Auditdienst Rijk
Ministerie van Financiën

Assurancerapport
Audit Monitoring PPS De Knoop Utrecht 2021

Colofon

Titel	Audit Monitoring PPS De Knoop Utrecht 2021
Uitgebracht aan	Persoonsgegevens van het DG Belastingdienst
Datum	18 augustus 2022
Kenmerk	2022-0000271157

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Aanleiding opdracht

Het facilitair beheer van het rijkskantoor De Knoop in Utrecht is ingericht op basis van het samenwerkingsmodel Publiek-Private Samenwerking (PPS). De afspraken die gemaakt zijn tussen de private partij (R Creators) en de publieke partij zijn vastgesteld in een DBFMO[1] overeenkomst (verder de overeenkomst). De publieke partij, de Shared Service Organisatie (SSO CFD) van het Directoraat Generaal Belastingdienst, treedt op als verantwoordelijke vertegenwoordiger van de publieke partij voor de prestatieverklaring van de dienstverlening die door de private partij wordt geleverd.

De -eisen voor het facilitair beheer waaraan de private partij moet voldoen zijn vastgelegd in de Outputspecificaties (OS). Deze prestatie-eisen zijn volgens bepalingen van de overeenkomst uitgewerkt in een contractueel vastgesteld monitoringsplan en geconcretiseerd in een geautomatiseerd registratiesysteem waaraan het betalingsmechanisme is gekoppeld (Axxerion). Dit registratiesysteem vormt het hart van het monitoren van de overeenkomst. Gezien het belang van een integer en betrouwbaar registratiesysteem is er in de overeenkomst opgenomen dat het totale monitoringsproces wordt ge-audit. Deze audit geeft zekerheid over de beheersmaatregelen die de kwaliteit van het monitoringsproces moeten waarborgen. De opdracht voor deze audit door de Belastingdienst komt uit de auditprogrammering van de Belastingdienst periode 1 april 2022 – 31 maart 2023.

Gebouwgebruikers en medewerkers van R Creators kunnen meldingen doen die te maken hebben met het facilitair beheer. De meldingen van gebouwgebruikers worden geregistreerd in een SAP-registratiesysteem van SSO CFD: hierna FMIS genaamd. Daarna worden ze via een interface geregistreerd, (handmatig) geclassificeerd en verwerkt in Axxerion. Meldingen van medewerkers van R Creators worden rechtstreeks in Axxerion geregistreerd en verwerkt.

Er is onderscheid te maken tussen verschillende soorten meldingen. Ze kunnen geregistreerd worden als klachten, wensen, informatieverzoeken en storingen, kortweg KWIS-meldingen.

Ook zijn er periodieke testen afgesproken die de kwaliteit testen van aspecten van het facilitair beheer. Alleen de door de gebouwgebuikers doorgegeven storingen en resultaten van periodieke testen kunnen in de regel tot een korting leiden (kortingsplichtig) bij afwijkingen van de OS eisen.

Leeswijzer

In hoofdstuk 1 is de conclusie van de audit verwoord. De hoofdstukken 2 tot en met 4 verwoorden de belangrijkste bevindingen. Niet alle bevindingen zijn verwoord en m.n. de afwijkingen op de normen komen aan de orde. De aanbevelingen zijn voor de auditee: R Creators. In hoofdstuk 5 hebben we de stand van zaken van de aanbevelingen uit de audit over 2020 opgenomen. In hoofdstuk 6 volgt de auditverantwoording. Bijlage 1 bevat de managementreactie van de opdrachtgever op dit rapport. In Bijlage 2 en Bijlage 3 staan het normenkader resp. het wegingsmodel.

[1] DBFMO staat voor Design, Build, Finance, Maintain en Operate

1 Conclusie

Naar ons oordeel is het geheel aan beheersmaatregelen in het monitoringsproces van de dienstverlening voortkomende uit de Publiek-Private Samenwerking in het rijksgebouw De Knoop in Utrecht in alle van materieel belang zijnde opzichten in opzet en bestaan per 31 december 2021 effectief en hebben gedurende 2021 als zodanig gewerkt.

Toelichting op de conclusie:
Deze audit is gepland en uitgevoerd zodat er een redelijke mate van zekerheid is verkregen over de beheersmaatregelen in het monitoringsproces en daarin geen afwijkingen van materieel belang zijn. Een goedkeurende conclusie wil niet zeggen dat aan alle normen in volledige mate hoeft te zijn voldaan. Bij een afwijking op een norm kunnen maatregelen bij een andere norm mitigerend zijn op het risico en/of aanvullende (ADR-) werkzaamheden kunnen aantonen dat het risico zich niet heeft voorgedaan.

Op basis van het wegingsmodel komt het volgende beeld eruit:

Weging normen (zie normenkader)	**Aantal afwijkingen**	**Leidt tot**
Zeer hoog	Geen afwijkingen	Geen effect op positief oordeel
Hoog	2 afwijkingen met een gemiddeld restrisico	Geen effect op positief oordeel
Gemiddeld en laag	2 afwijkingen met een gemiddeld restrisico	Geen effect op positief oordeel

De afwijkingen waarvan de weging van de norm 'hoog' is met een gemiddeld restrisico, betreffen de volgende bevindingen:
1. Eenmaal is de aanpassing van de toegestane hersteltijd niet geheel volgens de procedure verlopen (zie de toelichting in paragraaf 3.1.1);
2. Eenmaal is de implementatie van een wijziging in Axxerion niet voorafgegaan aan de toestemming van de eigenaar Axxerion (zie de toelichting in paragraaf 4.1.3).

De afwijkingen waarvan de weging van de norm 'gemiddeld' is met een gemiddeld restrisico, betreffen de volgende bevindingen:
1. Eenmaal is een functionele wijziging in Axxerion niet getest (zie de toelichting in paragraaf 4.1.3);
2. We kunnen geen uitspraak doen over het feit of de back-up – en recoverymaatregelen afdoende zijn getest (zie de toelichting in paragraaf 4.1.2).

Aanvullend op bovenstaande afwijkingen hebben we in de volgende hoofdstukken bevindingen genoemd die weliswaar nu een laag restrisico kennen, maar toch om een besluit over een mogelijke oplossing vragen.

2 Autorisaties voldoen aan de normen, behalve de niet-persoonsgebonden rechten

Onderstaande bevindingen zijn de belangrijkste bevindingen voor het onderwerp 'Rollen en autorisaties' uit de audit. Daar waar sprake is van een afwijking op de norm is deze meegewogen bij de oordeelsvorming.

2.1 Functiescheiding en periodieke controle van autorisaties zijn ingeregeld

Zowel in opzet, bestaan als werking is de organisatorische functiescheiding ingeregeld en gewaarborgd in Axxerion. Minimaal tweemaal per jaar voert R Creators hierop een formele controle uit. De laatste getekende versie van de autorisatiematrix (functie/autorisaties) is van 2020; er zijn sindsdien geen wijzigingen geweest. In een rapportage van Axxerion is inzichtelijk welke wijzigingen in de (niet speciale) toegangsrechten hebben plaatsgevonden (zie het volgende punt). Bij beëindiging van het dienstverband worden rechten ingetrokken.

De wachtwoordpolicy voldoet aan de normstelling.

2.2 Mutaties in medewerkers met speciale toegangsrechten zijn niet inzichtelijk

De rol van functioneel beheerder was in 2020 beperkt toegekend aan 3 medewerkers van R Creators, in 2022 zijn dit nog 2 medewerkers.
Het doorvoeren van mutaties in autorisaties voor medewerkers met speciale toegangsrechten (bv. de functioneel beheer rechten) worden uitgevoerd door de beheerder van Axxerion. De mutaties in deze autorisaties zijn niet vermeld in de rapportage van Axxerion.

Risico
Ongewenste of niet geaccordeerde autorisaties voor speciale toegangsrechten kunnen buiten zicht blijven waardoor deze rechten te ruim worden toegekend met als mogelijk gevolg dat wijzigingen in de KWIS-meldingen doorgevoerd kunnen worden door onbevoegde medewerkers. Dit risico is als 'laag' ingeschat.

Aanbeveling
Zorg dat mutaties in medewerkers met speciale toegangsrechten gelogd worden en inzichtelijk zijn, bijv. door periodieke rapportages met datumtoevoeging van ingang en intrekking van autorisaties.

2.3 Niet-persoonsgebonden accounts niet wenselijk

Bij de audit hebben we geconstateerd dat 3 actieve 'volledige gebruikers' niet persoonsgebonden zijn. Dit is onwenselijk omdat hiermee mutaties uitgevoerd kunnen worden waarvan niet inzichtelijk is of de mutaties zijn uitgevoerd door een medewerker die hiervoor de functie heeft. In de deelwaarneming van de KWIS-meldingen zijn overigens geen onterechte mutaties geconstateerd.

Dit is een vergelijkbare bevinding als over 2020 in het rapport is opgenomen.

Risico
Risico is het uitvoeren van mutaties door iemand die daarvoor niet de functie heeft en/of het onterecht kennisnemen van de gegevens in Axxerion. Dit risico is als 'laag' ingeschat.

Aanbeveling
We bevelen aan om de niet-persoonsgebonden accounts direct in te trekken.
- in juni 2022 is hiervoor een aanpassing in de policy doorgevoerd.

3 De verwerking van KWIS-meldingen voldoet aan de normen, feestdagen zijn verkeerd geprogrammeerd

Onderstaande bevindingen zijn de belangrijkste bevindingen voor het verwerken van de KWIS-meldingen uit de audit. Daar waar sprake is van een afwijking op de norm is deze meegewogen bij de oordeelsvorming.

3.1 Meldingen zijn verwerkt overeenkomstig de Outputspecificaties

Uit de door ons uitgevoerde deelwaarnemingen is gebleken dat de registratie en classificatie[2] overeenkomstig de OS zijn.
In Axxerion worden alle mutaties gelogd. Wijzigingen zijn hierdoor altijd traceerbaar ook voor de opdrachtgever. Uit de deelwaarneming en een aantal integrale controles blijkt dat de registratie van de datum/tijdstippen van melding en gereedmelding geen onverwachte structuren laten zien.

De verschillende processen rondom het verwerken en afhandelen van de KWIS-meldingen zijn beschreven in het Monitoringplan en de bijlagen daarbij. Deze processen worden in de praktijk ook grotendeels gevolgd. Er zijn enkele afwijkingen aangetroffen:

3.1.1 Eén aanpassing van de THT zonder BOM-formulier

Handmatige aanpassingen in de toegestane hersteltijd (THT) met een financieel gevolg mogen alleen met goedkeuring van de opdrachtgever worden uitgevoerd. Hiervoor dient een formulier gebruikt te worden waarop de details worden vermeld en de opdrachtgever officieel akkoord geeft. Wij hebben geconstateerd dat er bij 1 wijziging van de in totaal 29 wijzigingen in de THT het officiële BOM[3]- formulier niet aanwezig is. Er is wel een mail met akkoord van de opdrachtgever, dit sluit aan bij de registratie in Axxerion.

Axxerion voorziet verder in een dashboard voor het volgen van KWIS-meldingen, waarbij o.a. signaalwerking zit op het tijdig oplossen ervan.

Risico

Het is technisch mogelijk om een melding aan te passen zonder toestemming van de opdrachtgever. Dit kan effect kan hebben op de kortingsberekening. Dit risico is als 'gemiddeld' ingeschat.

Aanbeveling

Onderzoek of het mogelijk is om een Axxerion-rapport te maken met meldingen waarbij de THT is aangepast gecombineerd met de aanwezigheid van de BOM-formulieren.

3.1.2 Verkeerde instelling feestdag in systeem

De feestdagen zijn tot en met 2024 handmatig geprogrammeerd in Axxerion. Voor de pinksterdagen in 2021 is hiervoor een verkeerde datum gebruikt, nl. 23 en 24 april in plaats van 23 en 24 mei. Voor de kortingsplichtige meldingen zijn hierdoor een aantal THT's niet correct berekend:

---

[2] Hier zijnde de standaardmelding en het daarbij behorende regime, toegestane hersteltijd en wegingsfactor van de KWIS-meldingen
[3] BOM is een acroniem voor Betalingsmechanisme, Output Specificaties en Monitoring

- 1 THT is te vroeg berekend, deze was binnen de deadline opgelost – geen gevolgen.
- 3 THT's zijn later berekend dan zou moeten:
    - 2 meldingen hiervan zijn binnen de juiste THT opgelost;
    - 1 melding is niet binnen de juiste THT opgelost; voor deze melding was al een korting in rekening gebracht (€ 1.501,35), de korting komt met de juiste deadlineberekening neer op € 3.139,35.

Overigens is in Axxerion ook 5 mei (Bevrijdingsdag) niet als een feestdag opgenomen en wordt dus niet meegenomen in de berekening van de deadline.

Risico
Het risico bestaat dat door de verkeerde programmering van feestdagen een verkeerde berekening van de kortingen plaatsvindt. Dit risico heeft zich voorgedaan.

Aanbeveling
Controleer de juistheid van de reeds geprogrammeerde feestdagen. Volg bij mutaties het wijzigingsbeheerproces. Check jaarlijks voorafgaand aan het nieuwe jaar de ingestelde feestdagen. R Creators geeft aan in ieder geval dit laatste te gaan uitvoeren.

3.1.3 Reden van annuleren van KWIS-meldingen niet altijd helder beschreven

Voor de deelwaarneming en de geannuleerde meldingen is beoordeeld of het duidelijk is hoe de melding is opgelost. Als een KWIS-melding is geannuleerd valt deze verder buiten de monitoring. Voor de KWIS-meldingen (deelwaarneming) zijn de oplossingen goed gedocumenteerd. Hoewel het met enige inspanning vaak wel te herleiden is, is niet in alle gevallen de achterliggende reden van de annulering inzichtelijk gemaakt.

Een vergelijkbare bevinding is in het rapport over de audit 2020 opgenomen. Zie voor een toelichting hoofdstuk 5.

Risico
Gebrek aan inzicht in de achterliggende redenen van het annuleren van KWIS-meldingen of mogelijk niet terecht annuleren van meldingen. Dit risico is als 'laag' ingeschat.

Aanbeveling
Registreer de achterliggende reden van de annulering bij de KWIS-melding in Axxerion.

3.2 Doorlopende nummering loopt niet door

Bij de beoordeling van de doorlopende nummering van de KWIS-meldingen is geconstateerd dat er 1 nummer ontbreekt. Dit betreft een door systeembeheer uitgevoerde test die per abuis in de productieomgeving is uitgevoerd. Deze specifieke meldingen hebben geen invloed op de monitoring en het betalingsmechanisme het is echter onwenselijk dat er op deze wijze testen in de productieomgeving worden uitgevoerd omdat zonder specifieke rechten deze meldingen ook niet zijn te herkennen of in te zien. De logging en meldings-gegevens zijn wel opvraagbaar via functioneel beheer/systeembeheer. Vanuit de reguliere schermen voor registratie is het niet mogelijk om een melding te verwijderen.

Een vergelijkbare bevinding is in het rapport over de audit 2020 opgenomen. Zie voor een toelichting hoofdstuk 5.

Risico
KWIS-meldingen lopen niet mee in het betalingsmechanisme. Dit risico is als 'laag' ingeschat.

Aanbeveling
Voer het testen van KWIS-meldingen in de testomgeving uit. Als dit niet mogelijk is, volg dan de procedure voor het annuleren van een KWIS-melding.

3.3 Periodieke testen zijn uitgevoerd conform Monitoringsplan

De periodieke testen zijn uitgevoerd conform het Monitoringsplan, tenzij – volgens procedure – in overleg met de opdrachtgever daarvan af is geweken. De planning, uitvoering en resultaten zijn in Axxerion vastgelegd.
Er is een wijziging geweest van de test Integrale toegankelijkheid. De jaarlijkse visuele controles zijn hierbij komen te vervallen. Hiervoor is een nieuw plan van aanpak. De OS en Monitoringsplan zijn hier nog niet op aangepast.

3.4 Kortingen correct doorberekend

Vanuit de uitgevoerde deelwaarneming blijkt dat het betalingsmechanisme de kortingen correct heeft berekend. De kortingen zijn gefactureerd en afwijkingen en correcties zijn door de OG geaccordeerd.

De goedgekeurde wijzigingen zijn verwerkt in Relatics en alle partijen hebben de wijzigingen geaccordeerd. Uit Relatics blijkt dat er geen wijzigingen zijn geweest die van invloed zijn geweest op de standaardmeldingen (incl. de THT of de kortingsbedragen).

4 General IT-controls voldoen aan de norm, 1 norm is niet beoordeeld

4.1 Er kan gesteund worden op de GITC-beheersmaatregelen van de hostingpartij

Spacewell Axxerion voert het beheer voor haar eigen tool uit. Voor het beheer door deze organisatie is over de periode 1 januari tot en met 30 september 2021 een 3402 Type II – verklaring[4] afgegeven door Deloitte Consulting and Advisory BV/SRL. Aansluitend is er door Spacewell Axxerion over de periode 1 oktober tot en met 31 december 2021 een Bridgeletter afgegeven waarin is verklaard dat er geen significante wijzigingen zijn geweest in de control-omgeving.

Op basis van de conclusie en de bevindingen die staan beschreven in de ISAE3402 type II – verklaring over 2021 is de conclusie dat er gesteund kan worden op de GITC- beheersmaatregelen bij de hostingpartij.

De volgende bevindingen zijn aan de orde.

4.1.1 *Logische toegangsbeveiliging voldoet*

Aan de normen voor de logische toegangsbeveiliging is voldaan.

4.1.2 *Geen beoordeling van het periodiek toetsen van de back-up en recovery-maateregelen*

Er zijn geen specifieke beschikbaarheidseisen gesteld door de opdrachtgever, m.u.v. van de aanwezigheid van een Escrow contract. Op dat punt is voldaan aan de norm.

We kunnen geen uitspraak doen over de norm 5.4 'Back-up en recovery-maatregelen worden periodiek getest'. Uit het 3402-rapport blijkt niet of dit periodiek testen van de back-up – en recovery-maatregelen is beoordeeld in de audit. Wel blijkt uit het rapport dat de architectuur en de procedures voor back-up en recovery zijn beoordeeld.

Dit is een vergelijkbare bevinding als in 2020 in het rapport is opgenomen. Zie voor een toelichting hoofdstuk 5.

Risico

De back-up- en recovery-faciliteiten zijn ontoereikend. Dit risico is als 'gemiddeld' ingeschat.

Aanbeveling

Verzoek Axxerion om de auditfirma het periodiek testen van de back-up- en recovery-maatregelen op te nemen in de audit.

Door de migratie naar een ander platform zijn de back-upgegevens niet bewaard gebleven voor de periode 1 januari - 31 mei 2021. De auditor kon daardoor de effectiviteit van het back-up proces én de monitoring daarvan door de hostingpartij niet beoordelen. Voor de periode 1 juni – 30 september zijn geen relevante afwijkingen geconstateerd voor de betreffende normen.

[4] Bij een 3402-verklaring type II is zowel de opzet, het bestaan als de werking van de maatregelen in de scope beoordeeld door de auditor.

4.1.3 *Implementatie wijziging niet altijd voorafgegaan door test en toestemming eigenaar*

Uit de 3402-verklaring blijkt dat in een geval de implementatie van een wijziging niet voorafgegaan is door testen van de wijziging. Naderhand heeft de hostingpartij nog een review uitgevoerd op de wijziging en alsnog akkoord bevonden.

Bij een andere wijziging is geen toestemming van de interne eigenaar gegeven voorafgaand aan in-productieneming van een wijziging.

Risico

Wijzigingen die niet het gewenste effect hebben kunnen worden doorgevoerd of wijzigingen worden op het verkeerde moment geïmplementeerd. Deze risico's zijn als gemiddeld ingeschat.

Aanbeveling

Houd bij wijzigingen de procedure aan.

5 Opvolging aanbevelingen 2020

Een aantal bevindingen zijn bij de vorige audit over 2020 ook geconstateerd en gerapporteerd. Dit rapport is gedateerd op 7 januari 2022. R Creators geeft aan dat door de ontvangstdatum in maart 2022 van dit rapport en daarmee de kennisneming van de bevindingen over 2020 het opvolgen van de aanbevelingen niet voor het huidige controlejaar (2021) heeft kunnen uitvoeren.
We zien dit terug in het terugkeren van een aantal bevindingen uit 2020. De ADR heeft geconstateerd dat voor de aanbevelingen uit het controlejaar 2020 in de loop van 2022 een aantal verbeteringen in gang zijn gezet of zijn uitgevoerd, hiervan is bij de bevindingen melding gemaakt. Dit heeft echter geen invloed op het oordeel over de 2021 bevindingen.

De bevindingen met aanbevelingen uit 2020 en waarvoor in 2021 een vergelijkbare bevinding is geweest zijn terug te vinden in de hoofdstukken:
2.3 Niet-persoonsgebonden accounts niet wenselijk
3.2 Doorlopende nummering loopt niet door
3.1.3 Reden van annuleren van KWIS-meldingen niet altijd helder beschreven
4.1.2 Geen beoordeling van het periodiek toetsen van de back-up en recovery-maateregelen

Nieuwe bevindingen met aanbevelingen zijn:
2.2 Mutaties in medewerkers met speciale toegangsrechten zijn niet inzichtelijk
3.1.1 Eén aanpassing van de THT zonder BOM-formulier
3.1.2 Verkeerde instelling feestdag in systeem
4.1.3 Implementatie wijziging niet altijd voorafgegaan door test en toestemming eigenaar

Bevindingen uit 2020 die in 2021 niet meer voorkomen:
Niet van toepassing

6 Verantwoording onderzoek

6.1 Afbakening

Doelstelling

De doelstelling is om met een redelijke mate van zekerheid een oordeel te vormen over de betrouwbaarheid van de opzet en bestaan van het monitoringsproces per 31 december 2021 en de werking over de periode 1 januari - 31 december 2021. Dit houdt in dat vastgesteld zal worden of de registratie, rapportage en facturatie van de geleverde prestaties juist, tijdig en volledig zijn.

Onderzoeksobject

Bij het in de doelstelling benoemde monitoringsproces is een aantal onderdelen te onderscheiden die tot het object van het onderzoek behoren. Dit zijn:

- De procedures en de gegevens van de verwerking van de meldingen en de periodieke testen die betrekking hebben op de OS. Dit is inclusief het interne proces van categorisering van meldingen door R Creators;
- De procedure van de afhandeling van niet correcte – of niet volledige meldingen;
- Het proces van de berekening en de financiële afwikkeling van de eventuele kortingen;
- De procedure van het wijzigen van stamgegevens/outputspecificaties in Axxerion;
- De verleende toegangsrechten (op applicatieniveau) in Axxerion;
- Het beheer van Axxerion door de leverancier, meer specifiek de maatregelen op het gebied van de beveiliging en continuïteit.

Buiten het object van onderzoek vallen de interfaces met de aanleverende applicaties, zoals het FMIS van de opdrachtgever en het Gebouwbeheersysteem. De audit start bij de registratie in Axxerion. Niet gemelde- en niet doorgegeven KWIS-meldingen vanuit de opdrachtgever vallen buiten de scope.

Bij de normen aangaande KWIS-meldingen wordt over het algemeen gefocust op de kortingsplichtige meldingen, dit zijn de storingsmeldingen afkomstig uit FMIS van de opdrachtgever.

Normenkader

In de bijlage 1 staat het normenkader. Wij hebben dit normenkader speciaal voor audits van de monitoring van PPS-opdrachten opgesteld. De opdrachtgever heeft mede input geleverd voor het normenkader, de weging aan de normen gegeven en het normenkader goedgekeurd. De auditee is geïnformeerd over het normenkader door de opdrachtgever.

Het normenkader is bedoeld als algemeen geldend kader voor audits als deze. De normen zijn afkomstig uit de Baseline Informatiebeveiliging Overheid, algemene IT-beheernormen en de processen zoals die naar voren komen in het Monitoringsplan en de bijlagen bij het Monitoringsplan. Per audit zal gebruik worden gemaakt van de specifieke afspraken als die meer invulling geven aan een norm. Deze afspraken kunnen afkomstig zijn uit het Monitoringsplan (incl. de bijlagen), het DBFMO-contract, de Outputspecificaties en beheerhandboeken als bij de auditee aanwezig.

Materialiteit

Materialiteit is een maatstaf om te bepalen of een afwijking significant is. Met andere woorden: met materialiteit definieer je een drempel. Bij deze audit is materialiteit vormgegeven door weging van de normen (zie Bijlage 2) en de eventuele afwijkingen van die normen. De weging van mogelijke afwijkingen is opgenomen in Bijlage 3.

Significante inherente beperkingen
In dit rapport geven we een oordeel over de periode 1 januari 2021 tot en met 31 december 2021. We doen geen uitspraken over de opzet, het bestaan en/of de werking in toekomstige perioden.

Niveau van zekerheid
Deze audit is uitgevoerd met een redelijke mate van zekerheid. Dit wil zeggen dat onze assurance-opdracht is uitgevoerd met een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens onze assurance-opdracht niet alle materiële fouten en fraude ontdekken.

Opdrachtgever en opdrachtnemer en verantwoordelijkheden
Deze assurance-opdracht is door de Auditdienst Rijk uitgevoerd in opdracht van de Persoonsgegevens van het Directoraat Generaal Belastingdienst van het Ministerie van Financiën. Opdrachtnemer namens de ADR is de Persoonsgegevens Persoonsgegevens bij de Auditdienst Rijk, ressorterend onder het Ministerie van Financiën.

Het is de verantwoordelijkheid van de opdrachtgever om de bevindingen te delen met de auditee en afspraken te maken over het oplossen van de afwijkingen van de normen. Het is de rol van de IT-auditor om onafhankelijk een conclusie tot uitdrukking te brengen over het onderzoeksobject.

6.2 Gehanteerde Standaarden

Deze opdracht is uitgevoerd volgens de Richtlijn voor assurance-opdrachten door IT-auditors (NOREA Richtlijn 3000D). De vereisten uit het Reglement Gedragscode ('Code of Ethics') zijn nageleefd. Op grond van artikel 900.11.T5 van dit reglement is dit onderzoek uitgevoerd door een onafhankelijke IT-auditor.

6.3 Werkzaamheden

Deze audit komt voort uit de auditprogrammering van de Belastingdienst periode 1 april 2022 – 31 maart 2023. Om ons oordeel te kunnen formuleren hebben we kunnen beschikken over voldoende en geschikte controle-informatie. Alle onderkende werkzaamheden zijn volledig uitgevoerd.

De werkzaamheden hebben o.a. bestaan uit het beoordelen van:
- Het Monitoringsplan en de daarin verwoorde procesbeschrijvingen;
- Het bestaan en de werking van het proces van het melden en registreren van de KWIS-meldingen door het uitvoeren van een deelwaarneming en data-analyses;
- De berekening van de kortingen en de verwerking ervan in de facturatie;
- De toegekende autorisaties in Axxerion gedurende 2021 (m.n. gericht op geen doorbreking functiescheiding);
- De 3402-verklaring Type II van Axxerion en de bridgeletter (ten behoeve van de kwaliteit van het beheer door de leverancier).

De auditinformatie is verkregen door het houden van interviews, het beoordelen van de documentatie en het uitvoeren van lijncontroles, data-analyses, deelwaarnemingen en analyses. De interviews zijn vastgelegd in verslagen welke voor hoor en wederhoor zijn voorgelegd aan de geïnterviewden.

Daarna heeft analyse en oordeelsvorming plaatsgevonden. De bevindingen die daaraan ten grondslag liggen hebben wij voor hoor en wederhoor met de auditee op 2 augustus 2022 besproken. De gemaakte opmerkingen zijn verwerkt.

De auditee heeft op 11 juli 2022 in een Letter of Representation bevestigd verantwoordelijk te zijn voor het onderzoeksobject en dat alle relevante informatie aan ons is aangeboden.

De bevindingen, conclusies en aanbevelingen in het conceptrapport zijn besproken met de opdrachtgever op 18 augustus 2022.

6.4 Verspreiding rapport

De opdrachtgever, Persoonsgegevens van het Directoraat Generaal Belastingdienst, is eigenaar van dit rapport.

Dit rapport is primair bestemd voor deze opdrachtgever met wie wij deze opdracht zijn overeengekomen. Hoewel het rapport de context van het onderzoek zo goed mogelijk probeert te beschrijven, is het mogelijk dat iemand die de context niet (volledig) kent de uitkomsten anders interpreteert dan bedoeld.

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Voor openbaarmaking door het opdrachtgevende ministerie van door de ADR aan dit ministerie uitgebrachte rapporten gelden de voorschriften uit de Wet open overheid. De minister van Financiën stuurt elk halfjaar een overzicht van door de ADR uitgebrachte rapporten naar de Tweede Kamer.

7 Ondertekening

Groningen, 18 augustus 2022

Persoonsgegevens

Auditdienst Rijk

Belastingdienst

Naam dienstonderdeel
SSO CFD
HFA
Facilitaire Ontwikkeling & Strategisch Advies
Tiberdreef 12-24
3661 GG Utrecht
Contactpersoon
Persoonsgegevens

Management reactie
Assurancerapport monitoring PPS De Knoop Utrecht 2021

Datum
21 oktober 2022

Hierbij de reactie op de rapportage van de Auditdienst Rijk betreffende het Assurancerapport monitoring PPS De Knoop 2021.

Het oordeel van de audit is positief, de genoemde aandachtspunten welke zijn benoemd in hoofdstuk 5 worden geagendeerd en voorzien van een actiehouder op het monitoringsoverleg PPS de Knoop Utrecht. De afspraken worden indien van toepassing vastgelegd in het monitoringsplan.

Met vriendelijke groet,

Persoonsgegevens

Bijlage 2 Normenkader

Nr.	Norm	Zwaarte van de norm
A	**Proces en applicatie controls**	
1	**Rollen en autorisaties**	
1.1	Organisatorische functiescheidingen zoals belegd in de organisatie dienen te zijn gewaarborgd door middel van autorisaties in de applicatie.	Hoog
1.2	Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld. De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld.	Laag
1.3	Het gebruiken van groepsaccounts is niet toegestaan, tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.	Gemiddeld
1.4	Autorisatie op basis van need to know principe: Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.	Laag
1.5	Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.	Zeer hoog
1.6	De autorisatiematrix dient te zijn gedocumenteerd, actueel te zijn en door de eigenaar van de applicatie te zijn geautoriseerd.	Hoog
1.7	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.	Gemiddeld
1.8	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd. Bij wijzigingen behoren ze te worden aangepast. Mutaties in autorisaties dienen te worden gelogd.	Zeer hoog
1.9	Wachtwoorden dienen sterk te zijn en periodiek te worden gewijzigd (password policy). Sterk is: • Als er geen gebruik wordt gemaakt van two-factor authenticatie, is de wachtwoordlengte minimaal 8 posities en complex van samenstelling. Vanaf een wachtwoordlengte van 20 posities vervalt de complexiteitseis. • In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord vernieuwd.	Hoog
2	**Vastleggen van meldingen**	
2.1	Incidenten, storingen en helpdeskverzoeken (meldingen) dienen betrouwbaar (juist, tijdig en volledig) te worden geregistreerd.	
a	*Het tool dient te zijn voorzien van een gesynchroniseerde standaarddatum/tijdsaanduiding gebaseerd op standaard UTC.*	*Gemiddeld*
b	*Meldingen mogen niet onvolledig kunnen worden ingevoerd.*	*Hoog*
c	*Meldingen worden geclassificeerd en geprioriteerd conform de afspraken in de Outputspecificaties.*	*Hoog*
d	*Meldingen zijn doorlopend genummerd.*	*Gemiddeld*
e	*Datum/tijd van invoer van de melding en registratie hebben een logisch verband. (bijv. invoertijdstip = 'meld'tijdstip (meegegeven uit FMIS) en afwijkingen zijn herleidbaar).*	*Hoog*
f	*Indien van toepassing: indien de koppeling tussen de afzonderlijke registratiesystemen niet functioneert, is er een workaround waarbij de procedures een betrouwbare verwerking van de meldingen waarborgen.*	*Laag*

Nr.	Norm	Zwaarte van de norm
2.2	Incidenten, storingen en helpdeskverzoeken (meldingen) dienen op een betrouwbare wijze en conform de opgestelde procesgang en workflow te worden afgehandeld.	
a	*Gegevens die van invloed zijn op de 'afrekening' mogen niet tussentijds gecorrigeerd worden zonder correctieformulier van de Opdrachtgever.*	*Hoog*
b	*Meldingen kunnen niet worden verwijderd.*	*Zeer hoog*
c	*Meldingen worden bewaakt op tijdige afhandeling*	*Laag*
2.3	De betrouwbaarheid (juist-, tijdig- en volledigheid) van het gereedmeldingstijdstip dient te zijn gewaarborgd.	
a	*Melding dient op juiste tijdstip te worden gereed gemeld.*	*Hoog*
b	*Oplossing van de melding dient te worden gedocumenteerd.*	*Gemiddeld*
2.4	Het plannen van de periodieke testen (periodiciteit bepaald in het Monitoringsplan), het uitvoeren daarvan alsmede de betrouwbare vastlegging dienen te zijn gewaarborgd.	Hoog
3	**Rekenregels en Kortingsberekeningsmechanisme**	
3.1	De relatie tussen de Outputspecificaties en de kortingberekeningsregels is eenduidig.	Zeer hoog
3.2	Nieuwe Outputspecificaties en wijzingen daarin zijn op een beheerste wijze geïmplementeerd in het monitoringsysteem inclusief het kortingsberekenings-mechanisme.	Zeer hoog
3.3	De kortingen uit het kortingsberekeningsmechanisme zijn gefactureerd; eventuele afwijkingen zijn goedgekeurd door de opdrachtgever.	Zeer hoog
B	**IT General Controls**	
4	**Logische toegangsbeveiliging**	
4.1	Remote access is beveiligd door middel van user-ids en wachtwoorden (eventueel ook op basis van tokens).	Hoog
4.2	Remote datacommunicatie is beschermd (VPN, HTTPS).	Hoog
5	**Continuïteit**	
5.1	Continuïteitsmaatregelen zijn in overeenstemming met de contractueel overeengekomen beschikbaarheidseisen.	Gemiddeld
5.2	Er is een actueel, gedocumenteerd en door het management geaccordeerd plan voor continuering van de dienstverlening en handhaving van het service niveau.	Gemiddeld
5.3	Maatregelen van back-up en recovery zijn getroffen opdat gegevens niet verloren gaan en de beschikbaarheid van de applicatie binnen de contractueel overeengekomen tijden kan worden hersteld.	Hoog
5.4	Back-up en recovery maatregelen worden periodiek getest. Op basis hiervan wordt het plan geëvalueerd en indien nodig verbeteringen getroffen.	Gemiddeld
6	**Wijzigingsbeheer monitoringsapplicatie**	
6.1	Wijzigingen in (1) de programmatuur, in (2) de applicatie, in (3) de database en in (4) het onderliggende platform dienen op een gecontroleerde en gedocumenteerde manier plaats te vinden.	Hoog
a	Wijzigingsverzoeken en de afhandeling daarvan is gedocumenteerd en voor ieder wijzigingsverzoek is (achteraf) een audittrail beschikbaar.	Hoog
b	Wijzigen dienen voor in gebruik name te worden getest.	Gemiddeld
c	Gebruikers dienen in de test te worden betrokken.	Laag
d	Testscenario's worden gehanteerd en testbevindingen worden gedocumenteerd.	Hoog

Nr.	Norm	Zwaarte van de norm
e	Wijzigingen dienen alleen met toestemming van de interne eigenaar van de applicatie te worden geïmplementeerd in de productieomgeving.	Hoog
f	Gebruikers worden geïnformeerd over aard van de wijziging en het moment van implementatie.	Gemiddeld
g	Na de implementatie van wijzigingen vindt aanvullende monitoring plaats op het correct werken van de applicatie.	Hoog

Bijlage 3 Wegingsmodel

Weging normen (zie normenkader)	**Verschil**	**Leidt tot een oordeel met een**
Zeer hoog	1 (en meer) x resterend hoog restrisico	Afkeurende conclusie
Zeer hoog	>1 x resterend gemiddeld restrisico	Afkeurende conclusie
Hoog	1 (en meer) x resterend hoog restrisico	Afkeurende conclusie
Hoog	>2 x resterend gemiddeld restrisico	Afkeurende conclusie
Gemiddeld en laag	>5 resterend gemiddeld restrisico	Afkeurende conclusie. Indien het gemiddeld restrisico 1 onderwerp betreft, dan een oordeel met een beperking

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