Belastingdienst

Naam dienstonderdeel
SSO CFD
HFA
Facilitaire Productontwikkeling (FPO)
Tiberdreef 12-24
3661 GG Utrecht

Contactpersoon
persoonsgegevens

Datum
21 september 2021

Management reactie
Assurancerapport monitoring PPS Hamburgerbroeklaan Doetinchem 2020

Hierbij de reactie op de rapportage van de Auditdienst Rijk betreffende het Assurancerapport monitoring PPS Hamburgerbroeklaan Doetinchem 2020.
Het oordeel van de audit is positief, de genoemde aanbevelingen welke zijn geconstateerd in hoofdstuk 2.1. - 2.2 - 3.1. - 3.4 – 4 en 5 worden geagendeerd en voorzien van een actiehouder op het tactisch PPS Doetinchem overleg.

Met vriendelijke groet,

persoonsgegevens
persoonsgegevens Huisvesting, Facilitaire Productontwikkeling en ARBO

Auditdienst Rijk
Ministerie van Financiën

Assurancerapport
Monitoring PPS Hamburgerbroeklaan Doetinchem 2020

definitief

Colofon

Titel	Monitoring PPS Hamburgerbroeklaan Doetinchem 2020
Uitgebracht aan	Directeur CFD
Datum	21 september 2021
Kenmerk	

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Context opdracht

Inleiding

Het facilitair beheer van het Belastingdienst kantoor te Doetinchem is ingericht op basis van het samenwerkingsmodel Publiek-Private Samenwerking (PPS). De afspraken die zijn gemaakt tussen de private partij en de publieke partij zijn vastgesteld in een DBFMO overeenkomst. De Shared Service Organisatie voor Facilitaire Dienstverlening (verder in deze opdrachtbevestiging afgekort tot SSO CFD) treedt op als verantwoordelijke vertegenwoordiger van de publieke partij voor de prestatieverklaring van dienstverlening die door de private partij wordt geleverd. De prestatie-eisen waaraan de private partij (Facilicom) moet voldoen zijn vastgelegd in de Outputspecificaties (OS) welke een onderdeel is van de DBFMO-overeenkomst. De 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. Dit registratiesysteem is een SAAS-oplossing dat wordt beheerd door een derde partij, te weten Axxerion. Het vormt het hart van het monitoren van de overeenkomst. Facilicom is verantwoordelijk voor de uitvoering van de afspraken en de registratie in het registratiesysteem Axxerion (in het vervolg van het rapport kortweg met Axxerion aangeduid).

Gezien het belang van een integer en betrouwbaar registratiesysteem is er in de overeenkomst opgenomen dat jaarlijks het totale monitoringsproces (melding - registratie - afhandeling, facturatie inclusief de werking van het registratiesysteem) wordt ge-audit.

Opdrachtgever en opdrachtnemer

Deze assurance-opdracht is door de Auditdienst Rijk (ADR) uitgevoerd in opdracht van de persoonsgegevens SSO CFD. Opdrachtnemer namens de ADR is de persoonsgegevens VOS bij de Auditdienst Rijk (ADR).

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 2020 en de werking over 2020. Dit houdt in dat vastgesteld zal worden of de registratie, rapportage en facturatie van de geleverde prestaties juist, tijdig en volledig zijn.

Leeswijzer

In hoofdstuk 1 is de conclusie uit de audit verwoord. De hoofdstukken 2 tot en met 5 verwoorden de belangrijkste, niet alle, bevindingen. In hoofdstuk 6 volgt de auditverantwoording. In de bijlagen 1 en 2 staan het normenkader en het wegingsmodel. Bijlage 3 bevat de reactie van de opdrachtgever op dit rapport.

1 Conclusie

Naar ons oordeel is het geheel aan beheersmaatregelen in het monitoringsproces in alle van materieel belang zijnde opzichten in opzet en bestaan per 31 december 2020 effectief en hebben gedurende 2020 als zodanig gewerkt.

De conclusie is afgegeven op basis van het vooraf afgesproken wegingsmodel van de bevindingen (bijlage 2) en de weging van de normen (bijlage 1). De conclusie is afgegeven met een redelijke mate van zekerheid. Dat wil niet zeggen dat aan alle normen is voldaan, maar de afwijkingen zijn niet van dusdanige aard dat het van invloed is op het materieel belang.

2 Autorisatiebeheer voldoet grotendeels aan de normstelling; de wachtwoordeisen zijn onvoldoende

2.1 Autorisatiebeheer voldoet grotendeels aan de normstelling

In het Monitoringsplan is de procedure voor het autorisatiebeheer beschreven. Deze procedure voldoet aan de eisen vanuit het oogpunt van functiescheiding bij het toekennen van autorisaties. De opzet voldoet. Wij hebben geconstateerd dat bij het toekennen van de autorisaties de functiescheiding tussen beschikken, uitvoeren en controleren is gehandhaafd. De procedure is als een proces ingebouwd in Axxerion. De procedure is in 'bestaan' en 'werking' aanwezig.

De autorisaties zelf zijn role-based en zijn toegekend op basis van het need-to-know-principe. Vergaande bevoegdheden zijn slechts aan de 2 functioneel beheerders toegekend. Hiermee is aan de normen voldaan.

De autorisatiematrix is aanwezig en is actueel. Het is in 2020 niet op enig moment door de verantwoordelijk persoonsgegevens van Facilicom goedgekeurd.

Risico

Er is een risico dat medewerkers geautoriseerd zijn waarvan de verantwoordelijk persoonsgegevens dit niet gewenst vindt.

Aanbeveling

We bevelen aan éénmaal per jaar de autorisatiematrix door de verantwoordelijk persoonsgegevens van Facilicom te laten autoriseren.

2.2 Eisen aan de wachtwoorden zijn onvoldoende

Een gebruiker heeft toegang tot Axxerion door gebruik te maken van een gebruikersnaam en een wachtwoord. De gebruikersnaam is gekoppeld aan een rol die past bij de functie van de gebruiker. De eisen die aan de wachtwoorden zijn gesteld zijn niet voldoende. Feitelijk zijn er geen eisen gesteld, met uitzondering dat het wachtwoord eenmaal in de 60 dagen gewijzigd dient te worden.

Risico

Het risico is dat gegevens niet integer zijn doordat een wachtwoord is geraden/gehackt zodat onbevoegden misbruik konden maken van de bevoegdheden van anderen met ruimere rechten. Afhankelijk van welke gegevens gewijzigd worden kan dit tot gevolg hebben dat kortingen niet juist berekend worden. Ook privacy-gevoelige gegevens kunnen ongewenst verkregen worden.

Aanbeveling

We bevelen aan om meer eisen aan de wachtwoorden te stellen, passend bij de risico's die gepaard gaan met de systeemgerelateerde gegevens.

3 KWIS-meldingen: niet alle GBS-meldingen in Axxerion, classificatie juist en tijdig gereed gemeld.

3.1 Volledigheid van de GBS-meldingen in Axxerion niet gewaarborgd

We hebben geconstateerd dat de KWIS-meldingen niet doorlopend zijn genummerd, waardoor het onzeker is of alle KWIS-meldingen zijn geregistreerd. Er is naar aanleiding van deze tussentijdse bevinding door Facilicom en de toolleverancier van Axxerion onderzoek gedaan naar mogelijke oorzaken van de missende KWIS-meldingen. Uit dit onderzoek bleek dat een belangrijke oorzaak is gelegen in een niet goed werkende interface tussen het Gebouwbeheersysteem (GBS) en Axxerion. Dit onderzoek is uitgevoerd op basis van logging uit het GBS en rapportages uit Axxerion met aanvullende toepasbare informatie die de functioneel beheerder tot zijn beschikking had. Met dit onderzoek is aangetoond dat voor het grootste deel van de KWIS-meldingen de oorzaak ligt aan niet vastgelegde meldingen uit het GBS. Overige missende nummers konden worden verklaard door het feit dat de oorspronkelijke rapportage van de KWIS-meldingen een onvolledige weergave was.

De operationeel manager heeft aangegeven dat de GBS-meldingen op zichzelf zijn gemonitord vanuit de signalering van het GBS.

Desalniettemin bestaat het onderstaande risico hiermee nog steeds.

Risico
Voor de opdrachtgever niet goed inzichtelijke GBS-meldingen doordat niet alle meldingen in Axxerion zijn geregistreerd en mogelijke kortingen hierdoor niet worden doorberekend aan de opdrachtgever.

Aanbevelingen
We doen de volgende aanbevelingen:

- Los het probleem op van de niet goed functionerende interface tussen het GBS en Axxerion;
- Zorg voor een continue sluitende verklaring van de missende meldingen en de daarbij behorende kortingsberekeningen.

3.2 KWIS-meldingen zijn juist geclassificeerd

Op basis van de deelwaarneming is de conclusie dat de KWIS-meldingen juist zijn geclassificeerd. Dat houdt in dat de classificatie conform de Outputspecificaties is uitgevoerd en de juiste toegestane hersteltijd is gehanteerd. Gegevens die van invloed zijn op de afrekening, zoals de classificatie, mogen volgens afspraak alleen worden gewijzigd na goedkeuring van de opdrachtgever. Dit is een enkele maal voorgekomen en is altijd voorzien van een akkoord van de opdrachtgever.

3.3 KWIS-meldingen zijn terecht en tijdig gereed gemeld.

Voor alle posten uit de deelwaarneming is er afdoende informatie aanwezig die aantoont dat de KWIS-meldingen terecht en met de juiste tijd gereed zijn gemeld. Het annuleren dan wel niet-ontvankelijk verklaren van een KWIS-melding is door ons integraal beoordeeld. Al deze KWIS-meldingen zijn conform de procedure verlopen.

3.4 Kortingen juist berekend

Bij overschrijding van de toegestane hersteltijd zijn de kortingsbedragen cf. de Outputspecificaties berekend. Bij de handmatige doorrekening naar de factuur van Q4 is vergeten de indexatie toe te passen (het bedrag is niet materieel: betreft € 24).

Risico
De indexatie wordt niet (juist) toegepast.

Aanbeveling
Wij bevelen aan om na te gaan of de procedure aangepast dient te worden, met name voor de handmatige doorberekening van de indexatie.

4 Alle periodieke testen zijn uitgevoerd, conclusie uit de periodieke test naar de brandmeldinstallatie niet consistent

4.1 Alle periodieke testen zijn uitgevoerd

In 2020 hebben de PPS-partijen wijzigingen aangebracht in de periodieke testen. Er zijn periodieke testen vervallen en nieuwe periodieke testen geformuleerd. De bijbehorende protocollen zijn aangepast, inclusief de periodiciteit en kortingsbedragen. Alle periodieke testen zijn uitgevoerd, verwerkt en verantwoord volgens de vastgelegde processen in het Monitoringsplan.

4.2 Conclusie uit de periodieke test naar de brandmeldinstallatie niet consistent

In het kader van de periodieke test 'beschikbaarheid rapportages, vergunningen en certificaten' is er een test door een externe partij uitgevoerd naar de brandmeldinstallatie en de sprinklerinstallatie (document PRV12-219016921 d.d. 21 februari 2020). Het oordeel van de uitvoerder van deze test is positief geformuleerd. Echter indien wordt gekeken naar de voorwaarden waaronder een dergelijk oordeel mag worden afgegeven, zou het oordeel niet positief kunnen zijn. Dit gaat om opmerkingen in de rapportage die te maken hebben met een aantal NEN-normen waaraan voldaan dient te zijn, waarvan het in het kader van onze audit te ver gaat om de impact ervan te (kunnen) beoordelen. Niet alle opmerkingen uit de rapportage zijn in 2020 verholpen.

Risico
Risico is dat de brandmeldinstallatie en/of de sprinklerinstallatie niet correct functioneert indien het noodzakelijk is.

Aanbeveling
Bespreek met de externe partij wat de waarde van de opmerkingen in de rapportage is, terwijl er een positief oordeel is afgegeven en leg de conclusie hieruit vast met akkoord van beide partijen.

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

Wij hebben de beschikking gekregen over de ISAE3402 type II – verklaring over 2020 die betrekking heeft op GITC-beheersmaatregelen bij de hostingpartij van Axxerion. Dat wil zeggen dat door de auditfirma die de verklaring heeft afgegeven zowel de opzet en het bestaan als de werking is getoetst van de GITC-beheersmaatregelen bij de hostingpartij.

Op basis van de bevindingen die staan beschreven in de ISAE3402 type II – verklaring over 2020 is de conclusie dat er gesteund kan worden op de GITC-beheersmaatregelen bij de hostingpartij. Aan de normen op dit gebied uit ons normenkader is voldaan. Op 1 punt kunnen we echter geen uitspraak doen, omdat dit niet is getoetst. Dit betreft de norm 7.4 'Back-up en recovery-maatregelen worden periodiek getest'.

Risico
De back-up en recovery-maatregelen werken niet in de situatie dat ze nodig zijn.

Aanbeveling
We bevelen aan te overleggen met de auditfirma de ISAE3402 type II – audit uit te breiden met de toets op het testen van de back-up- en recovery-maatregelen.

6 Verantwoording onderzoek

6.1 Afbakening en werkzaamheden

Bij de 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 classificeren van meldingen bij Facilicom;
- Het proces van de berekening en de financiële afwikkeling van de eventuele kortingen;
- De verleende toegangsrechten (autorisaties) in Axxerion;
- Het beheer van Axxerion door de leverancier.

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.
- de berekening van de kortingen en de verwerking ervan in de facturatie.
- de toegekende autorisaties in Axxerion gedurende 2020 (m.n. gericht op geen doorbreking functiescheiding).
- De 3402-verklaring Type II van Axxerion (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, deelwaarnemingen en analyses al dan niet met geautomatiseerde tools. De interviews zijn vastgelegd in verslagen welke voor hoor en wederhoor zijn voorgelegd aan de geïnterviewden.

6.2 Gehanteerde Standaard

Deze opdracht is uitgevoerd volgens de Richtlijn voor assurance-opdrachten door IT-auditors (NOREA Richtlijn 3000D).

6.3 Verspreiding rapport

De opdrachtgever persoonsgegevens CFD, is eigenaar van dit rapport.

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de ADR een rapport heeft geschreven, het rapport binnen zes weken op de website van de rijksoverheid plaatst, tenzij daarvoor een uitzondering geldt. De minister van Financiën stuurt elk halfjaar een overzicht naar de Tweede Kamer met de titels van door de ADR uitgebrachte rapporten en plaatst dit overzicht op de website.

7 Ondertekening

Groningen, 21 september 2021

persoonsgegevens

Auditdienst Rijk

Bijlage 1 Normenkader

Nr.	Norm	weging 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	Periodiek worden toegekende autorisaties op actualiteit (uitdiensttredingen, functiewijzigingen, geen gebruik, aangepaste rechten) gecontroleerd en bevestigd door het management.	Laag
1.3	Autorisaties dienen te zijn gebaseerd op een role-based toegangsconcept waarbij gebruikers behoren tot rollen en aan rollen autorisaties zijn toegewezen	Gemiddeld
1.4	Autorisatie op basis van need to know principe: Gebruikers dienen uitsluitend toegang te hebben tot programma's (rollen) die zij ten behoeve van hun werkzaamheden nodig hebben.	Laag
1.5	Administrator rechten zijn beperkt toegekend.	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	Aanvragen van autorisaties c.q. aanpassen van autorisaties verloopt via een formele procedure en pas na goedkeuring worden rechten toegekend.	Gemiddeld
1.8	Mutaties in autorisaties dienen te worden gelogd zodat wijzigingen achteraf herleidbaar en controleerbaar zijn (audittrail).	Zeer hoog
1.9	Wachtwoorden dienen sterk te zijn en periodiek te worden gewijzigd (password policy).	Hoog
2	**Vastleggen van meldingen**	
2.1	Incidenten, storingen en helpdeskverzoeken (meldingen) dienen betrouwbaar (juist, tijdig en volledig) te worden geregistreerd.	
a	Het gehele systeem dient te zijn voorzien van een gesynchroniseerde standaarddatum/tijdsaanduiding gebaseerd op standaard UTC.	middel
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	Indien van toepassing: indien de koppeling tussen de afzonderlijke registratiesystemen niet functioneert, is er een workaround waarbij de betrouwbare verwerking van de meldingen is getoetst.	Laag
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	Wijzigingen in gegevens die mogelijk van invloed zijn op de "Afrekening" (bijv. on hold, niet ontvankelijk of facilitair) dienen achteraf inzichtelijk te zijn.	Zeer hoog
c	Meldingen kunnen niet worden verwijderd.	Zeer hoog

d	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
c	indien van toepassing: indien de koppeling tussen de afzonderlijke registratiesystemen niet functioneert dient in de workaround getoetst te worden dat het gereedmeldingstijdstip juist is en de afmelding naar de melder te zijn opgenomen.	Gemiddeld
2.4	Het plannen van de periodieke testen (als onderdeel van de PPS-overeenkomst), het uitvoeren daarvan alsmede de betrouwbare vastlegging dienen te zijn gewaarborgd.	Hoog
3	**Rekenregels**	
3.1	De relatie tussen de outputspecificatie en de kortingberekeningsregels moet eenduidig zijn vast te stellen	Zeer hoog
3.2	Betrouwbaarheid van kortingberekeningsregels voor alle Outputspecificaties dient te zijn gewaarborgd.	Zeer hoog
3.3	Betrouwbaarheid van het geautomatiseerde kortingberekeningsmechanisme moet zijn gewaarborgd.	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 (volgens procedures die in het monitoringsplan of het kwaliteitsplan zijn vastgesteld)**	
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 (in lijn met het plan) 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

Bijlage 2 Wegingsmodel

Het oordeel is goedkeurend tenzij afgeweken wordt van de normen. In de onderstaande tabel is het effect op het oordeel na weging van de verschillen met de normen en het restrisico weergegeven:

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

Er zal een oordeelsonthouding worden afgegeven indien er geen toereikende informatie gegeven kan worden.

Bijlage 3 Managementreactie

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