering van het interne beheerssysteem.

Het is in dit stadium nog te vroeg om vast te stellen dat de (deel)projecten tot concrete verbeteringen hebben geleid, echter zijn wij positief over de inzet van BZ op dit veelomvattende plan en verwachten wij ook dat deze inzet onverminderd doorgang zal vinden tot het moment dat BZ er in slaagt zelf aantoonbaar in control te zijn. Naast de nodige capaciteit vanuit FEZ vraagt dit plan veel commitment vanuit de lijnorganisatie. *Overigens zijn wij bij de meeste deelprojecten als klankbordfunctie betrokken en zullen wij de verdere voortgang van het plan blijven monitoren.*

3.4.2 *Risicoparagraaf in bemo's*

De afgelopen jaren heeft BZ, met positief resultaat, veel inzet getoond op het structureel verbeteren van de kwaliteit van de risicoparagraaf in beoordelingsmemoranda (bemo's). Dit heeft in 2021 geleid tot het opheffen van onze lichte bevinding. De verantwoordelijkheid voor het opstellen van een risicoparagraaf van voldoende kwaliteit ligt bij de lijnorganisatie. Het Expertise Centrum Malversaties (ECM), onderdeel van FEZ, houdt hier toezicht op en voert interne controles uit op de kwaliteit van de risicoparagraaf, onderhoudt contacten met de risicomanagers en verzorgt de opleidingsmodule voor de risicoparagraaf.

Deze acties hebben zijn beslag gekregen in 2022. De e-learning en de praktijkworkshop zijn ontwikkeld en uitgerold en de interne controle op risicoparagrafen van budgethouders met een zeker risicoprofiel (13 waarnemingen) is over het eerste halfjaar 2022 uitgevoerd. De uitkomst van deze interne controle is dat er geen sprake is van risicoparagrafen van onvoldoende kwaliteit. Volgens ECM is een zestal risicoparagrafen voor verbetering vatbaar, zeven risicoparagrafen zijn op het gewenste niveau. *Wij zullen deze werkzaamheden reviewen en mogelijke bijzonderheden opnemen in ons auditrapport 2022.*

3.4.3 *Spendanalyse bij inkopen*

De spendanalyse is het sluitstuk van de borging van de rechtmatigheid van de inkopen, zodat achteraf kan worden vastgesteld dat de juiste inkoopprocedures zijn gevolgd. Tevens is de spendanalyse mede van belang om achteraf de volledigheid van het contractenregister te borgen.

De spendanalyse van BZ geeft inzicht in zes onderdelen ('key controls') die de rechtmatigheid zouden moeten borgen. Per 'key control' wordt door de meest belangrijke directies een analyse gemaakt. De spendanalyses over 2017 tot en met augustus 2021 zijn uitgevoerd. BZ is op dit moment nog bezig met het opstellen van de spendanalyse tot en met augustus 2022. In ons auditrapport over 2021 hebben wij aangeven dat wij de ontwikkelingen inzake de spendanalyse binnen BZ positief waarderen. *Om tot een verantwoordingsmiddel over de rechtmatigheid te komen herhalen wij echter ons advies om de spendanalyse twee keer per jaar uit te voeren, en wel in januari en juli, zodat de analyse van januari daadwerkelijk als verantwoording over de rechtmatigheid van de inkopen gebruikt kan worden als input voor de bedrijfsvoeringsparagraaf van BZ in het jaarverslag. Tevens adviseren wij FEZ/CDI van BZ om risicogericht de toelichtingen vanuit de directies, die uit de spendanalyse naar voren komen, te valideren.*

3.4.4 *Payment Factory ondersteunt het betaalproces*

Begin 2022 is gestart met het betalen via de Payment Factory. De Payment Factory is een automatiseringssysteem dat zorgdraagt voor het omzetten van betalingen uit SAP in het generieke betaalformat naar het specifieke betaalformat van de betalende bank. Betaalopdrachten worden vervolgens via SWIFT aangeleverd aan de betalende bank. Het elektronische betaalsysteem van de betalende bank wordt daarmee in principe overbodig. In de eerste zes maanden over het jaar 2022 zijn 22% van de betaalopdrachten verwerkt via de Payment Factory. Deze betalingen zijn goed voor ongeveer 20% van de omvang van de betalingen en dit aandeel zal toenemen. Overigens worden enkele banken alsnog in 2023 aangesloten op de Payment Factory en voor een klein aantal banken (vooral lokale banken) is afgezien van het gebruik van de Payment Factory. Hierdoor blijft sprake van een tweetal procedures, Payment Factory en elektronisch betalen, waarvan wij de getroffen beheersmaatregelen zullen toetsen.

Wij voeren momenteel een onderzoek uit op de getroffen beheersmaatregelen in de Payment Factory, die een betrouwbare verwerking van betaalopdrachten moeten

waarborgen. Voor de controle op de juistheid en volledigheid van gegevensoverdracht tussen SAP en de betaalapplicatie wordt geen gebruik gemaakt van hashtotals, zoals nu voor betalingen via ING, waardoor toereikende vervangende maatregelen noodzakelijk zijn. Vorig jaar hebben wij input geleverd op de door het implementatieteam voorgestelde maatregelen die dezelfde betrouwbaarheid bieden als hashtotals. Onze eerste indruk is dat deze maatregelen daadwerkelijk zijn getroffen, wel is nog nader onderzoek nodig om dit beeld verder bevestigd te krijgen.

De Payment Factory biedt veel opties die van invloed zijn op de te volgen workflow en application controls, die worden afgedwongen op zowel het te volgen proces bij betalen als bij beheeractiviteiten. Dit biedt mogelijkheden om de processen zo in te regelen dat de kans op ongewenste mutaties en transacties geminimaliseerd worden, maar zorgt ook voor een bepaalde complexiteit. *Het is daarom van belang om gemaakte inrichtingskeuzes goed vast te leggen, zodat de continuïteit van een betrouwbare werking geborgd kan worden.* Ook hier besteden wij tijdens ons onderzoek (verder) aandacht aan.

3.4.5 Eindejaarsdruk

Bij BZ is jaar op jaar sprake van een forse eindejaardruk, die veel druk legt op de organisatie en het risico op fouten vergroot. Diverse acties, zoals het dynamiseren van betalingen, hebben de afgelopen jaren plaatsgevonden om de eindejaarsdruk te verminderen, echter deze hebben niet geleid tot het gewenste resultaat.

Maandelijks wordt MT DGIS door FEZ geïnformeerd over de voortgang van het voorkomen van eindejaardrukte op basis van een vijftal pijlers: bemoplanning, budgetuitputting, rapportages in behandeling, rappelbeheer en oude voorschotten. Uit de laatste rapportage per 1 september 2022 blijkt dat het rappelbeheer, de budgetuitputting bij zowel de OS-directies als bij de OS-posten en de rapportages in behandeling nadere aandacht behoeven.

Een positief aspect is dat BZ vanaf 1 september 2022 voor 7 maanden vijf externe medewerkers heeft geworven om directies ondersteuning te bieden aan het wegwerken van rapportage-achterstanden en het uitvoeren van VIC's. Daarnaast heeft BZ ons gevraagd een onderzoek naar de eindejaarsdruk uit te voeren, dit onderzoek is lopende.

4 Overige onderwerpen en ontwikkelingen

4.1 Inleiding

In dit hoofdstuk behandelen wij de belangrijkste ontwikkelingen die kunnen leiden tot nieuwe beheerbevindingen vanuit onze wettelijke controletaak. Ook gaan wij in op onderwerpen die van belang zijn voor een goede bedrijfsvoering.

4.2 Verwerkingsregister onderhanden en afhandeling inzageverzoeken verbeterd

In 2021 constateerden wij dat verbeteringen zijn doorgevoerd in de naleving van de AVG maar dat BZ nog steeds niet volledig compliant is. Onze bevinding richtten zich met name op de verbetering van juistheid en volledigheid van het verwerkingsregister en de tijdige afhandeling van inzageverzoeken.

Verwerkingenregister

IDI-ISC heeft een AVG-werkplan 2022 opgesteld, met vijf focusgebieden, waaronder het AVG-Verwerkingsregister, verhogen van privacybewustzijn binnen BZ en wettelijke verplichtingen. Doelstelling is om eind 2022 80% van alle verwerkingen te hebben vastgesteld door de verantwoordelijke. Daarbinnen is het doel dat 95% van de hoog risico verwerkingen zijn vastgesteld. Het verwerkingenregister werkt nog niet naar behoren en dat is afgelopen zomer geëscaleerd. Momenteel wordt samen met de AVG-coördinatoren BZ gewerkt aan verbetering van de functionaliteiten.
Wij zullen de realisatie bij de eindcontrole toetsen.

Inzageverzoeken

Een procedure voor de afhandeling inzageverzoeken is ingericht. BZ heeft in 2022 negen inzageverzoeken ontvangen. BZ moet conform de Handleiding AVG BZ binnen vier weken reageren op het verzoek van de betrokkene. De wettelijke reactietermijn is echter één maand. Afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken kan die termijn, indien nodig, met nog eens twee maanden worden verlengd. De afhandeling van afhandeling van inzageverzoeken is verbeterd ten opzichte van 2021. De 8 verzoeken die in behandeling zijn genomen, zijn binnen de wettelijke termijn afgehandeld. Eén verzoek is om moverende redenen niet in behandeling genomen. BZ zal in de loop van 2023 een procesvolgsysteem voor onder meer de afhandeling van inzageverzoeken in gebruik nemen. Dit traject heeft vertraging opgelopen.
Wij adviseren de reactietermijn in de Handleiding AVG BZ in overeenstemming te brengen met de wettelijke termijn van een maand.

Opvolging bevindingen Autoriteit Persoonsgegevens m.b.t. NVIS

De Autoriteit Persoonsgegevens (AP) heeft de minister van Buitenlandse Zaken op 24 februari 2022 een boete en last onder dwangsom opgelegd voor het ontoereikend informeren van betrokkenen (lastonderdeel 2) en het onvoldoende waarborgen van de beveiliging van de verwerking van persoonsgegevens in de applicatie NVIS (lastonderdeel 1).
Op 31 maart 2022 heeft de AP bevestigd dat BZ verbetering heeft aangebracht t.a.v. lastonderdeel 2 van de last. Hiermee is de last onder dwangsom met betrekking tot onderdeel 2 op 24 maart 2022 geëindigd.
Op 22 juli 2022 heeft DCV een Plan van Aanpak (PvA) voor lastonderdeel 1 met de AP gedeeld, mede op basis van de appreciatie en advies van de BVA en FG om de tekortkomingen aan NVIS te herstellen. BZ heeft de AP om een reactie gevraagd op het PvA. Uit de reactie van de AP blijkt dat er op meerdere onderdelen nog zaken moeten worden aangescherpt of verduidelijkt. DCV geeft aan dat in het bijzonder de frequentie van de controle op toegangsrechten en de logging en monitoring de nodige tijd vereisen om, ook in overleg met de leverancier, aan de nieuwe vragen in

de reactie van de AP te voldoen. DCV streeft ernaar ook tijdig aan lastonderdeel 1 te voldoen. De structurele inrichting van de noodzakelijke maatregelen zal de nodige tijd vergen. Het is ons nog onduidelijk of dit vóór de gestelde termijn die de AP heeft gegeven haalbaar is.
Bij de eindcontrole zullen wij nagaan of alle activiteiten die in het PvA zijn opgenomen, zijn geïmplementeerd en of de last onder dwangsom daarmee is geëindigd.

4.3 Beperkte speelruimte in de planning van nieuwe IT-systemen; implementatie is haalbaar mits geen nieuwe tegenslagen

In ons auditrapport over 2021 constateerden wij dat BZ een ambitieuze doelstelling heeft voor de modernisering van het IT-landschap. Er is sprake van verschillende IT-projecten met krappe tijdlijnen. Een aantal projecten, zoals het nieuwe bedrijfsvoeringssysteem (VBS), de activiteitenapplicatie (IMPACT) en het managementinformatiesysteem (MI BZ), heeft een grote onderlinge afhankelijkheid in projectplanning, datamigratie en interfaces. Gezien deze afhankelijkheid stemmen de afzonderlijke projectleiders voortgang en planning periodiek met elkaar af. Op tactisch niveau is de product owner IMPACT vertegenwoordigd in zowel de stuurgroep van het nieuwe bedrijfsvoeringssysteem (VBS), als de stuurgroep van IMPACT en de stuurgroep MI BZ. Plaatsvervangend directeur IDI is vertegenwoordigd in stuurgroepen IMPACT en VBS. Het voorzitterschap van alle drie de stuurgroepen is belegd binnen FEZ.
Wij zien dat er hierdoor meer aandacht is voor de aansluiting tussen SAP BZ, BMS, IMPACT en MI BZ. Wij juichen dat toe, want met name op het gebied van interfaces, datamigratie en integrale fallbackscenario's zien wij risico's.

<u>Vervanging Bedrijfsvoeringssysteem – VBS (SAP BZ en BMS)</u>
BZ is voornemens met ingang van 2023 niet langer gebruik te maken van het bedrijfsvoeringssysteem van IenW. Hiervoor loopt een project VBS (vervanging bedrijfsvoeringssysteem). Het project heeft vertraging opgelopen maar koerst nog wel op implementatie per 1-1-2023. Onder andere de vertraging in het realiseren van de connectiviteit tussen de systemen van ATOS en BZ en de functionele inrichting van twee specifieke BZ-processen geven een onzekerheid over de haalbaarheid. Komende weken worden nog alternatieve scenario's uitgewerkt. Het ultieme fallbackscenario bestaat uit het langer gebruik blijven maken van het huidige SAP systeem van IenW. De ingebruikname van het BZ-systeem wordt dan uitgesteld tot 1-1-2024. Deze optie is afgestemd met IenW.
De vertraging en de daarmee samenhangende onzekerheden hebben geleid tot een intensivering van de betrokkenheid van de stuurgroep. Door de sterke afhankelijkheid met andere projecten zoals IMPACT en MI BZ heeft de vertraging in het realiseren van de interfaces ook invloed op deze projecten en daarmee ook weer op de haalbaarheid van de implementatie van het gehele programma.

<u>Modernisering Activiteitencyclus - IMPACT</u>
Ter vermindering van de beheerslast heeft BZ een project Modernisering Activiteitencyclus (MAC) gestart. Binnen dit project wordt een nieuwe applicatie (IMPACT) ontwikkeld ter ondersteuning van de activiteitencyclus. Deze applicatie vervangt onder andere SAP-GM.
Het project wordt voortvarend opgepakt. De stuurgroepleden zijn actief betrokken. Voor een deel van de directies en posten wordt inmiddels proefgedraaid met IMPACT als stand-alone systeem voor het eerste deel van de activiteiten. Het tweede deel vindt nog plaats in SAP GM. Volgens planning wordt IMPACT vanaf 2023 geïmplementeerd voor alle activiteiten. De functionaliteit van deze release is teruggebracht tot het minimaal noodzakelijke en het bouwteam is uitgebreid tot het maximaal haalbare. Dit impliceert wel dat er weinig regelmogelijkheden overblijven bij tegenvallers, met name als SAP BZ wel tijdig gereed is. Er is een fallbackscenario als IMPACT wel gereed is per 2023 maar SAP BZ niet. Het scenario dat SAP BZ wel gereed is maar IMPACT niet, is niet als realistisch beoordeeld. Onzekerheden liggen met name op het vlak van interfaces en datamigratie.

In de release van begin 2023 is er een beperkt aantal verschillende autorisatieprofielen, waardoor sommige gebruikers tijdelijk (te) ruime autorisaties kunnen hebben. Omdat dit alleen betrekking heeft op de beoordelings- en committeringsfase en FSO in deze release de definitieve activiteiten blijft invoeren, lijkt het risico beperkt.
Wij adviseren om de samenhang tussen de fallbackscenario's te bewaken en een integraal fallbackscenario te overwegen. Daarnaast adviseren wij om het controleren en invoeren door FSO van definitieve activiteiten te handhaven zolang sprake is van een beperkt aantal autorisatieprofielen in IMPACT.

4.4 Juiste registratie verplichtingen is een aandachtspunt

Uit onze controle van de (aangegane) verplichtingen op materiële uitgaven hebben wij een aantal aandachtspunten geconstateerd. Het betreft de juistheid van de verplichting omdat bijvoorbeeld het geregistreerde bedrag niet aansluit op het achterliggende contract. Tevens komt het voor dat niet de juiste valuta gehanteerd zijn bij het registreren van de verplichting in SAP (zoals gebruik van een dollarkoers in plaats van euro). Het risico is dat verplichtingen niet getrouw in de jaarrekening worden opgenomen of dat betalingen extra handelingen vergen omdat de verplichting eerst nog moet worden aangepast.
Wij adviseren BZ om intern afspraken te maken over de vastlegging van contracten en de interne controle vroegtijdig in het jaar uit te voeren zodat eventuele materiële correcties tijdig doorgevoerd kunnen worden.

4.5 Ontwikkelingen Invest International BV

Op 1 oktober 2021 is een vijftal regelingen, die ten laste komen van de BHOS begroting, in uitvoering overgeheveld van Rijksdienst voor Ondernemend Nederland (RVO.nl) naar Invest International Public Programmes BV, een dochteronderneming van Invest International BV (I&I).
I&I is een deelneming van het ministerie van Financiën (beschikt over 51% van de aandelen) en FMO. Het eerste boekjaar betreft een verlengd boekjaar, wat loopt van 1 oktober 2021 t/m 31 december 2022. Het verlengde boekjaar heeft alleen betrekking op de uitvoeringskosten van I&I. Voor de besteding van de beleidsgelden geldt het kalenderjaar als boekjaar.

In afwachting van de ontwikkeling en implementatie van de eigen administratieve systemen voor de regelingen verzorgt RVO.nl tot en met 31 december 2022 de administratie van de regelingen voor I&I. Dit is iets later dan verwacht, maar het is nog steeds de verwachting dat I&I per 1 januari 2023 de administratie volledig zal hebben overgenomen van RVO.nl. De controle van de BZ-regelingen, uitgevoerd door I&I, vindt over 2022 nog plaats door de ADR (team EZK), echter vanaf 2023 zal de controle door de externe accountant van I&I plaatsvinden. BZ en I&I zijn al enige tijd in overleg over het controleprotocol dat de accountant bij de controle van de projectverantwoording BZ dient te hanteren. Hierover is nog geen overeenstemming. De doorlooptijd is lang en het is nog onzeker of het controleprotocol voor 1 januari 2023 definitief is.
Wij adviseren de voortgang en tijdige afwikkeling van het controleprotocol te monitoren.

5 Ondertekening

Den Haag, 27 oktober 2022

Auditdienst Rijk

[redacted]

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