Auditdienst Rijk
Ministerie van Financiën

-

Assurancerapport
Audit monitoring PPS 2015 Kempkensberg Groningen

Colofon

Titel	Audit monitoring PPS 2015 Kempkensberg Groningen
Uitgebracht aan	B/CFD unit HFA Facilitaire Productontwikkeling
Datum	20 januari 2017
Kenmerk	2017-0000020647

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Aanleiding opdracht

Het beheer van de gebouwen aan de Kempkensberg in Groningen is georganiseerd volgens een Publiek-Private Samenwerking (PPS). Deze samenwerking betreft de Belastingdienst en de Dienst Uitvoering Onderwijs en een consortium van private partijen onder de naam DUO[2]. Het beheer dient te voldoen aan de bepalingen in de Outputspecificaties (OS). In de OS is de bepaling opgenomen dat één keer per jaar een audit wordt uitgevoerd naar de betrouwbaarheid van het monitoringssysteem op de kwaliteit van de facilitaire dienstverlening.

Deze opdracht is uitgevoerd in opdracht van de Belastingdienst/CFD Unit HFA Facilitaire Productontwikkeling (FPO)

Goedkeurend oordeel

Op grond van ons onderzoek zijn wij van oordeel dat de opzet en het bestaan per 31 december 2015 en de werking gedurende 2015 van het monitoringssysteem voor de monitoring van de PPS-afspraken voor het gebouw aan de Kempkensberg 12 in Groningen in alle van materieel zijnde opzichten hebben voldaan aan de gestelde normen.

1 Registratie KWIS-meldingen betrouwbaar

1.1 KWIS-meldingen betrouwbaar verwerkt

Uit de door de ons uitgevoerde deelwaarneming blijkt dat voor de registratie in NPQ, de juiste standaardmeldingen met de juiste classificaties zijn gebruikt (conform de OS). Bij het classificeren is rekening gehouden met ruimteafhankelijke classificaties. Meldingen afkomstig uit FMIS geven op een enkele uitzondering na voldoende informatie om de juiste classificatie toe te kennen. De meldingen zijn voor het overgrote deel binnen de toegestane hersteltijd opgelost.

Van de 1813 meldingen (in 2014: 1919) zijn er 4 (in 2014: 8,5) die tot een korting hebben geleid. De berekende kortingen zijn conform de OS.

1.2 Registratie wensen, onterechte meldingen en geannuleerde meldingen correct

Een deel van de meldingen is te classificeren als een wensmelding waarvoor geen toegestane hersteltijd geldt. Er zijn ook meldingen die niet voor DUO[2] blijken te zijn (onterechte meldingen), deze worden ook als wens geregistreerd in NPQ. Het is niet mogelijk om een melding uit NPQ te verwijderen. Overigens kunnen classificaties wel aangepast worden, ook de deadline kan aangepast worden. Deze wijzigingen vinden alleen plaats in overleg met de opdrachtgever.

Er zijn 122 meldingen geweest die als ‘wens’ zijn geregistreerd. Bij de beoordeling van de wensen is dat in 1 geval onterecht gebleken.

1.3 Periodieke testen zijn uitgevoerd

De periodieke testen zijn opgenomen in NPQ. In overleg met de opdrachtgever is in een aantal gevallen afgeweken van de uitvoering van de periodieke testen. Over de resultaten en de mogelijke gevolgen van enkele testen zijn FD en DUO[2] nog in gesprek. Het escalatiepad is hiervoor gevolgd, zoals dit is beschreven in het Monitoringsplan.

Uit de deelwaarneming blijkt dat de beschrijving in het OS niet altijd voldoende duidelijkheid geeft over de berekening van de toegestane afwijking op de norm.

We hebben begrepen dat in Q1 2017 de opdrachtgever en opdrachtnemer in gesprek zijn geweest over de nut en noodzaak van de uit te voeren periodieke testen en het ver-SMART-en van de eisen aan de uitkomsten.

In NPQ zijn de resultaten van de periodieke testen niet vastgelegd zoals in het Monitoringsplan is bepaald. De resultaten zijn wel inzichtelijk doordat de rapportages in Viadesk zijn vastgelegd.

2 Autorisaties NPQ actualiseren

2.1 Autorisaties op basis van ‘need to know’ met 1 uitzondering

De autorisaties voor het tool NPQ zijn uitgegeven op basis van het ‘need to know’-principe. Uit de autorisatiematrix blijkt dat er 1 userid 'onbekend' is. Deze autorisatie heeft leesrechten en rechten van de functioneel beheerder. Dit is een ongewenste situatie. Eventuele activiteiten met dit userid zijn niet terug te herleiden op persoonsniveau. Ook kan het een beveiligingsissue veroorzaken.

2.2 Autorisatiematrix is niet actueel

Uit de autorisatiematrix blijkt dat de autorisaties niet tijdig worden geactualiseerd. Medewerkers die geen taak meer hebben in dit verband hebben nog wel leesrechten in NPQ. Op zich heeft het mogelijke risico geringe implicaties.

Het management van DUO[2] ondertekent de autorisatiematrix niet en wordt ook niet periodiek ter beoordeling aan FD voorgelegd. Indien dit wel zou worden gedaan, is dit een ‘natuurlijk’ moment om de actualiteit van de uitgegeven autorisaties te toetsen.

2.3 Afhandeling beveiligingsmeldingen door beveiligingsfunctionaris

Net als vorig jaar is een van de medewerkers die KWIS-meldingen in NPQ kan afhandelen tevens beveiligingsfunctionaris. Het risico is dat een melding met een beveiligingsaspect onterecht gereed gemeld wordt. We hebben geen aanwijzingen dat dit zich heeft voorgedaan.

3 Haperingen in de geautomatiseerde verwerking

3.1 Niet altijd een registratie van een Toegestane hersteltijd in NPQ

In het stambestand van NPQ zijn 137 meldingen waaraan geen Toegestane Hersteltijd (THT) is toegekend, maar zijn geregistreerd als ‘nader te bepalen’. Dit is vanaf de start van het monitoren als zodanig vastgelegd.

In 2015 doet zich het fenomeen voor dat bij een aantal meldingen weliswaar een THT is vastgelegd in het stambestand, maar in de uitwerking een ‘nader te bepalen’-status is gegeven. Deze meldingen hebben we individueel onderzocht. Het blijkt dat in geen van de meldingen de vastgestelde THT uit het stambestand is overschreden. Er zijn geen financiële consequenties. DUO[2] heeft na onderzoek geconstateerd dat er sprake is van een systeemfout in NPQ.

3.2 Koppeling FMIS met NPQ hapert soms

In 2015 is geconstateerd dat in een 10-tal gevallen een hapering is voorgevallen in de doorlevering van KWIS-meldingen vanuit FMIS naar NPQ. Er is een work-around en de opdrachtgever geeft akkoord voor het verzetten voor de starttijd. De oorzaak van deze hapering ligt waarschijnlijk bij de Belastingdienst, maar is inhoudelijk niet bekend.

4 Aanbevelingen en/of vervolgstappen

Hieronder staan in korte bewoordingen de aanbevelingen voor de Opdrachtgever:

1. Maak afspraken met ON over het periodiek testen van de GBS-sensoren;
2. Verbeter de periodieke testen door de keuze voor de verschillende testen te herijken en de eisen aan de uitkomsten te concretiseren;
3. Onderzoek de mogelijkheid of het mogelijk is om vanuit NPQ dagelijks een signaal af te geven zodat de werking van de koppeling met FMIS wordt getest.

Hieronder staan in korte bewoordingen de aanbevelingen voor de Opdrachtnemer:

1. Leg de bevindingen van de periodieke testen vast in NPQ;
2. Ga in gesprek met FD hoe de bevindingen uit de periodieke testen dienen te worden vastgelegd;
3. Verwijder het userid ‘onbekend’;
4. Leg periodiek de autorisatiematrix voor aan de manager DUO[2] én aan de afdeling FD ter beoordeling;
5. Laat het gereed melden van beveiligingsissues uitvoeren door een andere functionaris dan een medewerker van beveiliging;
6. Beoordeel of het fenomeen van het niet vastleggen van een THT in NPQ, terwijl die wel in het stambestand staat, zich ook in 2016 heeft voorgedaan. Beoordeel of de THT uit het stambestand niet is overschreven.

5 Verantwoording onderzoek

5.1 Doel en Object van onderzoek

5.1.1 *Doel*

Het doel van dit assurance-onderzoek is een oordeel te vormen over de betrouwbaarheid van de opzet en bestaan per 31 december 2015 en de werking van het monitoringssysteem in 2015. Dit houdt in dat vastgesteld zal worden of de registratie, rapportage en de eventuele kortingen op de facturatie van de geleverde prestaties juist, tijdig en volledig is.

5.1.2 *Object van onderzoek*

Het object van onderzoek betreft de handmatige en geautomatiseerde procedures die tot doel hebben de kwaliteit van de dienstverlening door het consortium DUO^2 te monitoren. Voor de geautomatiseerde procedures betreft dit het FMIS (Financieel Management Informatie Systeem) bij CFD en het tool NPQ bij DUO^2.

Meer gespecificeerd betreft dit:

- De procedures van de verwerking van de meldingen die betrekking hebben op de OS;
- Het proces van de financiële afwikkeling;
- De interface tussen FMIS en NPQ;
- De interface tussen FMIS en het gebouwbeheersysteem;
- Het proces van de foutafhandeling (intrekken van foutieve meldingen);
- De stamgegevens;
- De verleende toegangsrechten (autorisaties) in FMIS en NPQ;
- Testen indien en voor zover er functionele wijzigingen zijn geweest in NPQ.

DUO^2 is de opdrachtgever voor het beheer van de NPQ door Strukton. Van de volgende onderdelen uit het normenkader zullen wij de afspraken met de leverancier en de naleving van deze afspraken door DUO^2 betrekken in de audit. Het betreft:

- logische toegangsbeveiliging;
- continuïteit;
- wijzigingsbeheer.

5.2 Normenkader

In bijlage 1 staat het normenkader. Dit normenkader is gebaseerd op het Monitoringsplan en algemene IT-beheernormen. Deze normen zijn afgestemd met de opdrachtgever.

5.3 Gehanteerde Standaard

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

5.4 Verspreidingskring rapport

De opdrachtgever, B/CFD unit HFA Facilitaire Productontwikkeling (FPO), is eigenaar van dit rapport. De opdrachtgever zal ervoor zorg dragen dat DUO^2 een exemplaar van dit rapport zal ontvangen.

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.

6 Ondertekening

Groningen, 20 januari 2017

Auditmanager
Auditdienst Rijk

Bijlage 1 Normenkader

Nr.	Norm
A	**Proces- en applicatiecontrols**
1	Rollen en autorisaties
1.1	Organisatorische functiescheidingen zoals belegd in de organisatie dienen te zijn gewaarborgd door middel van autorisaties in de applicatie.
1.2	Periodiek worden toegekende autorisaties op actualiteit (uitdiensttredingen, functiewijzigingen, geen gebruik, aangepaste rechten) gecontroleerd en bevestigd door het management.
1.3	Autorisaties dienen te zijn gebaseerd op een role-based toegangsconcept waarbij gebruikers behoren tot rollen en aan rollen autorisaties zijn toegewezen.
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.
1.5	Administrator rechten zijn beperkt toegekend.
1.6	De autorisatiematrix dient te zijn gedocumenteerd, actueel te zijn en door de eigenaar van de applicatie te zijn geautoriseerd.
1.7	Aanvragen van autorisaties c.q. aanpassen van autorisaties verloopt via een formele procedure en pas na goedkeuring worden rechten toegekend.
1.8	Mutaties in autorisaties dienen te worden gelogd zodat wijzigingen achteraf herleidbaar en controleerbaar zijn (audittrail).
1.9	Wachtwoorden dienen sterk te zijn en periodiek te worden gewijzigd (password policy).
2	Beheren meldingen
2.1	Incidenten, storingen en helpdeskverzoeken (meldingen) dienen betrouwbaar (juist, tijdig en volledig) te worden geregistreerd.
2.1	a -Het gehele systeem dient te zijn voorzien van een gesynchroniseerde standaarddatum/tijdsaanduiding gebaseerd op standaard UTC.
2.1	b - Meldingen mogen niet onvolledig kunnen worden ingevoerd.
2.1	c - Meldingen worden geclassificeerd en geprioriteerd conform de afspraken in de Outputspecificaties.
2.1	d - Meldingen zijn doorlopend genummerd.
2.1	e - Indien de koppeling tussen de afzonderlijke registratiesystemen (indien van toepassing: FMIS-NPQ) niet functioneert, is er een workaround waarbij de betrouwbare verwerking van de meldingen is getoetst.
2.2	Incidenten, storingen en helpdeskverzoeken (meldingen) dienen op een betrouwbare wijze en conform de opgestelde procesgang en workflow te worden afgehandeld.
2.2	a - Gegevens die van invloed zijn op de "afrekening" mogen niet tussentijds gecorrigeerd kunnen worden.
2.2	b - Wijzigingen in gegevens die mogelijk van invloed zijn op de "Afrekening" (bijv. on hold, niet ontvankelijk of facilitair) dienen achteraf inzichtelijk te zijn.
2.2	c - Meldingen kunnen niet worden verwijderd.
2.2	d - meldingen worden bewaakt op tijdige afhandeling.
2.3	De betrouwbaarheid (juist-, tijdig- en volledigheid) van het gereedmeldingstijdstip dient te zijn gewaarborgd.
2.3	a - melding dient op juiste tijdstip te worden gereed gemeld (systeem tijd).
2.3	b - oplossing van de melding dient te worden gedocumenteerd.
2.3	c - indien de koppeling tussen de afzonderlijke registratiesystemen (indien van toepassing:FMIS-NPQ) niet functioneert dient in de workaround getoetst te worden dat het gereedmeldingstijdstip juist is en de afmelding naar de melder te zijn opgenomen.
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.

Nr.	Norm
3	Interfaces met andere systemen
3.1	koppeling GBS: Via het gebouwregistratiesysteem worden meldingen ontvangen. De betrouwbare (juiste, tijdige en volledige) registratie van deze berichten in het NPQ/FMIS dient te zijn gewaarborgd.
3.1	a - Koppeling GBS: De inleesfunctie dient (na uitval of crash) herstartbaar te zijn zonder fouten (geen verstoring betrouwbaarheid). Fouten bij het inlezen worden herkend en opgelost.
3.1	b - De inregeling van het GBS wordt intern getoetst.
3.1	c - Koppeling GBS: Handmatig corrigeren c.q. invoeren van een GBS melding is alleen mogelijk voor daartoe geautoriseerde medewerkers en de handmatige vastlegging is als zodanig herkenbaar.
3.1	d - Koppeling GBS: Systeemklokken GBS en NPQ dienen te zijn gesynchroniseerd.
3.1	e - Koppeling GBS: De gegevens vanuit het GBS moeten de informatie leveren die een juiste classificatie mogelijk maakt.
3.2	koppeling GBS: Via het gebouwregistratiesysteem worden meldingen ontvangen. De betrouwbare (juiste, tijdige en volledige) verwerking van deze berichten in het NPQ dient te zijn gewaarborgd.
3.3	koppeling GBS: Via het GBS worden meldingen ontvangen. De betrouwbare (juiste, tijdige en volledige) afmelding van deze berichten in het NPQ dient te zijn gewaarborgd.
3.4	Koppeling GBS: De betrouwbaarheid van de koppeling tussen het GBS en het FMIS dient achteraf controleerbaar te zijn.
3.5	Koppeling intranet: Gebruikers voeren meldingen via het intranet portal. De betrouwbare (juiste, tijdige en volledige) verwerking van de meldingen in het FMIS dient te zijn gewaarborgd.
3.6	Inkomende e-mail: Gebruikers sturen e-mail berichten en de betrouwbare (jusite, tijdige en volledige) registratie van deze berichten in het FMIS dient te zijn gewaarborgd.
3.7	Uitgaande e-mail: Na registratie van de melding ontvangt de(gebruiker(melding) een emailbericht met bevestiging. De betrouwbaarheid (juistheid, tijdigheid en volledigheid) van deze email berichten dienst te zijn gewaarborgd.
4	Rekenregels
4.1	De relatie tussen de outputspecificatie en de kortingsberekeningregels moet eenduidig zijn vast te stellen.
4.2	Betrouwbaarheid van kortingsberekeningsregels voor alle Outputspecificaties dient te zijn gewaarborgd.
4.3	Betrouwbaarheid van het geautomatiseerde kortingsberekeningsmechanisme moet zijn gewaarborgd.
5	Onderhoud en beheer
5.1	Er is een actuele en door het management goedgekeurde procedure vastgelegd voor het wijzigen van Stamgegevens c.q. gegevens die van invloed zijn op de te berekenen kortingen.
5.2	De procedure voor wijzigen van stamgegevens is in overeenstemming c.q. sluit aan op contractuele afspraken met de belastingdienst.
5.3	Alleen geautoriseerde medewerkers kunnen wijzigingen in stamgegevens en rekenregels doorvoeren.
5.4	Mutaties op stamgegevens die direct of indirect van invloed kunnen zijn op de betrouwbaarheid van de kortingsberekening (o.a. meldingscategorie, kortingen en toegestane hersteltijden) dienen te worden gelogd zodat wijzigingen achteraf herleidbaar en controleerbaar zijn (audittrail).
5.5	Betrouwbaarheid van de ruimteclassificatie dient te zijn gewaarborgd.
5.6	Betrouwbaarheid van de normwaarde signalering dient te zijn gewaarborgd.
5.7	Betrouwbaarheid van de in het FMIS vastgelegde meldingen en classificatie dient te zijn gewaarborgd.
B	**IT General Controls**
6	Logische toegangsbeveiliging
6.1	Remote access (NPQ en Axxerion) is beveiligd door middel van user-ids en wachtwoorden (eventueel ook op basis van tokens).
6.2	Remote datacommunicatie (technische verbinding tussen gebruikersapplicatie (NPQ) en server) is beveiligd (VPN, HTTPS).
7	Continuïteit

Nr.	Norm
7.1	Continuïteitsmaatregelen (back-up, recovery, uitwijk etc.) zijn in overeenstemming met de contractueel overeengekomen beschikbaarheideisen.
7.2	De continuïteitsmaatregelen worden periodiek getest. Op basis hiervan wordt het plan geëvalueerd en indien nodig verbeteringen getroffen.
7.3	Er is een actueel, gedocumenteerd en door het management geaccordeerd plan voor continuering van de dienstverlening en handhaving van het service niveau.
8	Wijzigingsbeheer
8	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.
8.1	Er is een wijzigingsprotocol.
8.2	Wijzigingsverzoeken en de afhandeling daarvan is gedocumenteerd en voor ieder wijzigingsverzoek is (achteraf) een audittrail beschikbaar.
8.3	Wijzigen dienen voor in gebruik name te worden getest.
8.4	Gebruikers dienen in de test te worden betrokken.
8.5	Testscenario's worden gehanteerd en testbevindingen worden gedocumenteerd.
8.6	Wijzigingen dienen alleen met toestemming van de interne eigenaar van de applicatie te worden geïmplementeerd in de productieomgeving.
8.7	Gebruikers worden geïnformeerd over aard van de wijziging en het moment van implementatie.
8.8	Na de implementatie van wijzigingen vindt aanvullende monitoring plaats op het correct werken van de applicatie.
9	Uitbestede werkzaamheden (indien van toepassing)
9.1	Indien aan de applicatie gerelateerde systeembeheer en/of applicatie ontwikkelingswerkzaamheden zijn uitbesteed dan dienen daaraan contractuele afspraken ten grondslag te liggen (Service Level Agreements).
9.2	In de contractuele afspraken dient minimaal het dienstenniveau te zijn gedefinieerd.
9.3	De dienstverlener dient periodiek te rapporteren over het behaalde diensten niveau.
9.4	Rapportages over het behaalde dienstenniveau dienen te worden besproken tussen de partijen en indien van toepassing dienen verbeteracties te worden geïnitieerd.

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