Auditdienst Rijk
Ministerie van Financiën

Managementletter 2022
Belastingdienst

Colofon

Titel	Managementletter 2022 Belastingdienst
Kenmerk	2023-0000071311
Inlichtingen	Auditdienst Rijk Korte Voorhout 7 2511 CW Den Haag

Inhoud

Inleiding—4
Algemeen—4
Doel en doelgroepen—4
Leeswijzer—4

1 Samenvattend beeld—5

2 Bevindingen in het beheer—6
2.1 Inleiding—6
2.2 Opgeloste bevindingen—6
2.2.1 Kwaliteit IV-organisatie—6
2.2.2 Logische toegangsbeveiliging—7
2.2.3 Bedrijfsvoeringsfunctionaliteiten—7
2.2.4 Verplichtingenbeheer en prestatieverklaring—8
2.3 Bevindingen in het beheer 2022—9
2.3.1 Software wijzigingsbeheer—9
2.3.2 Portfoliomanagement—10
2.3.3 Scriptbeheer—11
2.3.4 Inkoopbeheer—11

3 Overige onderwerpen—12
3.1 Misbruik en oneigenlijk gebruik (M&O)—12
3.2 Work arounds in de bedrijfsvoering (LOA's en RTV's)—13
3.3 Capaciteit en single point of failure—14
3.4 Belastingdienst Caribisch Nederland—14
3.5 Processen op orde in het kader van sturen en beheersen—14
3.5.1 Informatiebeveiliging—14
3.5.2 Algemene Verordening Gegevensbescherming (AVG)—15
3.5.3 Administratieve organisatie en interne controle (AO/IC)—15

4 Ondertekening—16

Inleiding

Algemeen

In deze managementletter doen wij verslag van de uitkomsten van de werkzaamheden die wij als interne auditdienst van het Rijk in het kader van de door u aan ons verstrekte opdracht over 2022 bij de Belastingdienst hebben verricht.

Doel en doelgroepen

De managementletter is opgesteld voor de Persoonsgegevens Belastingdienst en wordt in afschrift verstrekt aan Persoonsgegevens Persoonsgegevens van het ministerie van Financiën en de Algemene Rekenkamer. De uitkomsten van onze werkzaamheden worden voor zover in dat kader relevant ook opgenomen in het auditrapport 2022 van het ministerie van Financiën en Nationale Schuld.

De managementletter wordt als bijlage bij het Auditrapport van het ministerie van Financiën gepubliceerd bij het Jaarverslag van het ministerie van Financiën op verantwoordingsdag.

Leeswijzer

Deze managementletter is als volgt ingedeeld:

- Een samenvatting van ons onderzoek naar het beheer (hoofdstuk 1);
- De (opgeloste) bevindingen in het beheer 2022 (hoofdstuk 2);
- Overige onderwerpen (hoofdstuk 3).

1 Samenvattend beeld

De Belastingdienst stond in 2022 voor veel uitdagingen. Het op onderdelen sterk verouderde IT-Landschap, de reeks herstelopgaven, capaciteitstekorten en steeds toenemende behoefte van de politiek en samenleving zorgt voor druk op de organisatie. Ondanks deze druk constateren wij dat hard is gewerkt aan het wegnemen van de financieel en IT-beheer problematiek. Dit heeft erin geresulteerd dat vier bevindingen zijn opgelost. Het gaat om de bevindingen kwaliteit IV-organisatie, logische toegangsbeveiliging, bedrijfsvoeringsfunctionaliteiten en verplichtingenbeheer & prestatieverklaring. Ook zien wij verbeteringen bij de openstaande bevinding inzake het portfoliomanagement en constateren wij dat verder is gewerkt aan de in control statement (ICS). Ondanks de verbetertrajecten zal het nog langere tijd duren dat het op onderdelen sterk verouderde IT-landschap is gemoderniseerd. Tot die tijd heeft dit consequenties voor de wendbaarheid en continuïteit van de legacy systemen.

Het beeld bij de openstaande bevinding over het wijzigingsbeheer is minder positief. Wij doen verder twee nieuwe bevindingen, te weten het scriptbeheer en inkoopbeheer.
Verder merken wij op dat het niveau van toezicht achteraf over de jaren heen een voortgaande en verdere daling doormaakt en dat voor de coronasteunmaatregelen de slechte financiële positie van ondernemers zorgt voor een forse toename van de werklast met eventuele gevolgen voor de uitvoering van reguliere taken.

De dynamische en complexe omgeving waar binnen de Belastingdienst opereert zorgt voor een situatie waarbij risicogericht werken steeds meer een noodzaak is. Uit het ADR-onderzoek Evaluatie programma Managementinformatie/Risico-management (RM/MI) blijkt dat het programma een belangrijke bijdrage heeft geleverd aan de ontwikkeling en professionalisering van de managementinformatie en het risicomanagement op concern en ketenniveau. Wel blijkt uit het onderzoek dat een verdere doorontwikkeling gewenst is, waarbij het concern en de ketens de ontwikkelde dashboards en risico- en managementinformatie daadwerkelijk gaan gebruiken. Overigens zien wij dat de Belastingdienst steeds beter zicht heeft op de risico's, maatregelen treft en waar nodig keuzes maakt en daarop stuurt en communiceert. Dit zien wij onder meer terug in de verbeteringen die zijn doorgevoerd in het portfoliomanagementproces en de verdere implementatie van het keuzeproces voor het Toezicht achteraf. Daarnaast worden op meerdere terreinen, zoals voor de inningsopdrachten, prioriteitskaders uitgewerkt. Wij vinden dit een goede ontwikkeling.

2 Bevindingen in het beheer

2.1 Inleiding

Als onderdeel van de door u aan ons verstrekte opdracht onderzoeken wij of de door ons geselecteerde processen van het beheer voldoen aan de normen uit de comptabele wet- en regelgeving. Het gaat hierbij primair om het financieel beheer en de daartoe bijgehouden administraties. Deze eisen zijn nader uitgewerkt 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 het auditrapport Belastingdienst 2021 en nieuwe bevindingen in het beheer. Voor de bevindingen die als opgelost zijn aangemerkt geldt dat de onderzochte beheerprocessen toereikend zijn opgezet uitgaande van de risico's en dat de maatregelen zijn geïmplementeerd. Om de beheersing blijvend op orde te hebben is het van belang dat de door ons vastgestelde werkwijze gecontinueerd wordt en daar waar nodig wordt aangepast aan de omstandigheden. Hiervoor is een adequaat werkende Plan Do Check Act cyclus (PDCA-cyclus) voor de beheerprocessen nodig.

2.2 Opgeloste bevindingen

2.2.1 Kwaliteit IV-organisatie

De kwaliteit van de IV-organisatie is een belangrijke randvoorwaarde voor de sturing en beheersing van systemen en applicaties. Het op een effectieve en efficiënte wijze onderhouden, verbeteren en moderniseren van IT-faciliteiten vraagt om een goed ingerichte IV-organisatie.

In 2019 heeft de Belastingdienst een onderzoek naar het IV-portfolioproces en een doorlichting van de IV-organisatie laten uitvoeren met als doel om nieuwe inzichten te krijgen die bijdragen aan een structurele verbetering op dit gebied. Mede naar aanleiding van dit onderzoek is het verbeterprogramma-IV opgezet om op basis van een groot aantal initiatieven de kwaliteitsslag te maken. In het programma IV-verbetertraject was sprake van 5 sporen, met initiatieven gericht op IV-portfoliomanagement, (Agile) werking van de ketens, specifieke aandachtsgebieden binnen IV, cultuur & gedrag en wegwerken technische schuld.

Het verbetertraject is conform planning ultimo 2022 afgesloten, waarbij de initiatieven van het IV-verbetertraject grotendeels zijn opgeleverd. Om de resterende veranderinitiatieven in samenhang werkend te krijgen is gestart met de transitieaanpak IV-voortbrenging. Hiermee wordt gekozen voor een aanpak in de lijn. Door te kiezen voor de geïntegreerde aanpak beoogt de Belastingdienst een verbeterde verbinding te creëren tussen met name portfolio-, business- en IV-transitie. Aandachtspunten bij de transitieaanpak IV-voortbrenging zijn capaciteitsmanagement, batenmanagement, verandermanagement en de verdere uitrol van Agile werken.

Hoewel nog niet alle verbeterinitiatieven zijn geïmplementeerd en er nog aandachtspunten resteren voor de IV-organisatie merken wij de (generieke) bevinding kwaliteit IV-organisatie als opgelost aan. Eventuele tekortkomingen in de randvoorwaardelijke elementen van het IT-beheer koppelen wij voortaan zoveel als mogelijk aan de specifieke IT-bevindingen, zoals op dit moment de nog openstaande bevindingen wijzigingsbeheer, portfoliomanagement en legacy. Wij verwijzen hiervoor naar de paragrafen 3.3.1 en 3.3.2. Eventuele andere randvoorwaardelijke elementen van het IT beheer die aandacht behoeven bespreken wij in het vervolg in Hoofdstuk 3 'overige onderwerpen en aandachtspunten'.

2.2.2 *Logische toegangsbeveiliging*

Wij hebben eerder geconstateerd dat het beheer op de SOD-lijsten (segregation of duties) voor applicaties niet op orde is. Met name bij het opleveren van nieuwe applicaties en nieuwe functionaliteiten in applicaties verzuimde de Belastingdienst de noodzakelijke ongewenste functievermengingen in beeld te brengen. Hierdoor waren niet alle ongewenste functievermengingen (conflicterende muteerrechten) in zicht en konden daardoor ook niet alle controles via het Information Management Systeem (IMS) worden uitgevoerd door de Belastingdienst.

Inmiddels heeft de Belastingdienst ontbrekende functievermengingen in de genoemde SOD-lijst opgevoerd en een tijdelijk proces ingericht. Een expertiseteam beoordeelt maandelijks of de in IMS nieuw opgevoerde permissies (aan te vragen autorisaties) in combinatie met andere permissies een ongewenste functievermenging betreffen. De resultaten van deze beoordelingen worden verwerkt in de SOD-lijst en opgevoerd in IMS zodat deze preventieve controles kan uitvoeren. Hiermee is de bevinding logische toegangsbeveiliging opgelost.

Naar de toekomst toe is door Informatievoorziening en Databeheersing (IV&D) opdracht gegeven om, in overeenstemming met kaderstelling vanuit IV&D en Control en Financiën (C&F), het procesontwerp voor Logisch Toegangsbeheer (LTB) aan te passen waarbij een aansluiting wordt gerealiseerd tussen de architectuur repository en IMS. Hiermee wordt gewerkt aan een structurele oplossing voor de logische toegangsbeveiliging. De Belastingdienst geeft aan dat tot die tijd het tijdelijke proces in werking blijft.

Voor het beheer van de SOD-lijst is specialistische kennis nodig. Wij merken dat deze niet bij alle directies aanwezig is en adviseren om bij het aanpassen van het proces logische toegangsbeveiliging bij de directies te inventariseren wat volgens hen nodig is om de vereiste functiescheidingen in systemen in te richten en te monitoren en hen hierin faciliterend te ondersteunen. Voor de structurele oplossing is het belangrijk om voldoende kennis en kunde bij de directies op te bouwen, zodat ze zelf in staat zijn om de functiescheidingen te onderhouden.

2.2.3 *Bedrijfsvoeringsfunctionaliteiten*

Voor het uitvoeren van taken van medewerkers is het nodig dat de bijbehorende functionaliteiten in de applicaties zijn geïmplementeerd. Het is van belang om bij de ontwikkeling en bouw van applicaties de business te betrekken, zodat zicht is op de functionaliteiten die nodig zijn voor het uitvoeren van de taken.

Eerder hebben wij vastgesteld dat bij het bouwen van nieuwe systemen, gezien de druk op de tijdige beschikbaarheid van deze systemen en de beperkt aanwezige capaciteit, het onderhanden werk wordt geprioriteerd om te komen tot een Minimal Viable Product (MVP). Hierbij werden de functionaliteiten die betrekking hebben op het totstandkomen van de benodigde managementinformatie en het uitvoeren van ingebouwde interne controles veelal laag gescoord, waardoor deze pas na in productiename aandacht kregen.

Wij hebben vastgesteld dat de Belastingdienst maatregelen heeft getroffen om ervoor te zorgen dat in nieuwe applicaties ook de minimale functionaliteiten, die benodigd zijn voor de bedrijfsvoering, ingericht worden. Zo zijn de beheereisen voor processen en systemen in de concernarchitectuur vastgesteld en wordt door een geïntegreerde aanpak gewaarborgd dat de business (inclusief de controlfunctie) betrokken is bij het ontwerp van de domein- en solutionarchitectuur.

Voor de monitoring op de opvolging van de vastgestelde kaders zijn op verschillende niveaus processen voor architectuurcontrol ingericht. Zo zijn domeinarchitectuur boards en een concernarchitectuurboard opgezet die adviseren over het goedkeuren van kaders en het toestaan van afwijkingen. Indien sprake is van een geaccepteerde afwijking dan wordt hierover gerapporteerd. Wij zien dat terug bij de structurele Viermaandrapportages (VMR-rapportages). Wij hebben begrepen dat ook de kader stellende directie IV&D is gestart met het toetsen van de relatie tussen de Solution- en Domeinarchitectuur. Wij vinden dit een goede ontwikkeling.

Wij merken de bevinding die wij eerder opgenomen hebben onder de term bedrijfsvoeringsfunctionaliteiten als opgelost, omdat bij de bouw en ontwikkeling van applicaties voldoende waarborgen zijn getroffen om ervoor te zorgen dat er zicht is op benodigde functionaliteiten voor de bedrijfsvoering en dat de minimale functionaliteiten ook in de applicaties worden opgenomen.

2.2.4 Verplichtingenbeheer en prestatieverklaring

Verplichtingenbeheer

Bij het opstellen van de jaarrekening 2021 waren op nieuw flinke correcties noodzakelijk op de aangegane verplichtingen en verplichtingenstand in de jaarrekening. Dit was nodig omdat gedurende het jaar de verplichtingen niet correct werden bijgehouden in de administratie. De Belastingdienst heeft afgelopen jaar met aanvullende maatregelen de verplichtingenadministratie op orde gebracht. Zo vindt voordat inhuurverplichtingen worden geboekt een extra controle plaats aan de hand van de onderliggende documentatie. Voor het bewaken van de openstaande verplichtingenstand zijn signaallijsten ontwikkeld die een analyse op ten onrechte openstaande verplichtingen mogelijk maakt. De Belastingdienst heeft deze analyse periodiek uitgevoerd.

Uit onze steekproefcontroles van het afgelopen jaar blijkt dat het aantal foutief geboekte verplichtingen fors is gereduceerd. Daarnaast hebben wij aan de hand van de controles van de Belastingdienst vastgesteld dat het risico op ten onrechte openstaande verplichtingen voldoende is gereduceerd. De bevinding verplichtingenbeheer is hiermee opgelost.

Wij willen nog meegeven dat in de administratie veel grote correctieboekingen worden gemaakt. Dit maakt de administratie minder overzichtelijk en verhoogt de kans op fouten. De belangrijkste oorzaak van deze correcties betreft de tariefswijziging na jaarlijkse indexatie voor de nadere overeenkomsten bij inhuur. Na een tariefswijziging worden de oude verplichtingen volledig afgeboekt en opnieuw ingeboekt tegen het nieuwe tarief. Wij adviseren om na te gaan of het in het vervolg bij een tariefswijziging mogelijk is de openstaande verplichting slechts met het bedrag volgend uit de tariefindexatie te verhogen of te verlagen.

Het afgeven van prestatieverklaringen

Bij onze controle van de materiële uitgaven zijn de afgelopen jaren tekortkomingen geconstateerd ten aanzien van het afgeven van de prestatieverklaring. De onderbouwing was onvoldoende of de verklaring was in een enkel geval onterecht afgegeven. Ook ten aanzien van de prestatieverklaringen heeft de Belastingdienst in 2022 aanvullende maatregelen getroffen. Bij de dienstonderdelen met de grootste en meer complexere materiële uitgaven zijn controleplannen ingericht om de prestatie vast te stellen. Met behulp van signaallijsten wordt verder bewaakt dat uit te betalen facturen in de administratie tijdig van een prestatieverklaring zijn voorzien.

Uit de steekproeven op de materiële uitgaven blijkt dat de fouten en onzekerheden met betrekking tot het vaststellen van de geleverde prestaties zijn afgenomen. De bevinding voor het afgeven van prestatieverklaringen is hiermee opgelost.

Wij willen nog meegeven dat uit de controle op de prestatieverklaring is gebleken dat in enkele gevallen is voorgekomen dat de prestatieverklaring aan de hand van urenbriefjes is afgegeven door een leidinggevende die is ingehuurd en dat de prestatieverklaring betrekking heeft op uren die zijn gemaakt door een medewerker van hetzelfde bedrijf. Dit is tegen de interne procedures van de Belastingdienst. Wij adviseren om nauwlettend toe te zien op de naleving hiervan.

2.3 Bevindingen in het beheer 2022

2.3.1 Software wijzigingsbeheer

Wijzigingsbeheer heeft tot doel om wijzigingen binnen het traject van applicatieontwikkeling op een beheerste en geautoriseerde wijze te laten verlopen, zodat voorkomen wordt dat de doorgevoerde wijzigingen allerlei verstoringen veroorzaken. Hiervoor is het noodzakelijk dat toereikende procedures zijn opgesteld en geïmplementeerd die een succesvolle prioritering, goedkeuring, planning en uitvoering van wijzigingen in IT-systemen garanderen.

De Belastingdienst heeft de afgelopen periode gewerkt aan het doorontwikkelen van diverse kaderstellende documenten voor het wijzigingsbeheer. Dit heeft geresulteerd in een IV-kaderdocument dat nader uitgewerkt is in AO-voortbrengingsprocessen per keten. Met daarna de koppeling naar de handreiking inrichting test in Agile omgeving. De opzet voor het wijzigingsbeheer is daardoor toereikend (met in achtneming van de laatste nog te treffen aanvullingen, zoals de genoemde handreiking te formaliseren naar een richtlijn).

Uit ons onderzoek is gebleken, dat het voorkomt dat het testproces wordt overgeslagen, dat belangrijke bewijsvoering van testen niet wordt opgeslagen en dat niet altijd wordt gewerkt volgens de procedure met gevolgen voor de aantoonbaarheid. Dit speelt met name bij bouwteams die volgens de nieuwere methodieken (SAFe Agile en steeds meer DEVOPS) werken. Een van de oorzaken dat bouwteams niet conform de kaders werken is dat ze aangeven hier niet bekend mee te zijn.

Het is noodzakelijk de kaders onder de aandacht van de bouwteams te brengen en de naleving ervan te monitoren. Daarnaast adviseren wij om aanwijzingen en eisen voor gebruik en inrichting op te stellen voor de ondersteunende tools voor het ontwikkelen (Confluence) en testen (Jira). Dit zou kunnen worden gedaan door de werkgroep test community.

Wij hebben ook vastgesteld dat er bouwteams zijn die volgens de nieuwere methodes werken en daarbij een goed proces voor het wijzigingsbeheer hebben ingericht. De werkwijze van deze bouwteams sluit goed aan op de kaders en kan, voor zover andere teams dezelfde methode hanteren, als best practice worden uitgerold.

2.3.2 *Portfoliomanagement*

Om de dienstverlening van de Belastingdienst op peil te houden is het van belang het IT-landschap goed te onderhouden en te laten aansluiten op de strategische doelstellingen van de organisatie. Gezien de vele IT-voorzieningen is het van belang dat de IT-projecten en programma's binnen de organisatie tegen elkaar worden afgewogen, geselecteerd en geprioriteerd, zodat de schaarse middelen worden besteed aan de meest waardevolle IT- projecten voor de Belastingdienst. Portfoliomanagement zorgt ervoor dat de organisatie hier op een planmatige manier voortdurend aan werkt. Het geeft het management zicht op het IT-portfolio en de risico's in relatie met de strategische doelstellingen, zodat zij weloverwogen keuzes kan maken.

Door politieke keuzes die steeds vaker leiden tot inbreuken, schaarse IT-capaciteit, een op onderdelen sterk verouderde landschap, de ontvlechting met de uitvoeringsorganisaties Douane en Toeslagen, is het essentieel dat risicogericht wordt gewerkt met behulp van portfoliomanagement. Zo kan men met behulp van portfoliomanagement in kaart brengen wat de gevolgen zijn voor de IT-portfolio in geval er sprake is van een (politieke) keuze. De risico's voor de gehele IT-portefeuille worden duidelijk en kunnen vervolgens worden gedeeld met de besluitvormers, waaronder de Tweede Kamer.

In 2022 is door de Belastingdienst verder gewerkt aan IV-portfoliomanagement, wat ultimo 2022 heeft geleid tot het een meerjarig portfolio (MJP). Het MJP sluit aan bij de ICT-doelstellingen van de Belastingdienst, het ministerie van Financiën en de I-strategie Rijk. Voor het MJP zijn inmiddels de kaders en randvoorwaarden vastgesteld. Daarbij is inzicht gegeven in perspectieven van de stakeholders, risico's, impact van gemaakte keuzes en hoe gestuurd wordt op de verhoudingen tussen de categorieën. Het MJP geeft inzicht in de initiatieven de aankomende jaren en geeft richting aan de meerjaren capaciteitsontwikkeling en middelen, zodat de Belastingdienst daar op een beheerste manier naar toe kan groeien.

Om volledig in control te komen op het portfoliomanagement zal de werking van het net tot stand gekomen MJP de komende periode nog aangetoond moeten worden. Dit met een volledig werkende PDCA-cyclus die de volgende elementen bevat; risicomanagement, herijken en prioriteren, stakeholder- en informatiemanagement. Hierbij adviseren wij om het prioriteitskader verder uit te werken en inzet van de beschikbare rapportage tooling te optimaliseren. Daarnaast is in het kader van een optimaal werkend portfoliomanagement een volledige administratie van belang waarin wordt bijgehouden uit welke componenten (bijv. servers, mainframes en applicaties) het IT-landschap bestaat en de onderlinge afhankelijkheden hierbij. Tot slot adviseren wij om te blijven sturen op samenwerken, cultuur, houding en gedrag door directies en ketens.

<u>Legacy</u>
Vanwege het op onderdelen sterk verouderde IT-landschap is enkele jaren geleden gestart met het project Modernisering IV-Landschap (MIV). Dit project is volgens planning eind 2022 gestopt. Omdat de Belastingdienst, gelet op het groot aantal applicaties, waarschijnlijk altijd te maken zal hebben met legacy systemen en er dus voortdurend moet worden gemoderniseerd, blijft de behoefte aan een regierol op het verder terugdringen van legacy bestaan. Vanaf 2023 is deze regierol belegd bij de Chief Technology Office (CTO) via een project 'Regie Op Modernisering (ROM)'. De nadruk zal daarbij zowel liggen op het verder uitfaseren van incourante platformen (zoals Cool:Gen) als het verbeteren van applicaties met verouderde technologie.

Gezien de uitdagingen binnen het portfolio voor belangrijke applicaties voor heffen en inningen blijven continuïteit en wendbaarheid de komende jaren belangrijke aandachtspunten. Wij hebben geconstateerd dat legacy een plek heeft gekregen binnen het MJP en dat legacy risico's voor de grote ketens Inkomensheffing, Loonheffingen en Omzetbelasting worden gemonitord. Zowel binnen als buiten deze applicaties zijn mitigerende maatregelen door de directies en ketens genomen om de continuïteitsrisico's te beperken. Voorbeelden hiervan zijn het vervangen en/of platformen van applicaties en het uitvoeren van verbijzonderde interne controles achteraf.

2.3.3 *Scriptbeheer*

Daar waar het (nog) niet mogelijk of doelmatig is om de vereiste functionaliteiten in de applicaties in te regelen kan worden gewerkt met alternatieve oplossingen, zoals het gebruik van scripts. Wij hebben vastgesteld dat de Belastingdienst veel gebruik maakt van scripts. Voorbeelden van scriptgebruik zijn het ophalen van gegevens uit applicaties en het aanpassen van gegevens in de database.

Het gebruik van scripts heeft voordelen, zo kun je hierdoor herhaalbare taken eenvoudig automatiseren. Dit biedt de organisatie mogelijkheden om op een flexibele wijze in te spelen op de behoefte van gebruikers. Het gebruik van scripts brengt echter ook risico's met zich mee, zoals het verkeerd aanmaken ervan. De gevolgen hiervan kunnen zijn; onbetrouwbare managementinformatie, verkeerde aanpassingen in de IT-functionaliteit (herstelscript) en ongecontroleerde aanpassingen in de database (SQL-injectie).

Vanwege de vele scripts die de Belastingdienst gebruikt is scriptbeheer belangrijk. Om dit te verbeteren heeft de Belastingdienst in 2022 een procedurebeschrijving opgesteld. Wij hebben de procedurebeschrijving beoordeeld en achten deze toereikend. Voor het oplossen van de bevinding scriptbeheer is het nodig dat de procedure volledig wordt toegepast door de functioneel beheerteams, hetgeen eind 2022 nog niet geheel het geval was.

Wij adviseren om een goed overzicht van de toegepaste scripts bij te houden, zodat te allen tijde bekend is welke scripts worden toegepast, wat het karakter hiervan is (herhaling of nieuw) en voor welk doel, maar ook wat de onderlinge afhankelijkheden zijn. Dit vergemakkelijkt het achterhalen van oorzaken van eventuele (kritieke) problemen die het gevolg zijn van scriptgebruik, zodat deze snel kunnen worden opgelost.

2.3.4 *Inkoopbeheer*

Bij ons onderzoek naar het aangaan van verplichtingen toetsen wij, mede op basis van de Europese aanbestedingsregels en contractuele afspraken, het rechtmatig tot stand komen van raamovereenkomsten, nadere overeenkomsten en de uitvoering van het bestelproces.

Wanneer het niet mogelijk is de Europese aanbestedingsregels te volgen wordt dit vastgelegd in een door de Persoonsgegevens getekende waiver. De Belastingdienst heeft over 2022 vastgesteld dat het aantal en bedrag aan verstrekte waivers is toegenomen. Bij het bestelproces is gebleken dat met name de procedures rondom het uitvoeren van contractueel verplichte minicompetities nog niet goed worden nageleefd.

De Belastingdienst laat nu extern onderzoek in stellen hoe de organisatie van het inkoopproces op een toereikend niveau gebracht kan worden. Om af te dwingen dat de afgesproken procedures beter gevolgd worden, kan sterker sturen op houding en gedrag, mogelijk al helpen bij het verbeteren van het inkoopbeheer.

3 Overige onderwerpen

3.1 Misbruik en oneigenlijk gebruik (M&O)

PDCA-cyclus
De Belastingdienst streeft ernaar dat burgers en bedrijven zoveel mogelijk uit zichzelf de fiscale verplichtingen nakomen (compliance). In de uitvoering van de taken zijn beperkingen zoals de beschikbaar gestelde personele en financiële middelen en ook zijn er maatschappelijke begrenzingen. Een goede PDCA-cyclus waarbij rekening wordt gehouden met deze beperkingen en begrenzingen, is noodzakelijk voor het omgaan met compliance risico's voor het M&O beleid en het toezicht. In 2021 is onder meer gerapporteerd over de PDCA-cyclus en de capaciteitsbeperkingen voor het uitvoeren van toezicht.

De Belastingdienst heeft in 2022 de PDCA-cyclus voor uitvoering- en handhaving verder ingericht door het opstellen van centrale kaders voor onder meer handhavingsplannen, beleidsevaluaties en waar nog niet aanwezig het opstellen van beschrijvingen van de PDCA-cyclus bij de betreffende dienstonderdelen. Voor een deel moet in 2023 de correcte werking van deze cyclus nog aangetoond worden. Het keuzeproces is een belangrijk element van de PDCA-cyclus. Dit proces gaat over de in te zetten handhavingsinstrumenten, de selectie van de nalevingsrisico's, voorraadbeheersing en toewijzen van personele capaciteit. Om tot verdere verbetering te komen heeft de Belastingdienst in 2022 een onderzoek gedaan naar het keuzeproces. Implementatie van de aanbevelingen is gepland voor 2023 en 2024 en maakt deel uit van de Strategische Ontwikkelagenda Belastingdienst en het Actieplan Toezicht.

Uitvoering M&O-beleid
De Belastingdienst ter beschikking staande mix van handhavingsinstrumenten hebben zowel betrekking op onder meer het geven van voorlichting, het koppelen van contra-informatie zoals dat gebeurt bij de vooraf ingevulde aangifte en toezicht achteraf (aanslagregeling en uitvoeren van boekenonderzoeken). Niet van alle handhavingsinstrumenten is bestuurlijke informatie aanwezig over de inzet van de instrumenten en het effect dat deze instrumenten bereiken. Van het toezicht achteraf is informatie bekend in de vorm output. Het gaat hierbij om aantallen boekenonderzoeken, geregelde aantallen aangiften en correctieresultaten. Het effect van de inzet van de handhavingsmix op de compliance meet de Belastingdienst met name met de Fiscale Monitor en de steekproefonderzoeken (per doelgroep).

In de begroting zijn na de herijking in 2019 KPI's opgenomen die toezien op het effect dat de Belastingdienst wil bereiken om de compliance te onderhouden, de outcome. Er zijn geen indicatoren meer opgenomen die toezien op output van de ingezette toezichtsinstrumenten, waaronder de output die betrekking heeft op uitgevoerde boekenonderzoeken en aanslagregeling. Daarbij merken wij op dat op strategisch niveau wordt gestuurd op outcome terwijl op operationeel niveau meer wordt gestuurd op te realiseren output. Wij vinden het daarom van belang dat de samenhang tussen de strategische doelstelling van compliance en het bereiken van operationele doelstellingen bij de dienstonderdelen zichtbaar wordt gemaakt.

Er is geen norm beschikbaar voor wat verstaan moet worden onder toereikend toezicht. Het aandeel van toezicht achteraf in de handhavingsmix is afgelopen jaren gedaald. Deze daling wordt onder meer veroorzaakt doordat bij het maken van keuzes het primaire proces prioriteit krijgt boven het toezicht achteraf. Daarnaast zijn er politieke keuzes waar prioriteit aan moet worden gegeven zoals de inzet voor box 3. De verwachting is dat een daling in het toezicht achteraf niet direct effect zal hebben op de compliance, maar dat dit zich opbouwt over enkele jaren. Er zijn daarom ook bij de Belastingdienst en de Kamer zorgen dat deze sinds 2016 ingezette daling in het toezicht achteraf een effect heeft voor het niveau van compliance en voor het nalevingstekort.

Het ontbreekt de Belastingdienst nog aan beleidsinformatie om de effecten van de verschillende handhavingsinstrumenten te kunnen duiden op de bijdrage aan compliance. Hierdoor is het nog niet mogelijk om vast te stellen of het achterblijven van het toezicht achteraf voldoende wordt gecompenseerd door de inzet van toezicht vooraf en actueel toezicht. Om te verkennen hoe het beste kan worden omgegaan met de risico's die verband houden met de dalende trend van het toezicht achteraf is het actieplan Toezicht uitgewerkt om zo onder meer te komen tot toezicht dat gegeven de beschikbare capaciteit de grootste bijdrage levert aan compliance.

Het is, naast het uitgewerkte actieplan toezicht, nodig dat meer inzicht komt op het effect van de verschillende instrumenten op compliance, zodat tijdig actie kan worden ondernomen om het risico op compliance en het naleveringstekort op een acceptabel niveau te houden.

3.2 Work arounds in de bedrijfsvoering (LOA's en RTV's)

De Belastingdienst maakt relatief veel gebruik van tijdelijke oplossingen, zoals 'Lokale Ontwikkelde Applicaties (LOA's)' en '(Robuuste) Tijdelijke Voorzieningen (RTV's)'. Deze oplossingen maken geen standaard onderdeel uit van beheersmaatregelen, zoals de active directory, wijzigingsbeheer en logische toegangsbeveiliging. Dit met de mogelijke risico's voor de continuïteit, betrouwbaarheid en kwaliteit van de data.

De risico's van het gebruik van RTV's zijn lager dan die van LOA's, omdat ze veelal vanuit het normale IV-voortbrengingsproces worden ontwikkeld. Dit betekent dat ze via een standaard (test)traject gaan. Een RTV wordt steeds meer ingezet als tijdelijke oplossing bij minder wendbare (legacy) applicaties om op een snelle en robuuste wijze de gevolgen van nieuwe wet- en regelgeving binnen het IT-landschap van een belastingmiddel te kunnen automatiseren. Bij LOA's daarentegen is sprake van een hoger risico omdat deze applicaties buiten het reguliere IV-voortbrengingsproces ontwikkeld worden en dat het gebruik ervan foutgevoeliger is als niet afdoende beheersmaatregelen worden getroffen (bijvoorbeeld bij werken in Excel). Het gebruik van LOA's in dagelijkse operationele uitvoeringsprocessen zou daarom zoveel als mogelijk moeten worden voorkomen.

Wij begrijpen dat de Belastingdienst via het CTO-project 'Regie op Modernisering' mede voornemens is om te werken aan het terugdringen van deze LOA's en RTV's. Dit is een goede ontwikkeling. In de tussentijd blijft het van belang om afdoende waarborgen te treffen.

3.3 Capaciteit en single point of failure

Op meerdere terreinen constateren wij capaciteitsgebrek. Het capaciteitsgebrek raakt het snel kunnen doorvoeren van acties voor herstel, het toezicht en kan risico's opleveren voor de uitvoering. De Belastingdienst onderkent deze problemen en speelt daar ook op in door het aantrekken van personeel. Het inwerken kost tijd en zal pas na verloop van tijd leiden tot de beoogde productiviteit van de medewerkers. Dit in combinatie met de grote afhankelijkheid van medewerkers, vanwege hun kennis, ervaring en expertise, zorgt voor risicovolle situaties (single point of failure). Wij adviseren daarom om na te gaan op welke cruciale onderdelen sprake is van een sterke afhankelijkheid van specialistische medewerkers, waarvan enkele binnenkort ook met pensioen gaan, en daar met voorrang maatregelen voor te treffen.

3.4 Belastingdienst Caribisch Nederland

De Belastingdienst Caribisch Nederland (BCN) maakt als RCN-dienst (verplicht) gebruik van de Shared Services Organisatie Caribisch Nederland (SSO CN) als ICT-serviceverlener.

Bij SSO CN is sinds 2018 sprake van een niet toereikende informatiebeveiliging. In 2022 hebben wij vastgesteld dat in opzet een belangrijke stap voorwaarts is gezet in het verbeteren van de informatiebeveiliging. De uitvoering is echter complex. Dit komt mede door de wijziging in IT-strategieën van deelnemende RCN-diensten (het publiceren van websites voor burgers en bedrijven). Daarnaast zorgt de keuze voor Cloudcomputing voor extra cyberrisico's.

Eind 2022 hebben SSO CN en de RCN-diensten overlegd over de concrete invulling van specifieke eisen en wensen ten aanzien van de IT-security. De RCN-diensten zijn zelf verantwoordelijk voor de informatiebeveiliging van hun eigen specifieke IT-applicaties waarbij verouderde software van één specifieke klant gevolgen kan hebben voor het geheel aan beveiligingsmaatregelen van RCN. Het is van belang om in gezamenlijkheid met SSO CN en de overige RCN-diensten de eisen en wensen ten aanzien van IT-security in onderlinge samenwerking te bespreken en de samenhang hiervan op het gehele beveiligingsstelsel van RCN aan te geven.

3.5 Processen op orde in het kader van sturen en beheersen

3.5.1 Informatiebeveiliging

Vanaf 2021 dienen alle dienstonderdelen van de Belastingdienst te verklaren dat ze voldoen aan de aan hen toegewezen Baseline Informatiebeveiliging Overheid (BIO)-controls. Bij onvoldoende informatiebeveiliging is er een verhoogd risico op incidenten, inbreuken op systemen en processen met mogelijke financiële- en imagoschade als gevolg.

De Belastingdienst werkt nog aan de opzet en implementatie van het informatiebeveiligingsbeleid. Diverse rapportages (bijvoorbeeld VMR) geven aan dat directies nog uitdagingen hebben om het proces optimaal te laten verlopen. Zo zijn er capaciteitstekorten (niet alleen te weinig personeel maar ook stapeling van vraagstukken bij dezelfde mensen) en signalen over een kloof tussen de kadersteller en uitvoering. Het programma OBIO (Ondersteuning Baseline Informatiebeveiliging Overheid) is bijvoorbeeld meervoudig uitgezet bij de directies zonder daarbij heldere instructies mee te geven over hoe opzet en bestaan van getroffen maatregelen kan worden aangetoond. Gevolg is dat directies (goedbedoeld), eigen tooling gaan inzetten en voorbijgaan aan de centraal gedeelde BIO-diagnosetool. Om ervoor te zorgen dat de centraal opgestelde kaders, verwachtingen en tools worden toegepast door de directies adviseren wij om de aansluiting tussen de kadersteller IV&D en de dienstonderdelen te verbeteren.

3.5.2 *Algemene Verordening Gegevensbescherming (AVG)*

Vanwege de vele persoonsgegevens die de Belastingdienst verwerkt is het belangrijk dat voldoende waarborgen zijn getroffen om de bescherming van de persoonsgegevens te garanderen. Dit in lijn met de AVG, dat in 2016 in werking is getreden.

Wij stellen vast dat de Belastingdienst nog niet geheel aan de AVG voldoet. Dit lijkt mede het gevolg van lange doorlooptijden voor onderzoeken die nodig zijn om zicht te krijgen op privacyrisico's, zoals de gegevensbeschermingseffect-beoordelingen (GEB's). Dit heeft tot gevolg dat het verwerkingsregister niet actueel is. Hierin staat informatie over de persoonsgegevens die worden verwerkt. Door het ontbreken van een actueel verwerkingsregister en achterblijven van GEB's heeft de Belastingdienst niet alle verwerkingen in beeld en weet zij ook niet of er voldoende maatregelen getroffen zijn en of de persoonsgegevens adequaat zijn beschermd.

Wij adviseren om de AVG-processen efficiënter en effectiever in te richten door het formeel initiëren van een overheidsbrede (verkorte) pre GEB-scan. Deze zou kunnen helpen vaststellen of een GEB nodig is waardoor kleinere processen versneld kunnen worden vastgesteld.

Tot slot zien wij dat onder regie van het kerndepartement een actieplan 'Privacy op orde' is opgesteld voor het kerndepartement, Belastingdienst, Douane en Toeslagen. Dit actieplan heeft tot doel de privacy-organisatie te versterken. Navraag en onderzoek leert dat de uitvoerende directies binnen de Belastingdienst nog niet inhoudelijk bekend zijn met dit actieplan en op eigen wijze (mede vanuit de door IV&D uitgedragen controlelijsten), de AVG-implementatie vormgeven. Meer onderlinge communicatie tussen kadersteller en uitvoering over een efficiënter proces, zou derhalve kunnen helpen om de AVG -implementatie gestructureerd en vanuit uniform gedragen uitgangspunten vorm te geven.

3.5.3 *Administratieve organisatie en interne controle (AO/IC)*

Naar aanleiding van het verbeterprogramma Herstellen Verbeteren Borgen (HVB) en het 'In Control Statement-traject (ICS)' is het project 'AO/IC op orde' ingesteld. Via dit project wordt capaciteit vrijgemaakt voor het op orde brengen van de beschrijvingen voor de werk- en bedrijfsprocessen. Dit heeft erin geresulteerd dat inmiddels de meest risicovolle werkprocessen van de dienstonderdelen in beeld zijn, maar nog niet allemaal zijn beschreven. De Belastingdienst geeft aan dat, gezien de hoeveelheid aan processen, het nog een paar jaar gaat duren voordat het einddoel is bereikt. Dat wil zeggen dat dan alle processen zijn beschreven en getoetst.

Uit ons onderzoek valt nog steeds de moeizame en derhalve tijdrovende verhouding tussen lijn- en ketenverantwoordelijkheid op als het gaat om het opstellen van beschrijvingen voor de bedrijfsprocessen. Wij willen daarom nogmaals het belang benadrukken van een goede samenwerking binnen en tussen de ketens en directies, omdat hierdoor het risico aanwezig is dat geen volledig inzicht wordt verkregen in de ketenprocesbeschrijving.

4 Ondertekening

Den Haag, 15 maart 2023

Auditdienst Rijk

Persoonsgegevens

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag

Persoonsgegevens