Auditdienst Rijk
Ministerie van Financiën

Assurancerapport
Audit opzet, bestaan en werking Monitoring PPS Kempkensberg 12 Groningen 2021

Colofon

Titel	Audit opzet, bestaan en werking Monitoring PPS Kempkensberg Groningen 2021
Uitgebracht aan	Persoonsgegevens Persoonsgegevens het DG Belastingdienst
Datum	2 augustus 2022
Kenmerk	2022-0000205980

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Aanleiding opdracht

Het facilitair beheer van het overheidsgebouw aan de Kempkensberg 12 in Groningen is ingericht op basis van het samenwerkingsmodel Publiek-Private Samenwerking (PPS). De afspraken die gemaakt zijn tussen de private partij en de publieke partij zijn vastgesteld in een DBFMO[1] overeenkomst. De directie SSO CFD[2] van het Directoraat Generaal Belastingdienst van het ministerie van Financiën treedt op als verantwoordelijke vertegenwoordiger van de publieke partij voor de prestatieverklaring van dienstverlening die door de private partij wordt geleverd. De private partij is een consortium van bedrijven die gezamenlijk het facilitair beheer uitvoeren onder de naam DUO[2]. De prestatie-eisen waaraan DUO[2] moet voldoen zijn vastgelegd in de Outputspecificaties (OS). Ook zijn er procedurele bepalingen van de overeenkomst uitgewerkt in een contractueel vastgesteld monitoringsplan. De Outputspecificaties zijn vastgelegd in het tool Relatics, dat het Rijksvastgoedbedrijf beheert namens de opdrachtgever.

De praktische uitwerking is geconcretiseerd in een geautomatiseerd registratiesysteem (MyPrequest) waaraan het betalingsmechanisme is gekoppeld. Het vormt het hart van het monitoren van de naleving van de overeenkomst. Een derde partij, NPQ Solutions (in het rapport verder kortweg NPQ genoemd), voert het technisch - en functioneel beheer voor MyPrequest uit.

De Auditdienst Rijk (ADR) is door Persoonsgegevens gevraagd een audit uit te voeren naar de monitoring zoals die is uitgevoerd door DUO[2] over 2021. Dit is ten behoeve van de gebruikers van het gebouw aan de Kempkensberg 12 in Groningen.

Leeswijzer
Hoofdstuk 1 betreft de conclusie naar aanleiding van de audit die is uitgevoerd. De hoofdstukken 2 t/m 4 bevatten de belangrijkste bevindingen waarna in hoofdstuk 5 een beschrijving volgt van de doelstelling en object van onderzoek en de uitgevoerde werkzaamheden. In bijlage 1 staat de managementreactie op dit rapport namens de opdrachtgever. In bijlage 2 staat het normenkader en in bijlage 3 is het wegingsmodel opgenomen.

[1] DBFMO staat voor Design, Build, Finance, Maintain and Operate
[2] Shared Service Organisatie Centrum voor Facilitaire Dienstverlening

1 Conclusie

Naar ons oordeel is het geheel aan beheersmaatregelen in het monitoringsproces van de dienstverlening voortkomende uit de Publiek-Private Samenwerking aan de Kempkensberg 12 te Groningen 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 het oordeel:
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 goedkeurend oordeel 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)	**Afwijking**	**Leidt tot**
Zeer hoog	Geen afwijkingen	Geen effect op positief oordeel
Hoog	Geen afwijkingen	Geen effect op positief oordeel
Gemiddeld en laag	1 afwijking met een gemiddeld restrisico	Geen effect op positief oordeel

2 KWIS[3]-meldingen zijn juist en tijdig verwerkt, volledigheid niet te constateren

Onderstaande bevindingen zijn de belangrijkste bevindingen voor dit aspect uit de audit. Daar waar sprake is van een afwijking op de norm is deze meegewogen bij de oordeelsvorming.

2.1 Juistheid en tijdigheid van registratie van KWIS-meldingen geconstateerd.

De KWIS-meldingen zijn juist en tijdig geregistreerd, correct geclassificeerd en bij een eventuele overschrijding van de toegestane hersteltijd is de korting correct toegepast. Als er sprake is van het overschrijden van de toegestane hersteltijd, maar de oorzaak buiten de invloedssfeer van DUO[2] heeft gelegen, heeft in alle gevallen de opdrachtgever formeel geaccordeerd dat er geen korting is doorberekend.

2.2 Volledigheid KWIS-meldingen niet vast te stellen

In MyPrequest is de volledige registratie van alle KWIS-meldingen niet te constateren. Er is geen sprake van een doorlopende nummering op meldingenniveau. Een mogelijk risico is dat KWIS-meldingen onterecht zijn verwijderd.

Voor wat betreft de KWIS-meldingen zijn er twee maatregelen die het risico op het onterecht verwijderen ervan verlagen:

1. Medewerkers hebben niet de mogelijkheid om KWIS-meldingen te verwijderen. Deze functionaliteit bestaat niet in MyPrequest.
2. Een tweede aspect dat hierbij speelt is het feit dat potentieel kortinghoudende KWIS-meldingen alleen afkomstig zijn van de opdrachtgever. De opdrachtgever monitort de afhandeling van KWIS-meldingen. Niet afgehandelde KWIS-meldingen zullen door de opdrachtgever worden geconstateerd. Ook zal de oorspronkelijke melder gaan reclameren als zijn melding niet tot een oplossing heeft geleid. De monitoring door de opdrachtgever valt buiten de scope van deze audit en is dus door ons niet verder beoordeeld.

Deze maatregelen hebben ertoe geleid dat naar onze inschatting een gemiddeld restrisico resteert voor de volledigheid van de KWIS-meldingen.

Wij bevelen aan om aanvullende maatregelen in MyPrequest te treffen zodat een doorlopende nummering van de KWIS-meldingen aantoonbaar is of periodiek een vergelijking te maken met de KWIS-meldingen zoals die staan geregistreerd in het systeem van de opdrachtgever, het FMIS-OG.

2.3 Niet-ontvankelijke meldingen zijn juist onderbouwd

We hebben de onderbouwing van de niet-ontvankelijke meldingen beoordeeld. Daarin hebben wij geen afwijkingen geconstateerd.

2.4 Gereedmelding KWIS-meldingen summier

Veel KWIS-meldingen zijn afgemeld met een portofoonmelding. In de registratie in MyPrequest is dan alleen een tijdstip zichtbaar van de portofoonmelding met een korte afmeldingstekst. Er is geen informatie vastgelegd door wie deze afmelding is gedaan. Aanvullend hebben wij mede hierom beoordeeld of er consequent meldingen zijn die dicht tegen de toegestane hersteltijd zijn gereed gemeld. Daarvan is geen sprake.

---

[3] KWIS is een acroniem voor Klacht, Wens, Informatie en Storing

Wij bevelen aan om bij de gereedmelding ook de naam van de afmelder te laten vermelden.

2.5 Periodieke testen zijn in overeenstemming met het protocol uitgevoerd

DUO^2 houdt de planning van de periodieke testen goed bij in MyPrequest. Na afronding van een periodieke test geeft de opdrachtgever een akkoord of niet akkoord. Ook registreert DUO^2 de uitkomsten de uitkomsten van de periodieke testen in een separate registratie. Uit onze deelwaarneming blijkt dat er de periodieke testen in overeenstemming met het protocol zijn uitgevoerd, de resultaten zijn herleidbaar en de kortingen zijn juist en volledig doorberekend.

3 Logische toegangsbeveiliging voldoet, twee aandachtspunten

Onderstaande bevindingen zijn de belangrijkste bevindingen voor dit aspect uit de audit. Daar waar sprake is van een afwijking op de norm is deze meegewogen bij de oordeelsvorming.

3.1 Toegekende rechten passen bij de functies

De toegekende rechten in MyPrequest passen bij de functies van de medewerkers. Activiteiten binnen MyPrequest zijn dus op persoonsniveau te herleiden. Wij hebben ons daarbij moeten baseren op de autorisatiematrix die door DUO[2] buiten MyPrequest is bijgehouden. Wenselijker is om inzicht te hebben in de toegekende rechten vanuit MyPrequest zelf. MyPrequest voorziet niet hierin.

Wij bevelen aan om te onderzoeken of het mogelijk is om de autorisatiematrix in MyPrequest als rapport in te bouwen, inclusief de logging van de mutaties.

3.2 Opzetbeschrijving accountmanagement is (te) beperkt

In het Monitoringsplan is een procedure beschreven voor het toekennen van rechten. Dit vormt een onderdeel van het accountmanagement. Feitelijk worden hierin de taken van 2 partijen beschreven; die van de gebruiker en die van de opdrachtnemer. Binnen de taak van de opdrachtnemer is er echter ook een taak voor een medewerker die een aanvraag beoordeeld/goedkeurt en een taak voor iemand die een goedgekeurde aanvraag daadwerkelijk invoert in MyPrequest. De daadwerkelijke gang van zaken doet recht aan de vereiste functiescheiding van aanvragen, beoordelen en invoeren. Deze functiescheiding blijkt niet uit de opzetbeschrijving van het accountmanagement in het Monitoringplan.

Wij bevelen aan om in het Monitoringsplan in de beschrijving van het accountmanagement de functiescheiding tussen aanvragen, beoordelen en invoeren van rechten op te nemen.

4 Er is voldaan aan de ITGC-normen

PinkRoccade Healthcare B.V. is de hostingpartij die voor NPQ het tool myPrequest in technisch beheer heeft. Voor het totale beheer door deze organisatie is over de maanden januari tot en met oktober 2021 een 3402 Type II – verklaring[4] afgegeven door Auvaro. Aansluitend is er door PinkRoccade Healthcare B.V. over de maanden november en december 2021 een Bridgeletter afgegeven waarin is verklaard dat er geen significante wijzigingen zijn geweest in de control-omgeving. Tevens is verklaard dat met een redelijke mate van zekerheid de controls zijn nageleefd zodat de controldoelen ('control objectives') zijn bereikt.

Het Monitoringsplan stelt geen eisen aan de continuïteit van MyPrequest; wel aan de beschikbaarheid. De beschikbaarheidseis is 24 uur per dag, 7 dagen in de week (24/7). Overigens blijkt uit de OS dat in het geval dat MyPrequest niet beschikbaar is, een toegestane hersteltijd is van een half uur. Uit de 3402-verklaring Type II blijkt niet of aan de beschikbaarheidseis voldaan kan worden. Wel blijkt dat er sprake is van voldoende maatregelen op het gebied van de blijvende continuïteit. Hierbij gaat het om:

- De aanwezigheid van een continuïteitsplan;
- Service Level Agreements met de afnemers;
- Service Level Reports over de afspraken in de Service Level Agreements;
- Dagelijkse back-up's inclusief monitoring;
- Maandelijkse selfassessments en recoverytests;
- Jaarlijkse een fail-overtest.

De ADR heeft met eigen (aanvullend) onderzoek geconstateerd dat voldaan is aan de normen die betrekking hebben op de remote access en remote datacommunicatie.

[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.

5 Verantwoording onderzoek

5.1 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 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 bij DUO[2];
- Het proces van de berekening en de financiële afwikkeling van de eventuele kortingen;
- De verleende toegangsrechten (autorisaties) in MyPrequest;
- Het beheer van MyPrequest door de leverancier.

Buiten het object van onderzoek vallen de interfaces met de aanleverende applicaties, te weten het financieel informatiesysteem (FMIS) van de opdrachtgever en het Gebouwbeheersysteem. De audit is gestart bij de registratie in MyPrequest. Niet gemelde- en niet doorgegeven KWIS-meldingen vanuit de opdrachtgever vallen buiten de scope.

Normenkader

Op basis van de in de doelstelling genoemde criteria is een normenkader opgesteld. In bijlage 2 staat het normenkader. Wij hebben dit normenkader speciaal voor audits van de monitoring van PPS-opdrachten opgesteld. De opdrachtgever heeft een weging aan de normen gegeven. De basis van de normen zijn afgeleid van het Monitoringsplan, DBFMO-contracten, de Baseline Informatiebeveiliging Overheid en IT-beheer-normen.

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 (ADR) uitgevoerd in opdracht van Persoonsgegevens het Directoraat Generaal Belastingdienst van het ministerie van Financiën. Opdrachtnemer namens de ADR is Persoonsgegevens Persoonsgegevens de Auditdienst Rijk (ADR).

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

5.2 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.

5.3 Werkzaamheden

Om ons oordeel te kunnen formuleren is het noodzakelijk dat we beschikken over voldoende en geschikte controle-informatie. De werkzaamheden die we hebben verricht om die controle-informatie te verkrijgen, zijn gebaseerd op de afspraken die zijn gemaakt in de met de opdrachtgever overeengekomen werkzaamheden die zijn beschreven in de opdrachtvestiging met als kenmerk 20211130_Audit monitoring PPS Groningen van 30 november 2021. 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;
- De berekening van de kortingen en de verwerking ervan in de facturatie;
- De toegekende autorisaties in MyPrequest gedurende 2021 (m.n. gericht op geen doorbreking functiescheiding);
- De 3402-verklaring Type II van MyPrequest (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. De interviews zijn vastgelegd in verslagen welke voor hoor en wederhoor zijn voorgelegd aan de geïnterviewden.

Daarna heeft analyse en oordeelsvorming plaatsgevonden. Dit heeft geleid tot een eerste concept van dit rapport. De bevindingen die daarin zijn beschreven hebben wij voor hoor en wederhoor met de auditee op 14 juli 2022 besproken. De gemaakte opmerkingen zijn verwerkt.

De auditee heeft op 20 juli 2022 in een Letter of Representation bevestigd verantwoordelijk te zijn voor het onderzoeksobject en dat alle relevante informatie aan ons is aangeboden.

De conclusie, bevindingen en aanbevelingen in het conceptrapport zijn besproken met de opdrachtgever op 29 juli 2022.

5.4 Verspreiding rapport

De opdrachtgever, Persoonsgegevens Persoonsgegevens 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.

6 Ondertekening

Groningen, 2 augustus 2022

Persoonsgegevens

Persoonsgegevens

Persoonsgegevens

Auditdienst Rijk

Bijlage 1 Managementreactie

Belastingdienst

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

Datum
4 augustus 2022

Management reactie
Assurancerapport
Monitoring PPS Kempkensberg Groningen 2021

Hierbij de management reactie op het assurancerapport Monitoring PPS Kempkensberg Groningen 2021 van de Auditdienst Rijk betreffende de periodieke test Monitoring.
Naar aanleiding van de genoemde aanbevelingen zijn e volgende afspraken gemaakt:

1. DUO² gaat aanvullende maatregelen in MyPrequest treffen zodat een doorlopende nummering van de KWIS-meldingen aantoonbaar is of periodiek een vergelijking te maken met de KWIS-meldingen zoals die staan geregistreerd in het systeem van de opdrachtgever, het FMIS-OG en rapporteert de voortgang via het monitoringsoverleg aan SSO CFD;
2. DUO² gaat onderzoeken of het mogelijk is om de autorisatiematrix in MyPrequest als rapport in te bouwen, inclusief de logging van de mutaties en rapporteert de voortgang via het monitoringsoverleg aan SSO CFD;
3. DUO² gaat in het Monitoringsplan de beschrijving van het accountmanagement, de functiescheiding tussen aanvragen, beoordelen en invoeren van rechten op nemen;

Met een vriendelijke groet,

Persoonsgegevens

VERTROUWELIJK

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*
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 (als onderdeel van de PPS-overeenkomst), het uitvoeren daarvan en de betrouwbare vastlegging dienen te zijn gewaarborgd.	Hoog
3	**Rekenregels en Kortingsberekeningsmechanisme**	
3.1	De relatie tussen de outputspecificatie en de kortingberekeningsregels is eenduidig.	Zeer hoog
3.2	Nieuwe Outputspecificaties (OS) en wijzingen in de OS zijn op een beheerste wijze geïmplementeerd in het monitoringsysteem inclusief het kortingsberekeningsmechanisme.	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 serviceniveau.	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	De in het Monitoringsplan vastgelegde procedure voor het doorvoeren van wijzigingen in het monitoringssysteem is gevolgd. Belangrijke processtappen zijn daarin: • Bij een wijziging is er een akkoord cf. de afgesproken procedure; • De contractbeheerder toetst het ontwerp van de wijziging; • De functioneel beheerder voert de acceptatietesten uit en geeft een akkoord; • De invloed van de nieuwe functionaliteit is gecommuniceerd naar de gebruikers.	Gemiddeld

Bijlage 3 Wegingsmodel

Onderstaand wegingsmodel is gebruikt om afwijkingen ten opzichte van de normen en de restrisico's te wegen ten einde de conclusie over het object van onderzoek te kunnen bepalen.

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. Als het gemiddeld restrisico 1 onderwerp betreft, dan een oordeel met een beperking

Een oordeelsonthouding wordt afgegeven als er geen toereikende informatie gegeven kan worden. In alle overige situaties zal er een goedkeurende conclusie worden afgegeven.

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