Auditdienst Rijk
Ministerie van Financiën

> Retouradres Postbus 20201 2500 EE Den Haag

Rijksdienst voor Ondernemend Nederland
x
Postbus 90357
2500 EE Den Haag

Auditdienst Rijk

Korte Voorhout 7
2511 CW Den Haag
Postbus 20201
2500 EE Den Haag
www.rijksoverheid.nl

Inlichtingen
x
T x
x
www.minfin.nl

Ons kenmerk
2022-0000170050

Uw brief (kenmerk)

Datum 23 juni 2022
Betreft Managementletter RVO 2021

Geachte x,

Naar aanleiding van de accountantscontrole van de beleidsgelden 2021 van het agentschap RVO hebben wij een aantal bevindingen, die wij graag onder uw aandacht brengen. De bevindingen betreffen de uitvoering van de beleidsgelden door RVO. Voor het agentschapsdeel hebben wij geen bevindingen.

Tot het geven van nadere toelichting zijn wij gaarne bereid.

x

x Auditdienst Rijk

1. Opgeloste bevindingen

In het afgelopen jaar zijn veel van de bevindingen uit voorgaande jaren opgelost. Dit geldt met name voor de bevindingen over de dossiervorming, over de IKS en over de garanties van oorsprong (CertiQ bij SDE). Daarnaast zijn verbeteringen doorgevoerd m.b.t. de restoretesten (bij SDE).

In de volgende paragrafen vermelden wij een aantal nog niet opgeloste en nieuwe bevindingen.

2. GITC voor UP.NL nog onvoldoende op orde

RVO moest in 2020 voor de uitvoering van onder andere de TVL-regeling snel schakelen naar het nieuwe platform UP.NL. Dit systeem was weliswaar reeds geruime tijd in ontwikkeling, maar nog niet in een stabiele aantoonbare beheermodus gekomen. Vorig jaar stelde RVO op basis van eigen onderzoek vast dat de general IT controls (GITC) rond dit systeem nog verder verbeterd dienden te worden. Begin 2021 zijn daarom afspraken gemaakt om het systeem te beschrijven en de betrouwbaarheid te onderzoeken waarbij de IAD ook zijn rol heeft gepakt.

Hoewel hierin voortgang is gemaakt zijn de GITC nog niet zodanig op orde dat kan worden aangetoond dat de GITC in opzet, bestaan en werking al volledig voldoen aan de gestelde eisen. Bij het gebruikers- en wijzigingenbeheer bestaan nog te veel onduidelijkheden over de opzet en het bestaan van de beheersingsmaatregelen. Voor de beveiliging van de IT-componenten waar UP.NL gebruik van maakt, geldt dat de vereiste maatregelen wel zijn geïnventariseerd, maar nog niet is vastgesteld dat deze ook allemaal zijn geïmplementeerd. Daarom geldt ook hier dat het vooralsnog te vroeg is om voor de controle die over heel 2022 gaat al de werking te gaan toetsen.

RVO onderkent de urgentie van verbetering van de GITC. In 2021 heeft RVO met alle beschikbare capaciteit gewerkt aan de verbeteringen. Extra beveiligingsonderzoeken en het per kwartaal opnieuw moeten inregelen van een nieuwe TVL-regeling heeft deze capaciteit echter voortdurend onder druk gezet. Daardoor heeft RVO minder voortgang kunnen boeken dan was gepland. Vanaf het vierde kwartaal 2021 heeft RVO kans gezien om meer snelheid te brengen in het invoeren van de verbeteringen.

Een aantoonbare werking van de GITC is een voorwaarde voor de waarborging van een continue en betrouwbaar werkend UP.NL-systeem en is een vereiste voor een systeemgerichte controle. Wij hebben voor onze controle over 2021 dan ook nog gegevensgericht gecontroleerd.

Wij bevelen aan voldoende capaciteit beschikbaar te stellen voor het roadmap-project om de GITC rondom UP.NL in opzet, bestaan en werking in 2022 op toereikend niveau te krijgen. Dit betreft concreet het gebruikersbeheer, het wijzigingenbeheer, en de beveiliging van de IT-componenten waar UP.NL gebruik van maakt[1]

3. Aansluiting data UPNL met EBS moeilijk navolgbaar

UP.NL is een platform (zaaksysteem) waarop aanvragen voor subsidieverleningen en vaststellingen, waaronder die voor de TVL, worden verwerkt. De hieruit resulterende verplichtingen, voorschotbetalingen en afrekeningen moeten worden doorgezet naar EBS, het systeem voor de financiële administratie. Wij hebben in 2020 vastgesteld dat een standaard interne controle ontbreekt of de verplichtingen en betalingen in de operationele systemen zoals UP.NL aansluiten op de boekingen in EBS.

Alle TVL-boekingen worden vanuit UP.NL verwerkt in EBS, maar het bleek niet mogelijk om te komen tot sluitende verbanden tussen UP.NL en EBS. Na extra inspanningen in het eindejaartraject kon worden aangetoond dat de boekingen correct worden verwerkt.

Een eerste oorzaak voor de verschillen is het feit dat de UP.NL-database niet rechtstreeks kan worden aangesloten met de standen uit EBS. Daardoor is voor de aansluitingen gewerkt met data uit de SAS-omgeving die met name voor rapportage doeleinden is gebouwd. Het is onvoldoende duidelijk hoe de data in de SAS-omgeving kunnen worden aangesloten op de data in EBS.

Een tweede oorzaak ligt in het feit dat een bezwaar of beroep tegen een subsidieverlening of vaststelling niet wordt afgehandeld in UP.NL, maar in BAS. Dit betekent dat de hieruit voortvloeiende mutaties vanuit BAS later handmatig in UP.NL worden geboekt en gesynchroniseerd met EBS. Deze latere mutaties dienen voor de volledigheid van de gegevens ook te worden toegevoegd aan de SAS-omgeving. Dit geschiedt door handmatige interventie via scripts en kan een aanzienlijk tijdsverschil opleveren tussen de oorspronkelijke boeking in EBS en de toevoeging aan de data in de SAS-omgeving. Wij hebben geen beschrijving aangetroffen van deze boekingsgang, met de risico's in dit proces en de wijze waarop die worden beheerst. Hiermee voldoet deze boekingsgang niet aan de criteria van ordelijkheid en controleerbaarheid.

Een derde oorzaak ligt daarin dat verstoringen in de middleware rondom FinDos kunnen leiden tot niet verwerkte transacties. Herstel hiervan vereist handmatige interventie op basis van de daarvoor opgestelde procedure. Gebleken is dat deze procedure echter niet altijd is gevolgd. Verder is monitoring nodig om te kunnen vaststellen of zich verstoringen hebben voorgedaan.

[1] Het beheer van wachtwoorden behoort ook tot de GITC-maatregelen. Binnen EZK is DICTU hiervoor verantwoordelijk. De invulling van de wachtwoordeisen zijn opgenomen in de dienstverleningsafspraken. De verantwoordelijkheid van RVO voor de GITC vereist wel dat RVO controleert dat deze eisen door DICTU worden nageleefd.

Wij bevelen aan na te gaan of het mogelijk is de aansluiting tussen UP.NL en EBS rechtstreeks te maken, zonder tussenkomst van de SAS-omgeving, en daarbij te zorgen voor een goede aansluiting van de mutaties (verplichtingen/uitgaven) tussen UPNL-FINFUN-FINDOS-EBS. Beoordeel de risico's hierin en neem daarop voldoende beheersmaatregelen ten einde de ordelijkheid en controleerbaarheid van deze stroom te borgen. Indien een rechtstreekse aansluiting tussen UP.NL en EBS niet mogelijk is geldt het voorgaande ook voor de mutaties in de SAS-omgeving.

4. Regelingen in BAS moeten over naar ander zaaksysteem

RVO gebruikt het zaaksysteem BAS voor de uitvoering van een groot aantal regelingen. In 2020 is besloten over een multi-platform strategie waarin RVO voor de uitvoering van regelingen beschikt over meerdere zaaksystemen en waarin oudere systemen worden uitgefaseerd. Voor nationale regelingen is UP.NL het voorkeursplatform tenzij dat niet kan. Voor BAS raakt een deel van de technische componenten verouderd doordat de fabrikanten van deze componenten stoppen met hun support en het onderhoud. Met RVO zijn we het eens dat BAS moet worden uitgefaseerd.

Voor de continuïteit van een betrouwbare uitvoering van regelingen, is het voor RVO daarom van belang dat het tijdig beschikt over nieuwe zaaksystemen. Dit is ook gewenst aangezien RVO een belangrijke rol heeft bij de uitvoering van de nieuwe kabinetsplannen, waarbij nieuwe regelingen worden opgetuigd en veranderingen elkaar snel zullen blijven opvolgen. Als voorbeeld geldt de SDE-regeling die als gevolg van de klimaatdoelen naar verwachting sterk zal gaan uitbreiden. Maar het is niet wenselijk die uitbreiding te realiseren in BAS gelet op de uitfasering, maar in één van de andere zaaksystemen. Welk ander zaaksysteem voor SDE geschikt is, is echter nog niet duidelijk.

Maak in 2022 duidelijke keuzes omtrent de zaaksystemen, waarbij de uitfasering van BAS een belangrijk aandachtspunt is.

5. SDE

5.1. Assuranceverklaringen CertiQ drie jaar achtereen oordelen met beperking

Het systeem van interne beheersing voor de certificering van duurzame energie bij CertiQ borgt de tijdigheid en betrouwbaarheid van de (aanlevering) van meetgegevens aan SDE. Dit systeem wordt jaarlijks onderzocht door een onafhankelijke accountant. Vanaf 2019 is er sprake van een oordeel met beperking. Hiervan is sprake als de werking van een deel van het systeem niet voldoet aan de interne beheersingsdoelstellingen. Dit is ook 2021 het geval. SDE concludeert dat de niet goed werkende systeemdelen, niet van invloed zijn op de verwerking van de meetgegevens van CertiQ. Een onderbouwing voor deze bewering ontbreekt echter.

Wij bevelen SDE aan te komen met een nadere analyse waarom de niet goed werkende systeemdelen van CertiQ geen invloed hebben op de tijdigheid en betrouwbaarheid van de meetgegevens. Tevens adviseren wij met CertiQ in overleg te treden over het oplossen van de (structurele) problemen zoals gerapporteerd door de onafhankelijke accountant.

5.2. Restore back-up verbeterd; recovery volgende stap

SDE heeft in 2021 samen met DICTU de eerste testen uitgevoerd op het terugzetten van back-up bestanden. SDE zal deze test jaarlijks herhalen. De ADR staat achter deze plannen.

Het is gewenst deze plannen zoveel mogelijk in lijn te brengen met het vernieuwde RVO-beleid ten aanzien van back-up en recovery. Daarin wordt een onderscheid gemaakt tussen restore en recovery. De huidige plannen van SDE zijn gericht op het terugzetten van back-up bestanden (restore) en niet op het herstellen van het gehele primaire proces na een calamiteit (recovery).

Wij bevelen SDE aan plannen te ontwikkelen voor een recovery-situatie en deze één keer per drie jaar te testen.

5.3. Aanbevelingen logging en monitoring niet afgerond in 2021

In 2020 heeft SDE logging ingevoerd voor het opsporen van ongeautoriseerde wijzigingen van belangrijke configuratie-instellingen in de SDE-applicatie. Om deze ongeautoriseerde wijzigingen daadwerkelijk te kunnen opsporen, dienen de loggingsgegevens ontsloten te worden in bijvoorbeeld een dashboard of rapportages. Deze actie is nog niet voltooid.

Wij adviseren SDE in 2022 een dashboard of rapportages te maken zodat deze belangrijke controles daadwerkelijk kunnen worden uitgevoerd.

6. Interpretatie regelgeving in de uitvoering

Wij kwamen in onze postencontroles bij een aantal regelingen tegen dat RVO aan de uitvoering van een voorwaarde in de regelgeving een eigen interpretatie gaf en dit niet altijd met de opdrachtgever had afgestemd. Indien afstemming wel had plaatsgevonden dan was dit soms op een te laag niveau bij de opdrachtgever.

Wij adviseren altijd op het juiste niveau issues over de uitvoering van de regelgeving met de opdrachtgever te bespreken en deze zodanig te documenteren dat ook achteraf is vast te stellen dat de goedkeuring op de juiste wijze is verleend. Daarbij kunnen wij ons voorstellen dat bij de departementen ook FEZ hierin door de opdrachtgever gekend wil worden.

7. Gebruik maken van werkzaamheden F&C en IAD

Wij willen in 2022 onderzoeken of wij meer gebruik kunnen maken van de IC-werkzaamheden van F&C. Mogelijk kunnen wij onze controle meer over het jaar in blokken indelen en met behulp van een PBC-list afspraken maken over de producten die wij van F&C daarbij kunnen gebruiken.

De ADR heeft het afgelopen controlejaar meer gebruik gemaakt van audits van de IAD. De ADR en IAD maken daar onderling afspraken over. Daarbij is het belangrijk om de planningen goed op elkaar af te blijven stemmen om wederzijds maximale synergie te behalen. Richting de toekomst wil de ADR de samenwerking met de IAD graag verder uitbouwen.

x

x

Auditdienst Rijk