Inspectie Leefomgeving en Transport
Ministerie van Infrastructuur en Waterstaat

Toezichtrapportage 2018 taakuitvoering Kiwa Register B.V.

Datum	2 juli 2020
Status	Definitief

Colofon

Inspectie Leefomgeving en Transport
afdeling Toezicht publieke instellingen
team Toezicht certificerende en erkende instellingen

Rijnstraat 8 Den Haag

Contactpersonen
Arie Visser (lead-auditor)
Pim Willems (auditor)

Versie 1.0
Opdrachtgever plv. Inspecteur-Generaal/directeur Omgeving en dienstverlening

Inleiding

Sinds 2010 heeft de Minister van Infrastructuur en Waterstaat taken gemandateerd aan Kiwa N.V. en in het verlengde hiervan aan Kiwa Register B.V. te Rijswijk (hierna aangeduid met *Kiwa*, tenzij specifiek onderscheid noodzakelijk is).

Een mandaat is de bevoegdheid om in naam van een bestuursorgaan besluiten te nemen. Een door een gemandateerde binnen de grenzen van zijn bevoegdheid genomen besluit, geldt als een besluit van het bestuursorgaan. De minister van Infrastructuur en Waterstaat blijft daarvoor verantwoordelijk.

Hoe de Inspectie Leefomgeving en Transport (hierna aangeduid met *inspectie)* invulling geeft aan haar toezicht, staat in de toezichtvisie op Kiwa N.V. en Kiwa Register B.V., zoals te vinden op www.ilent.nl. De toezichtvisie geeft de toezichtkaders, de inrichting en de aanpak van het toezicht op Kiwa weer.

Dit rapport bevat:

- een oordeel over de taakuitvoering over 2018 voor zover binnen de scope van dit onderzoek (zie paragraaf 2.1).
- een evaluatie van de problemen rond de certificering van de Public Key Infrastructure.
- een evaluatie van de uitgifte van nieuwe tachograafkaarten.

Per jaar voert de inspectie een audit uit op de uitvoering van taken door Kiwa. Daarbij wordt ook een realitycheck uitgevoerd door inhoudelijk deskundigen van de inspectie op een van de percelen Land, Water en Lucht. Doel van de realitycheck is om de feitelijke werking van het systeem te toetsen, door middel van een gegevensgerichte controle. In deze audit over 2018 betreft dit producten in het perceel Lucht.

Dit jaar is speciaal onderzoek gedaan naar de thema's Public Key Infrastructure en tachograafkaarten; hierbij zijn ook ontwikkelingen na 2018 meegenomen. Deze thema's zijn gekozen wegens geconstateerde risico's respectievelijk opgetreden vertragingen.

Naast de inspectie voeren ook andere partijen audits op Kiwa uit (onder andere European Union Aviation Safety Agency en British Standards Institution). Relevante bevindingen uit externe audits en de voortgang van de daaruit volgende verbeterplannen zijn in deze rapportage opgenomen. Doel hiervan is om een zo compleet mogelijk inzicht te bieden in de kwaliteit en continuïteit van de dienstverlening door Kiwa.

1 Samenvatting

In deze toezichtrapportage geeft de inspectie een beeld van het presteren van Kiwa Register B.V. (Kiwa) in het licht van de overeenkomst tussen de minister van Infrastructuur en Waterstaat en Kiwa N.V. De inspectie is met Kiwa overeengekomen dat Kiwa deze rapportage op zijn website publiceert.

1.1 Conclusie

De Inspectie Leefomgeving en Transport (de ILT) is van oordeel dat Kiwa gesteld staat voor de opgedragen taken en dat de kwaliteit en de continuïteit van de taakuitvoering in voldoende mate geborgd zijn.

De ILT heeft niettemin bevindingen gedaan waarvoor corrigerende maatregelen dienen te worden genomen.

Verder wees het externe toezicht door British Standards Institution op Kiwa uit dat Kiwa niet aan eisen voldeed, waardoor continuïteitsrisico's op het gebied van de Boordcomputer Taxi toenamen. Deze eisen betroffen de Public Key Infrastructure. Na inspanning van Kiwa is de situatie tijdig genormaliseerd.

1.2 Bevindingen

De audit heeft de volgende vier bevindingen opgeleverd:

- 2018B1 en 2018B2: Kiwa kon niet voor alle gevallen uit de deelwaarneming aantonen dat Aircraft Maintenance Licences en Flight Crew Licences zijn afgegeven in overeenstemming met de geldende wet- en regelgeving en de interne procedures. Kiwa onderzoekt voor deze individuele gevallen of dit heeft geleid tot risico's en zal zonodig maatregelen nemen.
- 2018B3: Kiwa voldoet nog niet aantoonbaar aan de vigerende eisen ten aanzien van informatiebeveiliging. Kiwa onderneemt op eigen initiatief stappen om aantoonbaar aan deze eisen te voldoen.
- 2018B4: Een gedegen onderzoek naar de oorzaken waardoor de gevraagde tachograafkaarten niet tijdig konden worden geleverd, is nog niet uitgevoerd.

1.3 Follow up

De inspectie wil uiterlijk 14 augustus 2020 een corrective action plan (CAP) ontvangen met verbeteracties naar aanleiding van de bevindingen uit dit rapport plus de resultaten van het onderzoek naar de individuele gevallen, bedoeld in bovengenoemde bevindingen 2018B1 en 2018B2.). De ILT is voornemens de verbetermaatregelen van Kiwa te beoordelen, voor zover mogelijk, tijdens de volgende audit. De ILT zal het effect van de verbetermaatregelen met belangstelling volgen en hierop terugkomen.

2 Doel en aanpak

2.1 Doel

Doel van het toezicht is te bepalen of de uitvoering van de overgedragen taken en bevoegdheden in overeenstemming is met de afgesproken prestatie-eisen en de geldende wet- en regelgeving. Het toezicht is gericht op het borgen van de continuïteit en kwaliteit van de taakuitvoering. De inspectie heeft haar toezichtvisie op Kiwa N.V en Kiwa Register B.V. gepubliceerd.

Het toezichtprogramma 2018 legt op basis van een risicoafweging het accent op de volgende onderwerpen:

1. Follow up van bevindingen uit de ILT-audit over 2017 en de werking van verbeterplannen;
2. Follow up van bevindingen uit Kiwa-interne audits en externe audits;
3. Opvolging klachten en bezwaren;
4. Naleving door Kiwa en de ILT van informatieprotocol (exclusief kostprijsgegevens);
5. Reality check perceel Lucht;
6. Public Key Infrastructure (PKI) ten behoeve van de boordcomputer taxi (BCT);
7. Tachograafkaarten (n.a.v. de uitwijk naar Kroatische kaarten voor de werkplaatskaarten en Britse kaarten voor chauffeurskaarten).

Bij de laatste twee onderwerpen heeft de inspectie zich niet beperkt tot 2018 omdat de evaluatie van deze onderwerpen dat vereiste.

2.2 Aanpak

De voorbereiding en feitelijke uitvoering van de audit vonden plaats in de tweede helft van 2019. Het toezicht bestond uit het afnemen van interviews en uit deskresearch. Voor bovengenoemde onderwerpen, behalve de reality check, hebben de interviews plaatsgevonden op 4 en 5 november 2019. De reality check is uitgevoerd op 16 en 19 december 2019.

De bevindingen zijn vastgelegd in deze rapportage. De inspectie heeft hoor en wederhoor gepleegd om te borgen dat feiten juist zijn weergegeven. De documenten die Kiwa beschikbaar stelde tijdens de audit en ter onderbouwing van dit rapport dienen, zijn in bewaring bij Kiwa.

3 Bevindingen

3.1 Follow up van bevindingen uit de ILT-audit over 2017

Kiwa heeft een *corrective action plan* (hierna: *CAP*) opgesteld op basis van de uitkomsten van de audit over 2017. Dit CAP is op 16 december 2019 aangeleverd nadat de definitieve versie van de toezichtrapportage op 1 oktober 2019 gereed is gekomen; zie bijlage B voor de CAP. Kiwa heeft daarmee in de plan-fase voldoende inspanning geleverd op de verbeterpunten. De inspectie zal bij de volgende audit aan de hand van een *corrective action report* (hierna: *CAR*) de effectiviteit van de genomen maatregelen beoordelen.

3.2 Follow up van bevindingen uit Kiwa-interne audits en externe audits

3.2.1 Interne audits

Interne audits worden uitgevoerd conform de Werkinstructie Interne Auditing en het Coporate Manual Kiwa.
De voortgang van alle acties die voortkomen uit interne audits (productaudits en procesaudits) wordt centraal bewaakt door de auditors.

Maandelijks wordt een rapportage vervaardigd waarin over de voortgang van acties wordt gerapporteerd aan het verantwoordelijk management.

Interne audits worden bij Kiwa op 3 jaarlijkse basis gepland en uitgevoerd. Van de primaire en secundaire processen wordt een risico profiel gemaakt en op basis hiervan wordt er een planning gemaakt. Producten en processen die een hoog risico vormen worden elk jaar (of soms 2 keer per jaar) in de planning opgenomen.

productaudits
Een team van drie auditors voert audits uit op productdossiers. Deze productaudits vinden voornamelijk plaats op fysieke dossiers die volgens een beschreven methode aselect en representatief worden geselecteerd.
De auditee stelt op basis van een uitgevoerde audit een CAR op dat gekeurd wordt door de lead auditor. De gereed gemelde acties worden door de lead auditor gecontroleerd (follow-up).
De product auditors vallen organisatorisch onder de afdeling Operations en IT en zijn daarom niet volledig onafhankelijk van alle onderdelen van Kiwa register. Door de gekozen werkwijze is het afhankelijkheidsrisico evenwel beperkt.

procesaudits
Procesaudits worden uitgevoerd door de kwaliteitscoördinator die ook verantwoordelijk is voor het opstellen en het beheer van het auditjaarplan. Het auditplan is risk-based waarbij de hoogte van het risico de auditfrequentie bepaalt.

Audits van applicaties vinden niet expliciet plaats, maar tijdens de audits kunnen tekortkomingen van applicaties worden geconstateerd. Er kan dan een zogenaamde call worden geïnitieerd (wijzigingsverzoek), om de tekortkoming te verhelpen.

3.2.2 Externe audits

Er worden bij Kiwa door verschillende organisaties externe audits uitgevoerd. Ook worden externe audits uitgevoerd bij de ILT waarbij ook de rol van Kiwa is betrokken.
Recente externe audits bij Kiwa zijn in onderstaande tabel genoemd.

Omschrijving audit	Uitgevoerd door	wanneer
ISO 9001	BSI	2019
PKI-ETSI ETSI: European Telecommunications Standards Institute De ETSI heeft normen opgesteld waaraan een PKI dient te voldoen.	BSI (meerdere audits in periode 2015-2018)	2015-2018
ERCA audit (European Root Certification Authority): Compliance of Kiwa Register B.V. with the MSA policy of The Netherlands	Price Waterhouse Coopers (hierna: *PWC*).	27-09-2018
Standardisation inspection	EASA	27-03-2019
Standardisation inspection	EASA	05-04-2018
Standardisation inspection	EASA	21-04-2017

Het kwaliteitssysteem van Kiwa is opgezet conform ISO 9001 en BSI is de geaccrediteerde partij die de daar bijbehorende audits uitvoert.

De EASA heeft verder aangegeven dat de samenwerking tussen ILT en Kiwa op sommige punten onduidelijk was. Naar aanleiding hiervan is het zogenaamde ‘interface document’ aangepast. Het interface document is een leidraad voor de samenwerking tussen de ILT (luchtvaart) en Kiwa, waarin is vastgelegd welke procedures en/of werkinstructies gevolgd moeten worden voor een goede invulling van de taken.

Resultaten van de ERCA audit zijn nog niet opgepakt. In deze audit is door PWC onderzocht in hoeverre de uitgifte van tachograafkaarten door Kiwa in overeenstemming is met het Nederlandse Member State Authority beleid (hierna: MSA). Kiwa vervult de rol van Card Issuing Authorithy (hierna: CIA) voor tachograafkaarten en de ILT vervult de rol van MSA.

In tegenstelling tot interne audits is er voor externe audits geen procedure geïmplementeerd voor de opvolging van bevindingen. Het risico bestaat dat bijvoorbeeld door personele wisselingen bevindingen niet of te laat worden opgepakt.

Observatie 2018O1
Een procedure voor de opvolging van bevindingen uit externe audits ontbreekt.

3.3 Opvolging klachten, bezwaren en claims

Opvolging van klachten, bezwaren en claims wordt door dezelfde 3 medewerkers uitgevoerd die ook de product audits uitvoeren (zie 3.2.1). Audits m.b.t. dit proces worden daarom uitgevoerd door de kwaliteitscoördinator.
Er is een werkinstructie en een procesbeschrijving beschikbaar voor de afhandeling van klachten, bezwaren en claims. Het proces wordt ondersteund door Livelink (workflow management).

In het protocol bezwaar en beroep (maakt sinds 2012 deel uit van de overeenkomst met Kiwa N.V.) is in artikel 2 vastgelegd aan welke tijdslijnen ILT en Kiwa zich dienen te houden: interne afhandeling binnen één week of sneller indien de casus daarom vraagt en voor elke klacht dient binnen twee werkdagen telefonisch contact te worden opgenomen met de indiener. In Bijlage 2 van de overeenkomst tussen Kiwa en de ILT zijn tevens de volgende kritische proces indicatoren (Kpi's) opgenomen: aantal bezwaarschriften en klachten (<1% aantal ingediende aanvragen).

Een klant van Kiwa kan binnen zes weken tegen een besluit (beschikking) in bezwaar gaan bij de ILT.

Voor klachten geldt dat wanneer de indiener van de klacht het niet eens is met de wijze waarop Kiwa de klacht heeft afgehandeld, hij naar de Nationale Ombudsman kan stappen. Dit is opgenomen in de clausule van een schriftelijke afhandeling van een klacht. De Nationale Ombudsman hanteert hiervoor een termijn één jaar.

Er wordt maandelijks gerapporteerd over het aantal klachten en claims van de afgelopen 7 maanden. In de kwartaalrapportage wordt uitgebreider gerapporteerd over klachten en claims. Deze kwartaalrapportage wordt door Kiwa aan de ILT gestuurd. Er wordt gerapporteerd over het aantal claims, klachten en bezwaarschriften.
Een rapportage over de afgesproken Kpi's is opgenomen in het jaarverslag van Kiwa Register B.V., hieruit blijkt dat in 2018 goeddeels aan de afgesproken normen is voldaan. In verhouding tot het aantal producten dat door Kiwa wordt afgegeven kan het aantal klachten, claims en bezwaren als zeer gering worden geclassificeerd, in 2018 zijn er 218 afgehandeld wat overeenkomt met 0,24 % van het aantal aangevraagde vergunningen. Over 2018 is 13% van het aantal ingediende bezwaarschriften door ILT toegekend. Dit is boven de vastgelegde norm van 5%. In het jaarverslag wordt gesteld dat hiervoor op moment van publicatie (juni 2019) nog geen analyse is uitgevoerd.

3.4 Naleving door Kiwa en de ILT van informatieprotocol

In het Topdocument QMS (Kiwa, 18 december 2018) zijn de overleggen beschreven tussen Kiwa en de buitenwereld (o.a. ILT). Dit overzicht is wordt jaarlijks geactualiseerd.

Er is daarnaast een overzicht van alle operationele informatie-uitwisseling met externe partijen. Het betreft twaalf geautomatiseerde informatiestromen waarvan 6 (ook) met de ILT. Het betreft vooral informatie die door Kiwa met verouderde software wordt aangemaakt. Omdat Kiwa deze software (persvv, Cavca, Flare) gaat vervangen door eigentijdse systemen (Appian als Target platform) is dit het moment om die informatie-uitwisseling kritisch te beschouwen (aanpassingen kunnen nu eenvoudig worden gerealiseerd).

Overleg tussen de ILT en Kiwa over de PKI vindt maandelijks plaats. Agenda's en verslagen van dit overleg zijn ingezien.
Ketenoverleg met vertegenwoordiging van: Kiwa, I&W, AMP, KPN en Idemia vindt ongeveer 2 maal per jaar plaats. Verslagen en agenda's hiervan zijn aanwezig.

3.5 Reality check perceel Lucht

Bij reality checks wordt met behulp van een gegevensgerichte controle de werking van het systeem getoetst, waarbij de inspectie kan vaststellen of wet- en regelgeving volledig,

juist en tijdig is verwerkt in systemen, producten en werkbeschrijvingen. Over 2018 is een reality check uitgevoerd op het perceel Lucht, onderdelen Aircraft Maintenance Licences (Part 66) en Flight Crew Licences (FCL).

De reality check heeft uitgewezen dat bij beide onderdelen niet in alle gevallen kon worden aangetoond dat bewijzen van bevoegdheid zijn afgegeven in overeenstemming met de geldende wet- en regelgeving en de interne procedures van Kiwa.
De deelwaarneming die tijdens de reality check is uitgevoerd, geeft geen aanleiding om uitgegeven brevetten in te trekken of te wijzigen. Kiwa onderzoekt voor deze individuele gevallen of dit heeft geleid tot risico's en zal zonodig maatregelen nemen.

Bevinding 2018B1
Kiwa kon niet voor alle gevallen aantonen dat Aircraft Maintenance Licences zijn afgegeven in overeenstemming met de geldende wet- en regelgeving en de interne procedures.

Bevinding 2018B2
Kiwa kon niet voor alle gevallen aantonen dat alle Flight Crew Licences zijn afgegeven in overeenstemming met de geldende wet- en regelgeving en de interne procedures.

3.6 Public Key Infrastructure

Een PKI is een systeem waarmee uitgifte en beheer van digitale certificaten wordt gerealiseerd. De PKI wordt toegepast door Kiwa en de ILT om de integriteit en vertrouwelijkheid van BCT-informatie te borgen (BCT=boordcomputer taxi). Om vast te stellen dat Kiwa voldoet aan de (informatiebeveiligings-)eisen die worden gesteld aan haar rol in de PKI worden certificeringsaudits uitgevoerd door (of namens) BSI.

In 2015 zijn door BSI tekortkomingen geconstateerd. In het auditrapport hercertificering van oktober 2017 zegt BSI het volgende:

> *"Tijdens de follow-up audit uitgevoerd in februari 2017 (auditreferenties 8663218 en 8663219) hebben wij reeds gewezen op de noodzaak tot vervanging van de Windows 2003 servers ("Wij willen benadrukken dat indien de Windows 2003 servers tijdens de volgende reguliere audit niet zijn gemigreerd, dit mogelijk negatieve impact zal hebben op de certificaatverlenging per 17-12-2017")"*

en

> *"Gezien de structurele afwijking ten aanzien van de niet ondersteunde Windows 2003 platformen brengt het auditteam een advies uit aan de BSI certificatiecommissie tot opschorten van beide conformiteitscertificaten. Dit betekent uiteraard ook dat wij geen advies tot verlenging van beide conformiteitscertificaten kunnen geven."*

In maart 2018 kon Kiwa aantonen dat alle 5 de servers waren gemigreerd naar Windows 2012 en is zij alsnog zonder voorwaarden voor 2 jaar gecertificeerd.

Het up to date houden van hard- en software is een belangrijk onderdeel van de inrichting van de informatiebeveiliging, waarover in de overeenkomst met Kiwa afspraken zijn opgenomen (in B7.3): "Kiwa draagt op voet van de ter zake voor de Rijksdienst vigerende geldende voorschriften zorg voor de nodige technische en organisatorische voorzieningen ter beveiliging van zijn gegevens tegen verlies of aantasting en tegen onbevoegde kennisneming, wijziging en verstrekking van die gegevens." Voor de Rijksoverheid is hiervoor de

BIO van toepassing (Baseline Informatiebeveiliging Overheid) voorheen BIR (Baseline Informatiebeveiliging Rijk). Zowel de BIO als de BIR zijn een kopie van ISO 27001 aangevuld met ISO 27002: ISO 27001 betreft de inrichting van een ISMS (Information Security Management System); ISO 27002 bevat 'best practices' voor te nemen maatregelen.

Bevinding 2018B3
Kiwa voldoet nog niet aantoonbaar aan de eisen ten aanzien van informatiebeveiliging. Kiwa onderneemt op eigen initiatief stappen om aantoonbaar aan deze eisen te voldoen.

Kiwa heeft belangrijke stappen genomen die informatiebeveiliging en het behoud van conformiteitscertificaten moeten borgen:

1. Er is een legacy road map opgesteld voor het vervangen van verouderde software.
2. Na vervanging van de legacy zal ook Kristal en vervolgens CABS worden vervangen.
3. Er zijn volgens mededeling stringente afspraken (SLA's) gemaakt met Axians over onder andere patching, upgrade en hardening. Wekelijks bespreken Kiwa en Axians de wijzigingen en vooruitgang.
4. Er wordt een Security Operations Centre (SOC) ingericht door Axians. Met behulp van een SOC worden de computer- en netwerkactiviteiten in een organisatie gemonitord. Log-informatie van applicaties en apparaten in het bedrijfsnetwerk wordt verzameld en onderzocht op afwijkende zaken
5. Kiwa servers zijn geplaatst bij de hosting partij waar ze in een en extra beveiligde omgeving worden geplaatst (zogenaamde kooi).
6. In samenwerking met de ILT wordt door Kiwa een ketenbrede risicoanalyse uitgevoerd.
7. Kiwa is voornemens om ISO 27001 (Informatiebeveiliging) te worden gecertificeerd. In voorbereiding daarop zal een Fit-gap analyse worden uitgevoerd.

3.7 Tachograafkaarten

Op 15 juni 2019 is de Uitvoeringsverordening (EU) Nr. 2016/799 in werking getreden die voorschrijft dat in alle nieuwe voertuigen vanaf die datum een 2e generatie digitale tachograaf, de zogenaamde smart tachograaf is geïnstalleerd. Deze nieuwe tachograaf moet worden geijkt/geïnstalleerd met behulp van een nieuwe versie van de werkplaatskaart en chauffeurs hebben een nieuwe versie van de chauffeurskaart nodig.
De levering van eerst nieuwe werkplaatskaarten en later nieuwe chauffeurskaarten is problematisch verlopen omdat de kaarten niet tijdig via de beoogde procedure (via Idemia) konden worden afgeleverd. De opeenvolging van zaken hieromtrent is gedocumenteerd in o.a. diverse kamerstukken (35 000 XII Nr. 76 en Nr. 78) en er zijn Kamervragen over gesteld aan de minister van Infrastructuur en Waterstaat.

Bevinding 2018B4
Een gedegen onderzoek naar de oorzaken waardoor de gevraagde kaarten niet tijdig konden worden geleverd, is nog niet uitgevoerd.
Daarom is niet zeker dat door diverse partijen voorgestelde oplossingen kunnen voorkomen dat een soortgelijk scenario zich herhaalt. Een dergelijk onderzoek of evaluatie dient nog plaats te vinden. Hierbij dienen alle deelnemende partijen te worden betrokken.

Factoren die van invloed lijken te zijn geweest op het niet kunnen leveren van kaarten:

1. De Nederlandse Certificate Policy Digitale Tachograaf Generatie 2 is laat opgeleverd door de MSA. De ILT vervult de rol van MSA. Kiwa heeft in een brief aan de ILT op 24 mei 2018 gemeld dat deze policy voor Kiwa en haar ketenpartners het vertrekpunt is om hun werkzaamheden uit te voeren. Door een verlate oplevering van de policy is het implementatietraject verkort.
2. De typegoedkeuring is in eerste instantie door de ILT in behandeling genomen, totdat bleek dat de ILT hiervoor niet de bevoegde instantie is. In tweede instantie is de typegoedkeuring door de RDW (de hiervoor bevoegde instantie) geweigerd vanwege de achtergrondkleur van de kaart. Afkeuring van de achtergrondkleur hield verband met een nieuwe interpretatie van bestaande regelgeving.
3. Tijdens de testen door het Joint Research Center (Hierna: JRC) werden fouten gevonden waardoor de kaart niet kon worden goedgekeurd. JRC test de werkplaatskaarten echter met een tachograaf die wordt gereset en niet met een tachograaf nieuw uit de doos. Dit blijkt de testresultaten te kunnen beïnvloeden.

De uitwijk naar Kroatische kaarten voor de werkplaatskaarten en Britse kaarten voor chauffeurskaarten heeft goed gewerkt.

Door Kiwa wordt aangegeven dat de werkplaatskaart pas eind september 2019 geleverd kon worden. Een belangrijke constatering is dat Kiwa in juli 2019 op eigen initiatief heeft getest (bij DAF trucks) of ze ook daadwerkelijk life konden gaan. Tijdens deze test bleek in speciale gevallen de tachograaf niet geijkt te kunnen worden. Door deze test uit te voeren is voorkomen dat nieuwe problemen zijn ontstaan.

Bijlage A Bevindingen en observaties 2018 met normen

Onderdeel	Bevindingen (B) en observaties (O)	Normen
Opvolging bevindingen/ verbeterpunten 2017	*Kiwa heeft een corrective action plan (CAP) opgesteld op basis van de uitkomsten van de audit over 2017. Dit CAP is op 16 december 2019 aangeleverd nadat de definitieve versie van de toezichtrapportage op 1 oktober 2019 gereed is gekomen. Kiwa heeft daarmee in de plan-fase voldoende inspanning geleverd op de verbeterpunten. De CAP is in bijlage B opgenomen. De inspectie zal bij de volgende audit aan de hand van de CAR de effectiviteit van de genomen maatregelen beoordelen.*	Hoofdstuk 5 uit Bijlage J van de overeenkomst: Het toezicht op de inhoudelijke taakuitvoering betreft ook het doen opstellen en doorvoeren door Kiwa van verbetermaatregelen op de in de audits geconstateerde tekortkomingen. De ILT beoordeelt de verbetermaatregelen en monitort het doorvoeren daarvan.
Follow up van bevindingen uit Kiwa interne audits	Geen bevindingen of observaties	De opvolging van interne audits dient te worden beheerst door gebruik te maken van het kwaliteitsmanagement systeem (KMS).
Follow up van bevindingen uit Kiwa externe audits	**2018O1** Een procedure voor de opvolging van non-conformities ofwel opvolging van CAP's (corrective action plans) die voortkomen uit externe audits ontbreekt.	De opvolging van externe audits dient te worden beheerst door gebruik te maken van het kwaliteitsmanagement systeem (KMS).
Realitycheck perceel Lucht	**2018B1** Kiwa kon niet voor alle gevallen uit de deelwaarneming aantonen dat Aircraft Maintenance Licences zijn afgegeven in overeenstemming met de geldende wet- en regelgeving en de interne procedures. **B018B2** Kiwa kon niet voor alle gevallen uit de deelwaarneming aantonen dat Flight Crew Licences zijn afgegeven in overeenstemming met de geldende wet- en regelgeving en de interne procedures.	66.B.100(a); Wet Luchtvaart art. 3.30; Besluit bewijzen van bevoegdheid voor de luchtvaart art. 2 ARA.GEN.315; ARA.FCL.200; ARA.FCL.220; Part FCL, Part MED
Public Key Infrastructure	**2018B3** Kiwa voldoet nog niet aantoonbaar aan de eisen ten aanzien van	Overeenkomst over-dracht taken

	informatiebeveiliging. Kiwa onderneemt op eigen initiatief overigens al stappen om aantoonbaar aan deze eisen te voldoen. Toelichting: Overheidsinstellingen dienen compliant te zijn met de BIO (Baseline Informatiebeveiliging Overheid) voorheen BIR (Baseline Informatiebeveiliging Rijk). Zowel de BIO als de BIR zijn een kopie van ISO 27001 aangevuld met ISO 27002). ISO 27001 betreft de inrichting van een ISMS (Information Security Management System). De ISO 27002 bevat “best practices” voor te nemen maatregelen	van de minister van Infra-structuur en Waterstaat en Kiwa N.V. B7.3. Kiwa draagt op voet van de ter zake voor de Rijksdienst vigerende geldende voorschriften zorg voor de nodige technische en organisatorische voorzieningen ter beveiliging van zijn gegevens tegen verlies of aantasting en tegen onbevoegde kennisneming, wijziging en verstrekking van die gegevens.
Tachograafkaarten	**2018B4** Een gedegen onderzoek naar de oorzaken waardoor Idemia uiteindelijk de gevraagde kaarten niet tijdig kon leveren heeft nog niet plaatsgevonden. Toelichting: Omdat evaluatie niet heeft plaatsgevonden is niet zeker dat door diverse partijen voorgestelde oplossingen kunnen voorkomen dat een soortgelijk scenario zich herhaalt. Een dergelijk onderzoek of evaluatie dient nog plaats te vinden. Hierbij dienen alle deelnemende partijen te worden betrokken.	Voor de dagelijkse beheersing van risico’s is het KMS (incl. audit, rapportage et cetera) een belangrijk middel. Als het dan toch mis gaat is het managen van incidenten en calamiteiten belangrijk. Evaluatie (=Check) van incidenten, als onderdeel van de PDCA-cyclus is een voorwaarde voor verbetering van de kwaliteit van het kaartvervangingsproces.

Bijlage B Opvolging bevindingen en observaties 2017

CAP Kiwa n.a.v. de ILT audit 2017		
Ref.	**Bevinding of observatie**	**Maatregel**
B1	Aantallen afgegeven producten in de rapportages sluiten niet aan.	Als maatregel hiervoor bevriest Kiwa vanaf het eerste kwartaal 2018 de data die gebruikt wordt voor het vullen van de kwartaalrapportage. Daarmee kan Kiwa op regelniveau aangeven waar eventuele verschillen zijn ontstaan. De volledige analyse op de verschillen zal in Q1 2020 plaatsvinden. Tevens worden de rapportages nu vanuit cumulatieven opgebouwd om te voorkomen dat mutaties / correcties in een voorgaande periode ten onrechte niet worden meegenomen.
B2	Tekortkomingen in de opzet en werking van het fraudebeheersingsproces	Kiwa Register heeft in november 2018 een interne audit uitgevoerd op het onderwerp Fraudebeheer. De maatregelen die daaruit zijn voortgekomen zijn gerealiseerd. Zo zijn o.a. het beleid en de procedures rondom fraudebeheersing geactualiseerd.
B3	De volledigheid van waardepapieren kan niet worden gegarandeerd.	Kiwa Register heeft in februari 2018 een interne audit uitgevoerd op dit specifieke onderwerp. De maatregelen die daaruit zijn voortgekomen zijn gerealiseerd. Tevens is de ruimte waar de blanco waardepapieren geprint worden met gegevens van de aanvrager afgesloten en alleen middels een tag toegankelijk voor een beperkt aantal print-operators. Het verbruik van waardepapieren wordt geregistreerd.
B4	Doorvertaling wet- en regelgeving in vele instrumenten en hierdoor zoeken voor de behandelaar. Dit vergroot de kans op het niet juist toepassen van alle toetsingscriteria. Uit dossiers is het toepassen van alle toetsingscriteria niet altijd navolgbaar.	De adviezen die gegeven zijn in de reality check voor Land zullen worden opgevolgd. Dit betreft o.a. het aanpassen van het Product Bron Boek en Werk Instructies. M.b.t Internationaal Vervoer is het beleid dat dit alleen door een ervaren medewerker wordt gedaan gezien de complexiteit van de regelgeving en de aanvragen. Bij nieuw in gebruik te nemen systemen voor vergunningverlening zullen de criteria waarop wordt getoetst worden vastgelegd. Een eerste release (voor de Ondernemersvergunningen voor Bus en Taxi) zal naar verwachting in Q4 live gaan.
B5	De rapportages van autorisatiecontroles geven geen inzicht in een integrale beoordeling van alle toegekende rollen irm. bevoegdheden van functionarissen.	De opbouw van de rapportage zal worden gewijzigd aan de hand van een door Kiwa Register op te stellen baseline voor applicatierollen en -autorisaties per unieke functie binnen de Kiwa Register organisatie.

B6	De toereikendheid van de verzekering is niet vast te stellen. Een ontoereikende verzekering kan een bedreiging vormen voor de continuïteit.	De onderbouwing van de toereikendheid van de verzekering(en) van Kiwa N.V. wordt periodiek getoetst door de Raad van Accreditatie. Hieruit zijn geen specifieke bevindingen naar voren gekomen.
O1	Op werkinstructieniveau zijn nog op enkele plekken verouderde afdelingsnamen, functienamen en ministerienaam aangetroffen.	Werkinstructies worden gecontroleerd op verouderde namen en waar nodig aangepast.
O2	Oude logo's en ondertekeningen worden nog gebruikt. De migratie van verschillende waardekenmerken dient in lijn te blijven.	Kiwa Register heeft ten tijde van de naamsverandering expliciet toestemming gevraagd en verkregen van de ILT om de bestaande voorraad waardepapieren op te maken. Nadat deze voorraad is verbruikt zal Kiwa Register nieuwe logo's en ondertekening in gebruik nemen.
O3	De PDCA-cyclus kan versterkt worden door tactisch overleg tussen de juridische functie van de inspectie en Kiwa over bezwaarzaken, afwegingskaders en motivering.	Er zijn periodiek overleggen tussen specialisten van Kiwa en de ILT binnen de diverse domeinen. Indien daar aanleiding toe is zal daarbij de juridische functie van Kiwa Register aanschuiven. Bezwaarzaken worden in de regel afgehandeld door de ILT waarbij de operationele functie van Kiwa Register het onderliggende aanvraagdossier aanreikt aan de juridische functie van de ILT. In bijzondere gevallen is er contact tussen de juridische functies van Kiwa Register en de ILT en kan dit leiden tot aanpassing van werkwijzen van Kiwa Register of de ILT. In 2019 is een overleg geïnitieerd om de processen rondom bezwaarzaken verder af te stemmen en te optimaliseren.
O4	Kiwa beschikt niet over de terugkoppeling van alle bezwaarzaken.	Zie ook O3.
O5	Versiehistorie en geldigheidsduur ontbreken in het informatie beveiligings beleid.	Versiehistorie is aangebracht in het informatiebeveiligingsbeleid. Het informatiebeveiligingsbeleid van Kiwa Register kent geen ingeperkte geldigheidsduur. Het document is geldig zolang er geen nieuwe versie is.
O6	Inzicht in de voortgang en effectiviteit van individuele maatregelen vanuit de risicoanalyse ontbreekt (alleen beschikbaar op hoog abstractieniveau)	De risicoanalyse is uitgebreid en geactualiseerd specifiek voor de Boordcomputer Taxi processen en producten. Bij de implementatie van ISO27001 in 2020 zal Kiwa Register ook de risico's voor andere processen meer gedetailleerd beschrijven. De daaruit voortvloeiende maatregelen zullen jaarlijks gereviewd worden op effectiviteit.