Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport
FMIS-systeem een facilitair systeem dat leidt tot facturatie

Definitief 1.0

Colofon

Titel	FMIS-systeem een facilitair systeem dat leidt tot facturatie
Uitgebracht aan	Directeur Generaal RIVM
Datum	19 november 2021
Kenmerk	2021-0000236579
Referentienummer	2021-VWS-009

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Managementsamenvatting

De nieuwe huisvesting van het Rijksinstituut voor Volksgezondheid en Milieu (RIVM) en het College ter Beoordeling van Geneesmiddelen (CBG) in het Utrecht Science Park is via Publiek Private Samenwerking (PPS) aanbesteed. FMIS-systeem is het facilitair registratiesysteem voor onder andere het registreren en afhandelen van meldingen en verstoringen, werkorders en het reserveren van zalen en lunches. Afhankelijk van de soort registraties en oplostijden kunnen de registraties financiële consequenties (zoals kortingen) hebben.

Wij hebben tijdens ons onderzoek duidelijke documentatie aangetroffen en een aantal demonstraties gezien van het FMIS-systeem. Ook hebben wij aan de hand van demonstraties en testresultaten gezien dat kortingen juist worden berekend. Uit het Monitoringsplan blijkt dat alle datawijzigingen zullen worden gelogd, zodat ook achteraf inzichtelijk is wie welke wijzigingen heeft uitgevoerd.

Wij hebben ook een aantal verbeterpunten geconstateerd.

Wij constateren dat veel, maar nog niet alle scenario's zijn getest:

- Het FMIS- systeem kent diverse koppelingen met andere systemen. Zo is er voor bijvoorbeeld meldingen vanuit het gebouw een koppeling met het Gebouwbeheersysteem. Er is ook een koppeling met de personeelssysteem van het RIVM om de gebruikerslijsten te onderhouden. De berichten van de koppelingen zijn navolgbaar getest. Een uitzondering is echter de koppeling met het personeelssysteem van het CBG. De koppeling tussen het personeelssysteem van het CBG en het FMIS-systeem was ten tijde van de audit nog niet aanwezig en niet getest.

- Kortingen zijn aantoonbaar getest behoudens herhaalkortingen met betrekking tot 'Veiligheid & Gezondheid' en 'Regelgeving'. Doordat een testscenario hiervoor ontbreekt, kan het gebeuren dat eventuele fouten in nieuwe versies niet worden opgemerkt.

- De Outputspecificaties zijn belangrijk omdat dat de definities zijn voor de dienstverlening inclusief de hoogte van de diverse soorten kortingen. De Outputspecificaties zijn geaccordeerd in een bronbestand. Dit bronbestand is ingelezen in het FMIS-systeem. Het is niet navolgbaar getest dat alle Outputspecificaties juist en volledig zijn overgekomen in het FMIS-systeem. Hierdoor kan het gebeuren dat kortingen onjuist worden berekend.

- Berekeningen van de kosten van variabele diensten en eventuele kortingen worden in drietal maandelijkse rapportages opgenomen. Deze rapportages dienen als onderdeel van de factuur. Wij hebben geen testresultaten aangetroffen aangaande maandelijkse rapportages met daarin kortingsbedragen en kosten van variabele diensten. Wanneer de rapportages niet juist zijn, zal dit consequenties hebben voor de juistheid van het factuurbedrag.

Wij constateren dat de documentatie op onderdelen verbeterd kan worden, voorbeelden zijn:

- In de documentatie is een overzicht van rollen en autorisaties opgenomen, echter deze documentatie sluit niet aan op de (voorgenomen) inrichting van het FMIS-systeem en op andere passages in de documentatie. Hierdoor is in de opzet van de rollen en autorisaties niet altijd duidelijk wie wat zou mogen.

- Voor logische toegangsbeveiliging wordt geen twee-factor authenticatie gebruikt in situaties waarin dit volgens de BIO-normering wel wordt voorgeschreven. We hebben niet aangetroffen waarom dat niet gebeurt en welke eventuele compenserende maatregelen getroffen zijn.

- Continuïteitsafspraken en bijbehorende kortingen zijn niet voldoende gespecificeerd. In de documentatie wordt gesproken als eis 7*24 uur maar een onderhoudswindow is niet beschreven. Deze zal er in de praktijk wel zijn.

- Wijzigingenbeheer voor het FMIS-systeem kan verbeterd worden. Belangrijk is dat wijzigingen gedocumenteerd worden en dat achteraf ook duidelijk is dat de betreffende partijen akkoord zijn met de doorgevoerde wijziging. Dit kan zowel een functionele wijziging als een wijziging in de tarieven van variabele diensten betreffen. Om zekerheid te verkrijgen over de juistheid van een doorgevoerde wijziging is het belangrijk dat de indiener van een wijziging betrokken is bij de goedkeuring van de wijziging. In de procesbeschrijving is de betrokkenheid van de indiener niet opgenomen.

Tijdens bespreking van de bevindingen is aangegeven dat op dit moment een acceptatie heeft plaatsgevonden van het FMIS-systeem en dat wijzigingen inmiddels volgens het wijzigingsproces worden uitgevoerd. Echter door de afwezigheid van de bewoners van het pand zullen de processen, die ondersteund worden door het FMIS-systeem, zoals de **k**lacht, **w**ens, **i**nformatieverzoeken of **s**toringen (KWIS-meldingen), reserveringen, catering en gebruikersmeldingen nog niet plaatsvinden. Derhalve is geen onderzoek uitgevoerd naar het bestaan.

1 Inleiding

De nieuwe huisvesting van het Rijksinstituut voor Volksgezondheid en Milieu (RIVM) en het College ter Beoordeling van Geneesmiddelen (CBG) in het Utrecht Science Park is via Publiek Private Samenwerking (PPS) aanbesteed. In deze PPS is de opdrachtgever het Rijksvastgoedbedrijf (RVB). MEET RIVM CBG B.V. (verder MEET) is als opdrachtnemer verantwoordelijk voor het ontwerp, de bouw, de financiering, het onderhoud en een groot deel van de facilitaire dienstverlening. De PPS-opdracht heeft een looptijd van 25 jaar. Ten behoeve van de oplevering, is een Voltooiingscertificaat nodig. Eén van de voorwaarden voor het verkrijgen van het Voltooiingscertificaat is dat MEET heeft aangetoond dat het FMIS-systeem werkt en leidt tot een rechtmatige facturatie. Het FMIS-systeem is het facilitair registratiesysteem voor onder andere het vastleggen en afhandelen van meldingen en het reserveren van zalen en lunches.

1.1 Aanleiding onderzoek en opdrachtgever

De directeur RIVM heeft de ADR verzocht een eerste onderzoek te doen naar het FMIS-systeem. Op dit moment is het FMIS-systeem klaar voor gebruik maar nog niet in gebruik. Het onderzoek zal gebruikt worden om mogelijk de laatste verbeteringen in FMIS-systeem aan te brengen zodat men op termijn voor het onderzoek in het kader van het voltooiingscertificaat goed is voorbereid. Op dit moment is de kennis van de ontwikkeling van FMIS-systeem nog aanwezig, deze situatie kan op het moment, waarop het voltooiingscertificaat actueel wordt, gewijzigd zijn. Eventuele benodigde wijzigingen lijken daarom nu eenvoudiger door te voeren dan te zijner tijd. Het ADR-onderzoek had niet tot doel tot een oordeel te komen over het FMIS-systeem.

1.2 Doelstelling

Doelstelling van dit onderzoek is te onderzoeken welke maatregelen in opzet zijn voorzien in de systeemprogrammatuur (modules), de systeeminrichting, de content zoals stamgegevens, rekenregels en Outputspecificaties (kortingen, categorieën) en de bijbehorende processen om tot een rechtmatige factuur te komen.
Er is geen onderzoek uitgevoerd naar het bestaan, omdat op dit moment het gebouw en daarmee samenhangende voorzieningen en rapportage t.b.v. facturatie nog niet in gebruik zijn. Op een later moment zal een onderzoek plaatsvinden naar het bestaan.

1.3 Afbakening

Het object van onderzoek bestaat uit de opzet van de processen en de componenten (modules) van het Registratiesysteem (FMIS-systeem) inclusief de daarbij aanwezige koppelingen, welke van invloed zullen zijn op het maandelijkse rapportage welke onderdeel zal zijn van de factuur.

De volgende modules van FMIS-systeem zijn in beschouwing genomen:

- Meldingen,
- Betalingsmechanisme (onderdeel van module Meldingen),
- Werkorders (onderdeel Periodieke Metingen),
- Reserveringen (onderdeel Aanvragen Catering),
- Bestellingen (t.b.v. Standaard Variabele Diensten en Bijzondere Dienstverlening).

Koppelingen (interfaces) zijn tijdens het onderzoek onderzocht op de aanwezigheid, bijvoorbeeld doordat dit is aangetoond middels testberichten. Tijdens dit onderzoek is niet gekeken naar de maatregelen voor de betrouwbaarheid van het berichtenverkeer. Het betreft de volgende koppelingen van het FMIS-systeem met:

- het Gebouw Beheer Systeem (GBS),
- het HR RIVM (personeelsgegevens)[1],
- het Inventaris Registratie- en Alarmeringssysteem (IRAS).

Overige onderdelen die in beschouwing zijn genomen:

- rapportages ten behoeve van de facturatie zoals Kortingsrapportage en Standaard Variabele Dienstenoverzicht,
- processen die als randvoorwaarden gelden voor rechtmatige facturatie zoals beheer stamgegevens (Outputspecificaties), beheer accounts, logging en noodscenario (continuïteit).

1.4 Leeswijzer

In het volgende hoofdstuk vindt u een overzicht van de bevindingen die het ADR-onderzoeksteam heeft. In dit hoofdstuk wordt per paragraaf kort aangegeven wat we hebben aangetroffen en indien van toepassing zijn daarbij bevindingen en aanbevelingen opgenomen.

In hoofdstuk 3 vindt u informatie over de wijze waarop het onderzoek is uitgevoerd.

[1] CBG heeft een ander personeelssysteem op dit moment is de koppeling nog niet aanwezig. Deze koppeling wordt als wijziging gezien op het contract.

2 Bevindingen

Wij hebben tijdens ons onderzoek bruikbare documentatie aangetroffen, zelfstandig inzage gehad in het systeem door persoonlijke inloggegevens met beperkte rechten en een aantal demonstraties meegemaakt van het FMIS-systeem. In dit hoofdstuk wordt per paragraaf kort aangegeven wat we hebben aangetroffen en indien van toepassing zijn daarbij bevindingen en aanbevelingen opgenomen.

2.1 Het overzicht van rollen en autorisaties sluit niet aan op het FMIS-systeem

We hebben diverse onderdelen in de documentatie aangetroffen voor het autorisatiebeheer. Het betreft de volgende onderdelen

- een autorisatiematrix waarin per gebruikersgroep de autorisaties (‘nieuw toevoegen’, ‘wijzigen’, ‘kijken’ of ‘niet beschikbaar’) per functie binnen het FMIS-systeem wordt weergegeven,
- een procesbeschrijving voor “Aanvragen of wijziging accounts”,
- een procesbeschrijving “Bewaking”. Hierin is aangegeven dat twee maal per jaar de gebruikersgroepen worden gecontroleerd,
- Logging: Wijzigingen in autorisaties worden gelogd, hierdoor zijn autorisatiewijzigingen achteraf detecteerbaar.

Na bestudering van de documentatie hebben we de volgende bevindingen:

- In de autorisatiematrix is te zien dat de gebruikersrollen beperkt zijn tot wat de betreffende gebruikersgroepen nodig zouden moeten hebben, gelet op de naamgeving van de rol;
- In het FMIS-systeem blijken meer functies aanwezig te zijn dan in de autorisatiematrix zijn opgenomen. Voorbeelden zijn: ‘Aanmaken account (gebruiker)*’ en ‘Aanleveren inloggegevens* ‘ en ‘Raadplegen rapportages*’. In een gesprek is door MEET toegelicht dat ‘Toegang tot de logging*’ niet als aparte functie beschouwd, maar is onderdeel van de functie ‘Raadplegen rapportages* ’;
- Uit de documentatie blijkt dat er autorisaties zijn voor “Masterdata” en “Beheer”, deze activiteiten zijn niet terug te vinden in de autorisatiematrix.
- Uit de documentatie blijkt dat ‘SUPER USER’ en ‘Applicatiebeheerder’ bepaalde functionaliteiten hebben in het systeem anders dan Functioneel Beheerder. Echter de gebruikersgroepen waartoe ‘SUPER USER’ en ‘Applicatiebeheerder’ behoren, zijn niet als zodanig herkenbaar in de autorisatiematrix.
- Tijdens de demo is door MEET aangegeven dat de logging van het systeem niet te wijzigen is. Het toegangsbeheer tot de database was geen onderdeel van onze werkzaamheden. Het beheer van de database wordt uitgevoerd door de hostingpartij. De database is voor MEET niet direct toegankelijk.

*fictieve naamgeving, wordt alleen gebruikt in dit rapport door de ADR

Gelet op de voormelde bevindingen is het risico dat de documentatie niet geheel aansluit op de mogelijke inrichting van het systeem. Hierdoor kan er onduidelijkheid ontstaan of kunnen rechten (onbewust) onjuist worden toebedeeld. De logging van de mutaties is een goede beheersmaatregel. Belangrijk daarbij is dat er voldoende zekerheid is over de integriteit van de logging, met andere woorden dat deze logging niet aangepast kan worden.

Wij bevelen aan om

- *de autorisatiematrix uit te breiden met*
  - *de gebruikersgroep(en) die nog niet gespecificeerd is (zijn) en*
  - *functies die wel in de applicatie of het monitoringsplan zijn opgenomen maar nog niet herkenbaar zijn in de aangetroffen matrix.*
- *zekerheid te verkrijgen aangaande het beheer en toegangsmogelijkheden door de hostingpartij van de onderliggende database.*

Voor de controle van gebruikersrechten valt het op dat een belangrijke rol is weggelegd voor de SUPER USER. Bij het onderdeel 'Aanleveren lijst gebruikers uit het FMIS-systeem' wordt door de SUPER USER uitgevoerd terwijl de SUPER USER zelf de autorisaties uitreikt en intrekt in het procesonderdelen 'Aanmaken account en aanleveren inloggegevens' en 'verwijderen account en dit bevestigen'.

Het risico is dat SUPER USER 'spook' gebruikers kan uitgeven, waardoor er mogelijk accounts voor fictieve personen kunnen worden aangemaakt. Hierdoor kan functiescheiding worden doorbroken.

Wij bevelen aan om

- *de activiteit 'aanleveren lijst gebruikers' te combineren met de rapportage van de logging van mutaties van de autorisaties door Exploitatie team Rijk*
- *eventuele tijdelijke 'spook' gebruikers uit te sluiten door de logging van mutaties van autorisaties te raadplegen. Deze activiteit zou dan idealiter belegd moeten worden bij een gebruikersgroep die niet de autorisaties uitreikt.*
- *bijzondere autorisaties (zoals rollen van SUPER USER, Functioneel beheer) ieder kwartaal in plaats van twee maal per jaar te controleren. De BIO-normering schrijft voor om 'speciale toegangsrechten' ieder kwartaal te controleren.*

2.2 Nog niet alle (onderdelen van) interfaces zijn navolgbaar getest

Het beheer van het gebouw is mede afhankelijk van de gegevens uit het Gebouwbeheersysteem (GBS) en het Inventarisatie Registratie Alarmering Systeem (IRAS). De mogelijkheid voor de pandbewoners om KWIS-meldingen in het FMIS-systeem te doen en/of een verzoek te doen voor specifieke dienstverlening is afhankelijk van het betrouwbaar functioneren van de interface met het personeelssysteem van het RIVM en CBG. Het functioneren van die interfaces is een combinatie van techniek, afspraken en procedures.
In de demonstratie op 2 juli 2021 hebben we kunnen constateren dat er een 'polling' is, waarmee dagelijks wordt getest of de interface tussen het GBS en het IRAS functioneert. In het Monitoringsplan (incl. de bijlagen) is het proces van de verwerking van de GBS- en IRAS-meldingen beschreven. Dit betreft zowel de verwerking in het FMIS-systeem en de meldingen naar de monteur (indien van toepassing) voor het verhelpen van een probleem. Ook de afmelding van deze meldingen is beschreven in een procedure. Deze procesbeschrijvingen geven in opzet een goed beeld bij de uit te voeren werkzaamheden en door wie. Het op 'niet-ontvankelijk' of terugzetten van een melding is beperkt tot de rollen 'ISP-functionaris' en 'Facility-manager'. Deze handelingen worden gelogd, zodat het achteraf inzichtelijk is.

De interfaces met het Gebouwbeheersysteem (GBS), Inventarisatie Registratie Alarmering Systeem (IRAS) en het personeelssysteem van het RIVM zijn getest. Naar aanleiding van de testen zijn nog aanpassingen aangebracht in de onderliggende techniek van de interface tussen het FMIS-systeem en IRAS. De aanpassingen zijn getest en akkoord bevonden. Het testen is een iteratief proces geweest, waarbij de aanpassingen zijn getest in het geheel van de functionaliteit. Bij de testen van de interface van het FMIS-systeem met het personeelssysteem is een medewerker van het RIVM betrokken geweest. Deze test omvatte niet alleen de interface, maar betrof ook het koppelen van een RIVM-medewerker aan het juiste autorisatieprofiel in FMIS-systeem. Er zijn ten tijde van ons onderzoek geen openstaande issues of casuïstiek die op een oplossing of besluit wachten.

Zowel het GBS als het IRAS kennen zogenoemde voormeldingen. Dit zijn meldingen die een signaal zijn voordat een bepaalde waarde wordt overschreden. Deze voormeldingen zullen ook in het FMIS-systeem worden geregistreerd. In de procesbeschrijving in de bijlage bij het Monitoringplan zijn deze voormeldingen echter niet opgenomen.

We bevelen aan om de voormeldingen op te nemen in de procesbeschrijving.

De interface met het personeelsbestand van het CBG kon ten tijde van ons onderzoek niet getest worden, omdat de interface nog niet operationeel was.

We bevelen aan om de interface met het personeelsbestand van het CBG ruim voor de oplevering van het FMIS-systeem technisch gereed en getest te hebben.

De monteurs werken met mobiele devices om de meldingen af te handelen. De interface van het FMIS-systeem met de te gebruiken mobiele devices is niet getest.

We bevelen aan om de interface met de mobiele devices te testen en een vastlegging daarvan te maken.

2.3 KWIS-meldingen en werkorders zijn getest en zijn herkenbaar in de documentatie

Een melding in FMIS-systeem betreft een klacht, wens, informatie verzoek of storing (KWIS). Alle gebruikersgroepen kunnen meldingen invoeren, maar het wijzigen van de melding, zoals classificeren, afmelden is voor behouden aan exploitatiemanager / Facilitair coördinator, ISP en functioneel beheer.

Werkorders worden gegenereerd na meldingen, reserveringen en bestellingen maar kunnen ook door ISP handmatig ingebracht worden (afspraken, planningen etc.).

Afhankelijk van de soort werkorders en meldingen, zijn ze wel of niet kortingsgevoelig. Die wel kortingsgevoelig zijn, hebben een link met de Outputspecificaties. Aan de hand van de demo van 5 juli en testverslagen zien wij dat de meldingen en werkorders in FMIS-systeem worden verwerkt conform de beschrijving in het monitoringsplan en de afspraken uit de Outputspecificaties.

De betrouwbare verwerking van de meldingen en werkorders wordt mede geborgd door doorlopende nummering (REQ-nummers voor meldingen en WRK-nummers voor werkorders) en een transparante registratie van alle mutaties op een melding c.q. werkorder. Dit geldt ook voor de gereed melding.

2.4 Kortingen zijn aantoonbaar getest behoudens kortingen met betrekking tot 'Veiligheid & Gezondheid' en 'Regelgeving'

Om tot kwalitatieve dienstverlening te komen waarin iedereen zijn rol heeft, is er een kortingen systeem aanwezig. Eenvoudig gezegd komt het erop neer dat wanner de dienstverlening niet voldoet aan de verwachtingen of afspraken een korting wordt berekend. Deze korting heeft zijn weerslag op de rapportage die verwerkt wordt op de maandelijkse factuur, die door MEET wordt opgesteld.

Er zijn verschillende soorten korting:

- Beschikbaarheidskorting (Kb) Is van toepassing als een *ruimte* niet voldoet aan de gestelde eisen;
- Prestatiekorting (Kp) Is van toepassing als een *dienst* niet aan de gestelde eisen voldoet;
- Herhalingskorting (Kh) Als er sprake is van meer dan in de Outputspecificaties opgegeven maximale toegestane soortgelijke gebreken per betaalperiode op een ruimte, dienst of voorziening. Er wordt per extra melding een Korting in rekening gebracht;
- Korting Periodieke Meting (Kq) of incidentele meting.

In het bijlagen document bij het Monitoringsplan is beschreven: "Voor Meldingen met betrekking tot 'Veiligheid & Gezondheid' en 'Regelgeving' hebben de dienst en ruimte waarop dit is gemeld geen invloed op de bepaling van de herhaling. Meer dan 4 Meldingen op deze categorieën in een Betaalperiode, ongeacht de ruimte of dienst waarop de melding betrekking heeft, betekent dat een Herhalingskorting van toepassing is."
Tijdens ons onderzoek is gebleken dat voor deze korting geen testscenario was opgenomen. Er zijn wel aanvullende screenshots ter beschikking gesteld, die de toepassing van deze korting weergeven. Wanneer er geen testscenario is, kan het gebeuren dat er bij nieuwe releases onopgemerkt de betreffende korting foutief wordt berekend.

Wij bevelen aan een toepassing van deze korting op te nemen in het testscenario zodat deze korting ook in de toekomst bij nieuwe releases getest wordt.

Meldingen waarvan de Werkelijke Hertsteltijd (WHT) langer is dan de 'Toegestane Hersteltijd' (THT) leiden in principe tot een korting tenzij via een standaardprocedure aan de opdrachtgever wordt gevraagd om verlenging van de THT. Voor de berekening van de hoogte van de kortingen wordt gebruik gemaakt van de afspraken in de Outputspecificaties (zie verderop).

In ons onderzoek hebben we tijdens de demo gezien dat de kortingsmodule in het FMIS-systeem de verschillende soorten korting berekent en dat deze zichtbaar zijn op het tabblad korting bij de betreffende melding. Ook de opbouw van de korting is bij de melding inzichtelijk. Tijdens de demo's hebben we gezien dat herhalingskortingen worden geregistreerd en deze worden gebaseerd op uitgevoerde meldingen.

Behoudens de eerder genoemde korting aangaande "Voor Meldingen met betrekking tot 'Veiligheid & Gezondheid' en 'Regelgeving' " dekken de testscenario's de verschillende type KWIS-meldingen af. Het betalingsmechanisme met de prestatie-, beschikbaarheids- en herhalingskortingen is getest. Er zijn geen openstaande issues of casuïstiek die op een oplossing of besluit wachten.

In het monitoringsplan is beschreven dat het totaal aan kortingen te vinden is in rapportages welke periodiek in het tactisch overleg worden besproken. Ook is aangegeven dat de geëffectueerde kortingen per maand op de factuur 'netto beschikbaarheidsvergoeding' worden verrekend.

2.5 Bestellingen ten behoeve van Standaard Variabele Diensten en Bijzondere Dienstverlening

Iedere gebruiker kan een bestelling plaatsen of een reservering maken zolang er geen extra kosten aan zijn verbonden. Reserveringen en bestellingen waarvoor kosten extra in rekening worden gebracht, zijn voorbehouden aan geautoriseerde medewerkers. Deze aanvraaggemachtigden zijn opgenomen in de autorisatiematrix. De actualiteit van deze matrix is dus essentieel, en een verantwoordelijkheid van Opdrachtgever (lees: RIVM & CBG).

Standaard Variabele Dienst: Deze dienst zal door MEET worden geleverd op basis van een verzoek door Aanvraaggemachtigde en waar een vaste prijs per eenheid voor is afgesproken.
Tijdens de demonstratie is toegelicht dat de prijzen zijn vastgesteld en dat deze geïndexeerd worden. Het prijsrisico ligt bij MEET. Het is ons niet duidelijk geworden op welke wijze (door wie, wanneer en hoe) de (geïndexeerde) prijzen in FMIS-systeem worden onderhouden.

Het doorvoeren van geïndexeerde prijzen niet beschreven is, hierdoor is er een risico dat er onduidelijkheid kan ontstaan wanneer een dergelijke wijziging zich aandient. Het is van belang dat vooraf is afgesproken welk vastleggingen benodigd zijn, zodat achteraf aangetoond kan worden dat dergelijke prijswijzigingen conform afspraken zijn doorgevoerd.

Wij bevelen aan om te beschrijven welke proces of hoe het FMIS-systeem voorziet in het onderhoud op prijzen van standaard variabele diensten en de indexatie daarvan.

In de procesbeschrijving is aangegeven dat de aanvraaggemachtigde een annulering kan doorgeven aan het integraal servicepunt (ISP). Het ISP zal deze annulering moeten registreren. Het is niet bekend welke datum / tijdstip door de ISP gehanteerd wordt bij het registreren van de annulering. Er staat ook dat eventuele annuleringskosten in FMIS-systeem worden vastgelegd. Het is voor ons niet duidelijk geworden wat en hoe hoog deze kosten zijn.

Wanneer bovenstaande niet duidelijk beschreven is, bestaat het risico dat bij het optreden van dergelijke situatie een discussie ontstaat en ad hoc besluiten moeten worden genomen.

We bevelen aan een testscenario op te stellen en uit te voeren en de resultaten vast te leggen van het proces van aanvragen tot en met de rapportage t.b.v. de facturatie van variabele diensten waarin

- *diverse soorten variabele diensten (w.o. catering) inzichtelijk zijn;*
- *een voorbeeld is opgenomen betreffende een annulering meer dan 24 uur van te voren is doorgegeven door de aanvraaggemachtigde aan de ISP, waardoor de catering kosten niet worden gefactureerd;*
- *een voorbeeld is opgenomen van annuleringskosten die in rekeningen worden gebracht en een toelichting waarin staat hoe deze zijn samengesteld.*

Er wordt verwezen naar: "De reservering- en annuleringsvoorwaarden catering zijn opgenomen in de PDC." De PDC verwijst weer naar het uitvoeringsplan producten en diensten (UPD). In dit plan wordt weer verwezen naar de banquetingmap met daarin de voorwaarden en tarieven van de cateraar. De banquetingmap was ten tijde van het onderzoek nog niet vastgesteld.

Doordat afspraken in verschillende documenten zijn opgenomen, bestaat het risico dat het onduidelijk is welke afspraken gemaakt zijn. Het is het van belang duidelijkheid te scheppen welke afspraken in welke documenten staan.

Wij bevelen aan een overzicht van afspraken en documentatie te maken waarin de afspraken zijn terug te vinden. Hierbij zal voorkomen moeten worden dat een afspraak in meerdere documenten staat beschreven of dat afspraken in geen document is opgenomen. Zorg daarbij dat het overzicht bij wijzigingen in de documentatie actueel blijft.

In het monitoringsplan (p.23) is het volgende aangegeven:

> Voor het aanvragen van Standaard Variabele Diensten (zoals catering) is de juiste autorisatie benodigd. Het Exploitatieteam Rijk kan bij MEET aangeven wie welke autorisatie heeft. In het FMIS is de autorisatie ingeregeld zodat alleen Aanvraaggemachtigden deze boekingen/ bestellingen kunnen registreren. In bijlage 12 is een overzicht opgenomen van de Standaard Variabele Diensten zoals zijn vastgelegd in de DBFMO overeenkomst, inclusief een indeling naar het soort dienst.

Het ontvangen Bijlagendocument Monitoringsplan V2.0 gaat tot en met bijlage 11, bijlage 12 is niet opgenomen. Wanneer de verwijzing niet correct is, is het risico dat op termijn het overzicht met Standaard Variabele Diensten onvindbaar is.

Wij bevelen aan om de verwijzing in tekst aan te passen en te laten verwijzen naar de juiste plaats in het juiste document.

In het bijlagendocument (p.27) staat "Een aantal diensten wordt op basis van verbruik (zoals afval en gassen) verrekend. Deze zijn dan ook niet toe te wijzen aan een aanvrager." In een toelichting gaf RIVM aan dat zij over afval en het gebruik van gassen separate milieurapportages moeten gaan maken. De kans dat hier onbedoeld hogere aantallen worden verrekend is klein, dit zal direct opvallen.

Het proces bijzondere dienstverlening betreft het proces van uitbrengen offerte t/m facturatie ten behoeve van extra dienstverlening. Aangegeven is dat "Dit proces valt onder de Dienst 'Managementafspraken' met de daarin opgenomen reactietijden." Wij hebben deze managementafspraken met daarin de reactietijden niet aangetroffen. Wanneer de verwijzing niet correct is, is het risico dat deze afspraken niet nageleefd worden en dit mogelijk tot discussie kan leiden.

Wij bevelen aan de managementafspraken in (een bijlage van) het monitoringsplan op te nemen of een concrete verwijzing naar het document waarin deze terug te vinden zijn.

2.6 Ingelezen Outputspecificaties niet volledig getest

De Outputspecificaties worden onder andere gebruikt voor het berekenen van kortingsbedragen. De Outputspecificaties zijn ingelezen in het FMIS-systeem. Tijdens ons onderzoek hebben wij geen documentatie aangetroffen waarin staat hoe het inleesproces is verlopen en hoe is getoetst dat de ingelezen Outputspecificaties juist en volledig zijn ingelezen in het FMIS-systeem. Wel hebben we een aantal testscenario's gezien waardoor af te leiden is dat de betreffende gegevens in de betreffende test scenario's juist zijn ingevoerd, maar dat is slechts een kleine hoeveelheid gegevens van de totale Outputspecificaties. Het is niet integraal getest dat de Outputspecificaties volledig en juist zijn overgenomen in het FMIS-systeem. Het risico is dat er voor eventuele kortingen met onjuiste bedragen gerekend wordt. In een nadere toelichting is aangegeven dat er inmiddels veel wijzigingen in de Outputspecificaties zijn aangebracht.

Wij bevelen aan om een integrale test te doen op de juistheid van de aanwezige Outputspecificaties in het FMIS-systeem rekening houdend met de reeds doorgevoerde wijzigingen en vastleggingen daarvan.

Onderhoud Outputspecificaties
Wij hebben geen eenduidige beschrijvingen aangetroffen aangaande het onderhoud van de Outputspecificaties. In het monitoringsplan (pag. 28) staat dat de opdrachtgever Relatics gebruikt voor het vastleggen van de Outputspecificaties. Ook staat dat de opdrachtgever *in FMIS-systeem* de wijziging voor Outputspecificaties

> Relatics wordt door de Opdrachtgever gebruikt voor het vastleggen van de Outputspecificatie in een samenhangend model. Tijdens de exploitatiefase zal dit model gebruikt worden voor het beheer van de Outputspecificatie en zullen wijzigingen hierin verwerkt worden. Het actueel houden van de Outputspecificatie is voor MEET van groot belang gezien de relatie tussen de Outputspecificatie, het FMIS, het BIM model en de inrichting van dienstverlening. Opdrachtgever is verantwoordelijk voor het beheer van de Outputspecificatie tijdens de exploitatiefase.

> Na een overeengekomen wijziging zijn deze data te importeren in het FMIS. Een door MEET ingevoerde wijziging in de Outputspecificatie, wordt door de Opdrachtgever in het FMIS geaccordeerd. Hiermee zijn eisen in de Outputspecificatie altijd beschikbaar, actueel en is MEET in staat om ook na wijzigingen blijvend aan de Outputspecificatie te voldoen.

accordeert. Wij hebben geen nadere informatie op welke wijze deze accordering door opdrachtgever in het FMIS-systeem plaatsvindt.

Tijdens een demo is aangegeven dat Relatics een applicatie is van en door het Rijksvastgoedbedrijf. Tussen opdrachtgever en opdrachtnemer worden evt. wijzigingen overeengekomen die via een Verzoek tot wijziging leiden tot aanpassing in Relatics. In het FMIS-systeem wordt de wijziging doorgevoerd via Change management.

In het bijlagendocument staat op pagina 20 dat MEET de overeengekomen wijziging in de Outputspecificaties wordt overgenomen in het systeem dat MEET beheert en dat daarna via workflow de opdrachtgever goedkeuring geeft voor de aanpassing in Relatics. Daarna wordt beoordeeld of er een aanpassing in FMIS-systeem nodig is.

> **Koppeling applicaties**
> - *Relatics*
>
> De Outputspecificatie, zoals vastgelegd in Relatics, geldt als uitgangspunt en onderlegger voor de dienstverlening. Wijzigingen op het contract worden vastgelegd in goedgekeurde Wijzigingen (VtW procedure). De overeengekomen tekst in de Wijziging zal door MEET worden overgenomen in het systeem dat MEET beheert. Via een geautomatiseerde workflow kan de contractmanager van Opdrachtgever de bewerking van MEET controleren. Pas bij goedkeuring wordt de ingevoerde aanpassing definitief opgenomen in Relatics. Tijdens de vastlegging kan direct een toets plaatsvinden of in het FMIS ook een wijziging nodig is. Dit maakt standaard onderdeel uit van de VTW procedure. De Outputspecificatie is hiermee 'functioneel' gekoppeld.

Aan de hand van de aangetroffen beschrijvingen is het niet eenduidig

- wie de beheerder is van de Outputspecificaties in Relatics. Bij bespreking van onze bevindingen werd duidelijk dat het monitoringsplan was "vastgesteld met opmerkingen". Eén van deze opmerkingen was dat de opdrachtgever de beheerder is van Relatics.
- hoe / of wijzigingen, die zijn oorsprong hebben in Relatics, ook in FMIS-systeem geaccordeerd worden door de opdrachtgever en
- of er een relatie is met het onderhoud van de prijzen van de standaard variabele diensten.

Wij bevelen aan de afspraken aangaande mutaties in de Outputspecificaties in het monitoringsplan en het bijlagendocument te verduidelijken en op elkaar af te stemmen. Daarbij is het van belang dat iedereen de afspraken kent en dat eventuele wijzigingen in Relatics tijdig worden doorgegeven aan MEET.

In een toelichting op 20 oktober en daarna door MEET werd duidelijk dat mutaties in Relatics leiden tot een melding bij de beheerder van het FMIS-systeem. Afhankelijk van de wijziging voert de beheerder de wijziging ook door in het FMIS-systeem. Op dit moment is niet voorzien dat na een dergelijke wijziging in het FMIS-systeem de opdrachtgever wordt ingelicht.

Wij bevelen aan om na aanpassing in het FMIS-systeem op basis van een melding vanuit Relatics de wijziging in het FMIS-systeem te laten verifiëren door de opdrachtgever en dit vast te leggen.

2.7 Geen testresultaten aangaande Rapportage t.b.v. facturatie aangetroffen

Het facturatieproces met daarin de verschillende rapportages is beschreven in bijlage 2 van het bijlagendocument. Wij zien geen bijzonderheden in deze beschrijving. Het gebouw is nog niet operationeel, waardoor we geen constateringen hebben ten aanzien van een feitelijke rapportage. We hebben geen testen aangetroffen ten aanzien van de rapportage met daarop de verschillende kortingen in een bepaalde periode. Wanneer dergelijke rapportages met financiële impact niet getest zijn, is het risico dat bij facturatie onjuiste bedragen worden verwerkt.

Wij bevelen aan de (kortingen) rapportages te testen en hiervan vastleggingen te maken.

2.8 Maatregelen voor logische toegangsbeveiliging kunnen beter worden beschreven

FMIS-systeem-gebruikers van RIVM gaan via een vertrouwd RIVM netwerk naar het FMIS-systeem of loggen in met de mobiele telefoon met de windows credentials. FMIS-systeem-gebruikers via een niet-RIVM netwerk of via mobiele telefoon loggen direct in op de beveiligde site (https). Bij aanmelden is een gebruikersnaam en wachtwoord vereist. Wachtwoordlengte, periode voor wachtwoord vernieuwen, aantal speciale karakters en wachtwoordgeschiedenis kunnen worden ingesteld in het FMIS-systeem. De eigenschappen in combinatie met de sterkte van de wachtwoorden zijn op dit moment nog niet vastgesteld.

Wij bevelen aan om

- *wachtwoordvereisten in te stellen conform de normering van Baseline Informatiebeveiliging Overheid (BIO),*
- *de toepassing van 2-factor authenticatie voor FMIS-systeem te onderzoeken. Dit is mede gebaseerd op de BIO-normering die stelt dat bij toegang van een onvertrouwde zone naar een vertrouwde zone er sprake moet zijn van 2-factor authenticatie.*

De verstrekking van gebruikersnaam en wachtwoord voor niet-RIVM gebruikers vindt plaats via e-mail. Risico is dat bij onjuiste e-mail adressering de autorisatie onbedoeld in handen van derden kan vallen.

Wij bevelen aan hiervoor extra maatregelen te overwegen. Hierbij kan gedacht worden aan de eerder genoemde 2-factor authenticatie maar dan ook toegepast voor de eerste aanmelding.

Wij hebben geen beschrijving of systeeminstelling gezien ten aanzien van blokkering na een aantal foutieve inlogpogingen. Navraag leert ons dat een account na drie foutieve inlogpogingen wordt geblokkeerd. Dit is een standaard instelling die niet kan worden gemuteerd waardoor er geen printscreen van deze instelling beschikbaar is. In een speciale extra demonstratie op 20 oktober hebben wij gezien dat het account daadwerkelijk geblokkeerd (inactief) wordt na drie foutieve inlogpogingen.
Wanneer een maatregel niet beschreven en getest wordt, kan het gebeuren dat een maatregel (onbewust) bij nieuwe releases verdwijnt.

Wij bevelen aan deze maatregel te beschrijven en op te nemen in regulier testproces bij nieuwe releases.

Uit de documentatie is niet gebleken welke functionaliteit voor ontgrendeling zorgt van geblokkeerde accounts en welke gebruikersgroep toegang heeft tot de deze functionaliteit. In een demo hebben wij gezien dat dit de functioneel beheerder is. Wanneer niet bekend is welke rollen cruciale autorisaties hebben, kan het gebeuren dat bij blokkering van alle accounts met betreffende rollen het systeem onbeheersbaar wordt.

Wij bevelen aan ervoor te zorgen dat er maatregelen zijn getroffen, die voorkomen dat niet alle accounts met cruciale autorisaties tegelijkertijd geblokkeerd kunnen worden (beperking van het risico dat alle 'super users' middels fout aanmelden (van buiten af) geblokkeerd worden.) Dit kan door een 'super user' aan te maken met een minder gebruikelijke inlognaam, die bij weinig mensen bekend is.

2.9 Continuïteitsafspraken dienen nader gespecificeerd te worden

Ten aanzien van continuïteit voor het FMIS-systeem is een afspraak tussen MEET en opdrachtgever in de Outputspecificaties aangetroffen. Daarin staat dat het systeem 7 * 24 uur beschikbaar moet zijn.
Na het raadplegen van de documentatie zijn er nog onduidelijkheden aangaande de definitie van 7 *24 uur, toezicht op de continuïteit en eventuele (herhalings-) kortingen. Het risico is dat verschillende partijen andere interpretatie hebben bij deze Outputspecificaties en dat eventuele kortingen niet juist worden berekend.

Wij bevelen aan om meer toelichting op te nemen over:

- *de definitie van '7 * 24 uur' (van wat) denk daarbij aan eventuele afgesproken onderhoudswindows;*
- *hoe toezicht op de continuïteit plaatsvindt;*
- *hoe (wanneer) hieraan eventuele kortingen worden berekend.*

2.10 Beschrijving Wijzigingenbeheer FMIS-systeem kan verbeterd worden

Het FMIS-systeem is een standaardpakket dat door de leverancier via een cloudoplossing ter beschikking wordt gesteld. Het standaardpakket is aan meerdere organisaties verkocht en wordt dus door meerdere organisaties gebruikt. Tijdens de demo is toegelicht dat versiebeheer door de leverancier van het pakket, in dit geval ook de hosting partij, wordt uitgevoerd. In geval van een nieuwe versie gaan de klanten van het FMIS-systeem in twee 'batches' over naar de nieuwe versie. De implementatie van MEET draait niet mee in de eerste batch om de risico's te beperken.
De leverancier van het FMIS-systeem brengt periodiek een nieuwe versie uit. De installatie van een nieuwe versie vindt eerst plaats op de testomgeving. Na een test door MEET mag de leverancier de nieuwe versie op de acceptatieomgeving installeren. Als ook deze succesvol door MEET is getest, kan de installatie op de productieomgeving plaatsvinden.
We hebben waargenomen dat alle datawijzigingen worden gelogd, zodat ook achteraf inzichtelijk is wie welke wijzigingen heeft uitgevoerd.

Wijzigingsbeheer voor het FMIS-systeem
In het bijlagendocument monitoringsplan zijn de processen incident-, problem- en changeproces visueel en tekstueel weergegeven.
Wij hebben volgende aandachtspunten:

- De tekstuele beschrijving en de visuele duiding sluiten niet altijd geheel op elkaar aan.
- In het incident- en problemproces zijn er twee beslispunten, het is niet aangegeven waarop deze beslissingen worden gebaseerd. Het betreft
  - 'besluit mgt nodig',
  - 'change noodzakelijk' (changeproces wordt gestart).
- Er zijn activiteiten in het proces (voorbeeld is 'besluitvorming' bij changeproces) die ongeacht de uitkomst dezelfde weg lijken te vervolgen. Na 'oplossing testen en goedkeuren' door SUPER USER MEET volgt altijd 'implementatie in…'. Theoretisch zou het kunnen gebeuren dat SUPER USER MEET bevindingen heeft, hierin is niet voorzien in de procesbeschrijvingen van incident-, problem- en changeproces.
- In de procesbeschrijving is niet aangegeven of en hoe argumenten, eventuele financiële consequenties, testscenario's en testresultaten, die ten grondslag liggen aan besluitvorming worden vastgelegd en achteraf raadpleegbaar zijn.
- Het goedkeuren van een wijziging is voorbehouden aan de rol 'SUPER USER MEET'. De finale, inhoudelijke goedkeuring komt niet van de oorspronkelijke indiener.
- In het proces is niet beschreven dat wijzigingen zullen worden terug gekoppeld naar de oorspronkelijke indiener van de wijziging.
- Testen worden uitgevoerd door SUPER USER MEET. Indien nodig wordt een presentatie / sessie met de gebruikersorganisatie georganiseerd. Het is niet aangegeven welke afweging aan het geven van dergelijke presentatie ten grondslag ligt.

Wij bevelen aan om

- *na te gaan welke vastleggingen nodig zijn in het wijzigingsproces om achteraf aan te kunnen tonen dat de wijziging weloverwogen en met consensus uitgevoerd zijn en dit op te nemen in de procesbeschrijving;*
- *vastleggingen aangaande benodigde testscenario's en testen op te nemen in de procesbeschrijvingen;*
- *de terugkoppeling van wijzigingen aan de oorspronkelijke indiener op te nemen in de beschrijving van het changemanagementproces en te overwegen om deze oorspronkelijke indiener ook de bevoegdheid voor de finale goedkeuring te geven.*

3 Verantwoording onderzoek

3.1 Werkzaamheden en afbakening

Het object van onderzoek bestond uit de volgende onderdelen:
Modules van het FMIS-systeem

- Meldingen,
- Betalingsmechanisme (onderdeel van module Meldingen),
- Werkorders (onderdeel Periodieke Metingen),
- Reserveringen (onderdeel Aanvragen Catering),
- Bestellingen (ten behoeve van Standaard Variabele Diensten en Bijzondere Dienstverlening).

Koppelingen (interfaces)

- koppeling met het Gebouw Beheer Systeem (GBS),
- koppelingen met HR RIVM (personeelsgegevens),
- koppeling Inventaris Registratie- en Alarmeringssysteem (IRAS).

Rapportages t.b.v. de facturatie zoals Kortingsrapportage en Standaard Variabele Dienstenoverzicht.
Processen die als randvoorwaarden gelden voor rechtmatige facturatie zoals beheer stamgegevens (Outputspecificaties), beheer accounts, logging en noodscenario (continuïteit).

Wij hebben onderzoek gedaan naar de opzet van de maatregelen, procedures en afspraken rondom de monitoring van de PPS-dienstverlening en de implementatie daarvan in het FMIS-systeem. We hebben geen onderzoek gedaan naar het 'bestaan' van het FMIS-systeem, omdat het nog niet volledig operationeel is.

Het onderzoek heeft plaatsgevonden in de periode van 18 juni 2021 tot 16 september 2021. Voor het onderzoek is documentatie bestudeerd en zijn vier interactieve demo's van het FMIS-systeem gevolgd, die via een digitale vergadering aan ons op 18 en 23 juni en 2 en 5 juli 2021 zijn vertoond. De voornaamste documenten waren Monitoringsplan (Versie 2.0, 26-03-2021, Status: Definitief) Bijlagendocument Monitoringsplan (Versie 2.0, 26-03-2021, Status: Definitief), testresultaten, Lijst GBS- + standaardmeldingen FMIS-systeem MEET. De testresultaten en de demo's zijn gebaseerd op versie 21.3.0 van FMIS-systeem. Met deze aanpak hebben wij het onderzoek uitgevoerd conform de opdrachtbevestiging (kenmerk: 2021-0000113606).

We hebben voor het onderzoek gebruik gemaakt van referentiekaders zoals deze bekend waren bij opdrachtgever en opdrachtnemer en die eerder door de ADR met betrekking tot PPS onderzoeken/audits zijn gebruikt.

De bevindingen zijn afgestemd voor hoor en wederhoor. De inhoudelijke afstemming van dit rapport heeft plaatsgevonden met de opdrachtgever en auditee.

3.2 Gehanteerde standaard en kwaliteitsborging

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing. Dit onderzoek verschaft geen zekerheid in de vorm van een oordeel of conclusie, omdat het een onderzoeksopdracht betreft en geen controle-, beoordelings- of andere assurance-opdracht. Als hier wel sprake van was geweest, dan zouden we wellicht andere zaken hebben geconstateerd en gerapporteerd.

De opdracht is uitgevoerd conform de algemene uitgangspunten voor de uitoefening van de interne auditfunctie bij de rijksdienst. Daarbij hoort ook een stelsel van kwaliteitsborging. Een onderdeel daarvan is dat er een onafhankelijke kwaliteitstoetsing heeft plaatsgevonden op deze onderzoeksopdracht.

3.3 Verspreiding rapport

De opdrachtgever, Directeur Generaal RIVM, is eigenaar van dit rapport. Dit rapport is primair bestemd voor de 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.

In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de Auditdienst Rijk (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 rapporten die de ADR heeft uitgebracht en plaatst dit overzicht op www.rijksoverheid.nl.

4 Ondertekening

Den Haag, 19 november 2021

Drs. C.N. de Vette RE

Auditmanager

Auditdienst Rijk

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