



Inspectie Leefomgeving en Transport
Ministerie van Infrastructuur en Waterstaat

Toezichtrapportage 2021

Kiwa Register B.V

Datum	11 maart 2022
Status	definitief

Colofon

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

Rijnstraat 8 Den Haag

Auteurs

A. Visser en P. Willems

Versie

1.0

Colofon—2

1	Inleiding—4
1.1	Aanleiding—4
1.2	Achtergrondinformatie—4
2	Managementsamenvatting en conclusie—5
2.1	Conclusie—5
2.2	Compliance management—5
2.3	Kennis en competentie management—5
2.4	Risk management—5
2.5	Bevindingen—5
2.6	Samenwerking Kiwa—6
3	Doelstelling en scope van het toezicht—7
3.1	Doel van het toezicht—7
3.2	Toezichtlandschap—7
3.3	Informatieverstrekking door KIWA—7
4	Toezicht 2021—9
4.1	Auditscope—9
4.2	Audit diepgang—9
5	Auditaanpak 2021—10
5.1	Uitvoering van de jaarlijkse audit—10
5.2	Auditrapportage—10
6	Bevindingen ILT—11
6.1	Opvolgingen bevindingen voorgaande audit—11
6.2	Audits door externe toezichthouders—12
6.3	Interne audits—12
6.4	Kwaliteitsmanagement—13
6.4.1	Compliance management—13
6.4.2	Kennis en competentie management—14
6.4.3	Risicomanagement, met focus op ILT-gerelateerde producten—14
Bijlage A	Virtual Vaults- Index—16
Bijlage B	Terugkoppeling Kiwa op conceptrapportage—20

1 Inleiding

1.1 Aanleiding

Op 10 juli 2009 is de overeenkomst tussen Kiwa NV en de Staat der Nederlanden getekend (hierna "de overeenkomst"), waarin de overdracht van een aantal taken van Inspectie Verkeer en Waterstaat (nu Inspectie Leefomgeving en Transport (hierna ILT)) aan Kiwa NV is vastgelegd. Kiwa NV heeft voor de uitvoering van de taken een aparte juridische entiteit opgericht: Kiwa Register BV (hierna Kiwa). De ILT houdt namens de minister van Infrastructuur en Waterstaat (I&W) toezicht op de uitvoering van de gemandateerde taken door Kiwa NV en Kiwa.

1.2 Achtergrondinformatie

De overgedragen taken betreffen werkzaamheden op het gebied van Luchtvaart, Scheepvaart en Wegvervoer. De overdracht van taken betekent niet dat de ministeriële verantwoordelijkheid is vervallen. De eindverantwoordelijkheid voor de juiste uitvoering van de taken door Kiwa ligt bij de minister van Infrastructuur en Waterstaat. De verdeling van verantwoordelijkheden, de rollen en de taken tussen ILT en Kiwa zijn beschreven in de overeenkomst, addenda en brieven.

Naast de ILT houden drie Europese organisaties toezicht op Kiwa, dit zijn EMSA (scheepvaart), EASA (luchtvaart) en ERCA (Digitale tachograaf (DT) kaarten).

2 Managementsamenvatting en conclusie

2.1 Conclusie

De inspectie is van oordeel dat de kwaliteit van de taakuitvoering door Kiwa, op een aantal punten verbetering behoeft.

Met betrekking tot informatiebeveiliging heeft Kiwa verbeteringen doorgevoerd, wat heeft geresulteerd in een ISO27001 certificering van het ISMS.

2.2 Compliance management

In de aangeleverde documentatie is compliance management als proces niet beschreven. Daarnaast is niet alle gevraagde documentatie aangeleverd en zijn niet alle gestelde vragen over dit onderwerp beantwoord.

Wij kunnen daarom niet beoordelen of Kiwa inzichtelijk heeft aan welke wetgeving dient te worden voldaan en of Kiwa (in opzet) compliant is met deze wetgeving.

Met name kunnen wij niet beoordelen of Kiwa voldoet aan de archiefwet en de AVG.

2.3 Kennis en competentie management

Wij kunnen niet beoordelen of Kiwa te allen tijde over noodzakelijke capaciteit, kennis en deskundigheid beschikt voor een juiste uitvoering van de taken en voor zover toepasselijk aan deskundigheids- en opleidingsvereisten uit wet- en regelgeving en internationale verdragen voldoet (ref. 5.1.4). Dit omdat het proces voor het maken van functiebeschrijvingen met competenties niet beschikbaar is en omdat de functiebeschrijvingen hiervoor te algemeen zijn opgesteld.

2.4 Risk management

Het is niet mogelijk om te beoordelen of afdoende mitigerende maatregelen zijn getroffen om relevante risico's te beheersen. Omdat kennelijk geen gebruik is gemaakt van een standaardrisicoanalyse methode is evenmin geborgd dat alle relevante risico's zijn onderkend.

2.5 Bevindingen

Tijdens de audit deed de inspectie zes bevindingen:

2021B1:¹

2021B2:

Het onderzoek dat door Kiwa is uitgevoerd n.a.v. eerdere bevindingen (2018B1 en 2018B2), wijst uit dat de kwaliteit van het aanvraag en afgifte proces voor AML's en FCL's nog niet optimaal is geborgd. Een root cause analyse van de bevindingen uit 2018 heeft niet plaatsgevonden.

¹ De bevinding 2021B1 komt te vervallen. Het onderwerp "Wet openbaarheid van bestuur" moet nog tussen ILT en KIWA besproken worden. Het is van belang dat KIWA die informatie levert welke nodig is, om op een bij ILT ontvangen WOB verzoek te kunnen reageren.

2021B3:

Naar aanleiding van een eerdere bevinding (2018B4) heeft Kiwa het project "G2 implementatie tachograafkaarten" geëvalueerd. Wat ontbreekt aan deze evaluatie is een hoofdstuk "lessons learned". Het risico bestaat nu dat bij een volgend project gelijksoortige fouten worden gemaakt.

2021B4:

Interne audits resulteren in veel gevallen in kritische tekortkomingen (KT), tekortkomingen (T) of observaties (O). Ons is niet gebleken dat root cause analyses in alle gevallen waar nodig worden uitgevoerd.

2021B5:

Ons is niet gebleken dat de monitoring op acties voortkomend uit interne audits, effectief is. O.a.:

- *acties om tekortkomingen op te lossen staan vaak te lang open en;*
- *niet alle tekortkomingen zijn opgenomen in de Excel die wordt gebruikt om de voortgang te monitoren.*

2021B6:

Ons is niet gebleken dat door Kiwa expliciet wordt geaudit op opzet bestaan en werking van risico mitigerende maatregelen. Er wordt door Kiwa zwaar gesteund op de collegiale toetsing (CT's) en op eindtoetsen (ET's) die voor de verschillende productiestraten zijn beschreven (opzet). Het ligt voor de hand om op bestaan en werking van deze maatregelen te auditen.

2021B7:

Compliance Management is niet als apart proces beschreven. Het is daarnaast niet duidelijk op welke wijze Kiwa voldoet aan de wettelijke eisen. Het is met andere woorden niet duidelijk hoe non-compliance risico's worden beheerst.

2.6 Samenwerking Kiwa

De samenwerking met Kiwa als auditee kan als moeizaam worden geïdentificeerd. De beperkingen die het gebruik van virtual vaults (zie H3.3) met zich meebrengt heeft een negatief effect gehad op de efficiëntie van het uitgevoerde onderzoek. Kiwa was daarnaast niet bereid om een fysiek dossier op locatie in te richten.

3 Doelstelling en scope van het toezicht

3.1 Doel van het toezicht

Kiwa voert namens de minister van Infrastructuur en Waterstaat vergunningverlenende taken uit. Door middel van toezicht wordt vastgesteld of de uitvoering van de overgedragen taken en bevoegdheden in overeenstemming is met de geldende wet- en regelgeving, binnen de randvoorwaarden zoals omschreven in de overeenkomst. Hiermee krijgt de minister als eindverantwoordelijke inzicht of de uitvoering van de overgedragen taken door Kiwa voldoet aan gestelde eisen.

Omdat de werking niet wordt beoordeeld (zie H4.2) heeft deze audit niet zoals in voorgaande jaren, betrekking op één specifiek uitvoeringsjaar. De uitvoering van deze audit heeft daarom tot doel om de huidige status te beoordelen van de objecten die binnen de scope van deze audit vallen.

3.2 Toezichtlandschap

Het toezicht omvat de uitvoering van de geldende wet- en regelgeving (waaronder de Algemene Wet Bestuursrecht) en de naleving van de overeenkomst tussen de ILT en Kiwa, en is gericht op het borgen van de continuïteit en kwaliteit van de taakuitvoering. Twee elementen die hier van belang zijn, zijn de inhoudelijke taakuitvoering en de bedrijfsvoering.

3.3 Informatieverstrekking door KIWA

In het Informatieprotocol (bijlage I bij de overeenkomst) en de addenda is vastgelegd welke informatie door Kiwa tenminste aan de ILT ter beschikking gesteld moet worden. De informatie in het Informatieprotocol dient voor de uitvoering van de Inspectietaken en geeft tegelijkertijd input voor de invulling van het toezicht. De kwaliteit van de beschikbare informatie is medebepalend voor de richting en diepgang van de toezichtactiviteiten.

De ILT hanteert het proportionaliteitsbeginsel en het principe van doelbinding, d.w.z. dat zij haar informatieverzoeken beperkt tot die informatie die nodig is om een oordeel te kunnen geven over de kwaliteit en continuïteit van taakuitvoering en het nakomen van de gemaakte afspraken. De ILT is zich bewust van het feit dat met het verkrijgen van extra informatie ten behoeve van het toezicht ook bedrijfsspecifieke en soms privacygevoelige informatie wordt verstrekt. De ILT gaat op zorgvuldige wijze om met deze gegevens, met inachtneming van de relevante wet- en regelgeving en de afspraken in de overeenkomst.

Kiwa stelt de door de ILT gevraagde documentatie beschikbaar door deze in een zogenaamde virtual vaults te plaatsen. Via deze virtual vaults kan steeds één document worden ingezien, tekst kan niet worden gekopieerd, er kan geen print screen worden gemaakt en de zoekfunctie voor het doorzoeken van een document werkt niet. Tenslotte hebben de ILT inspecteurs een geheimhoudingsverklaring moeten tekenen om toegang tot de vaults te kunnen krijgen. Alle handelingen van de ILT inspecteurs worden gelogd.

Opmerking

De beperkingen die het gebruik van virtual vaults met zich meebrengt heeft een negatief effect op de efficiëntie van het uitgevoerde onderzoek. Daarbij is ons gebleken dat voor BSI, die de ISO9001 en ISO27001 certificeringen heeft uitgevoerd, documentatie zonder meer ter beschikking is gesteld. BSI heeft alleen hoeven te verklaren dat na afronding van de audit documentatie zou worden verwijderd van laptops en smartphones.

4 Toezicht 2021

4.1 Auditscope

Voor het bepalen van de auditscope is o.a. gebruik gemaakt van door de ILT verzamelde signalen over de taakuitvoering en de bedrijfsvoering Kiwa en van input die is aangeleverd door het ILT programma inspectie en certificering.

De daadwerkelijke scope is tijdens het onderzoek beperkt omdat vragen over compliance management, kennismanagement en risicomanagement niet of niet tijdig) zijn beantwoord en de hierover gevraagde documentatie niet of niet tijdig is aangeleverd.

De auditscope is als volgt:

- A. De opvolging van auditbevindingen uit de audit over 2018;
- B. De audits door externe toezichthouders;
- C. Interne audits 2020 en 2021;
- D. Kwaliteitmanagement:
 - i. Compliance management;
 - ii. Kennismanagement;
 - iii. Risicomanagement, met focus op ILT-gerelateerde producten.

Kiwa dient op basis van de overeenkomst voor *alle* processen ISO 9001 (of vergelijkbaar) gecertificeerd te zijn. Er zal zoveel mogelijk gebruik worden gemaakt van de resultaten van de uitgevoerde ISO 9001 certificering (Overeenkomst, bijlage 4.2.d).

4.2 Audit diepgang

De diepgang van de audit is beperkt tot opzet en bestaan van genomen beheersmaatregelen die betrekking hebben op de objecten die binnen de scope vallen. Het bestaan is daarbij selectief getoetst. Op de werking is niet getoetst.

Onder opzet verstaan wij het definiëren en documenteren van maatregelen. Bestaan wordt vastgesteld als een maatregel voor één willekeurig geval is uitgevoerd. Bij het vaststellen van de werking wordt over een vastgestelde periode een representatieve steekproef genomen waarbij wordt getoetst of de maatregel voor alle gevallen uit de steekproef is uitgevoerd.

Bestaan kan niet worden beoordeeld indien de opzet niet voldoet of als documentatie over de opzet ontbreekt.

5 Auditaanpak 2021

5.1 Uitvoering van de jaarlijkse audit

De ILT heeft in de maand december 2021 de toezichtactiviteiten uitgevoerd.

Een belangrijk deel van het toezicht heeft plaatsgevonden op basis van analyses van informatie die Kiwa heeft aangeleverd, w.o.:

- de rapportages van de externe toezichthouders;
- interne audits;
- vastleggingen van de uitgevoerde certificeringen voor ISO27001 en ISO9001;
- procesbeschrijvingen;
- werkinstructies;
- documentatie kwaliteitsmanagementsysteem.

5.2 Auditrapportage

De ILT heeft 29-12-2021 een conceptrapportage van de audit opgeleverd. Deze rapportage is met Kiwa gedeeld met het oogmerk overeenstemming te hebben over de geconstateerde feiten.

6 Bevindingen ILT

6.1 Opvolgingen bevindingen voorgaande audit

Kiwa heeft een *corrective action report* (CAR) opgesteld op basis van de uitkomsten van de audit over 2018. De inspectie heeft de effectiviteit van de genomen maatregelen beoordeeld.

Bevindingen 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.

Onderzoek van Kiwa heeft uitgewezen dat:

- veel fouten worden veroorzaakt door onnauwkeurigheid tijdens de verwerking en;
- controlestappen (nog) niet worden afgedwongen door de geautomatiseerde systemen (o.a. Jump). De keuze om life te gaan met een minimale variant van Jump (waarbij er nog geen gedwongen beoordelingsproces is) is bewust genomen, n.l. omdat van het oude systeem (Flare) de continuïteitsrisico's te groot werden geacht (ref 2.1.3);
- het afgelopen jaar het aantal buitenlandse aanvragen exponentieel is toegenomen en daarom is de werkwijze voor buitenlandse aanvragen aangescherpt.

2021B2:

Het Kiwa onderzoek wijst uit dat de kwaliteit van het aanvraag en afgifte proces voor AML's en FCL's nog niet optimaal is geborgd. Een root cause analyse van de bevindingen uit 2018 heeft niet plaatsgevonden.

Bevinding 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.

Kiwa is inmiddels ISO27001 gecertificeerd door BSI, een certificaat is afgegeven d.d. 27-07-2021. Kiwa heeft hiermee aangetoond dat het in opzet beschikt over een ISMS (Information Security Management System).

Tijdens de certificering heeft BSI 12 minor non-conformities vastgesteld. Vanwege deze non-conformities is in oktober een follow up audit uitgevoerd door BSI die succesvol is afgerond.

Conclusie:

Wij feliciteren Kiwa met de behaalde certificering.

Bevinding 2018B4:

Een gedegen onderzoek naar de oorzaken waardoor de gevraagde tachograafkaarten (n.a.v. overgang naar 2e generatie digitale tachograaf), niet tijdig konden worden geleverd, is nog niet uitgevoerd.

Er heeft een evaluatie plaatsgevonden door Kiwa van het project "G2 implementatie tachograafkaarten", waarbij een chronologisch overzicht is gegeven van gemaakte fouten, onvoorziene problemen en de daaropvolgende op ad hoc basis gemaakte aanpassingen.

2021B3:

Wat ontbreekt aan de evaluatie van het project "G2 implementatie tachograafkaarten" is een hoofdstuk "lessons learned". Het risico bestaat nu dat bij een volgend project gelijksoortige fouten worden gemaakt.

6.2 Audits door externe toezichthouders

Er zijn een aantal externe onderzoeken uitgevoerd door externe toezichthouders in de periode vanaf 2019:

- 2020: ISO 9001:2015;
- 2020/2021: ISO 27001-2013 ;
- 2020: ETSI audit 319-401/411-1/411-2/ Netsec en PKIo 4.8 ;
- 2021 :ETSI audit 319-401/411-1/411-2/ Netsec en PKIo 4.9 and ISO 9001:2015.

CAP opvolging ISO 27001 en ETSI worden bijgehouden in het document: "Voortgang CAP (KIWA en ketenpartijen)". De opvolging van ETSI CAP wordt maandelijks gedeeld met ILT en besproken.

Verbeterpunten worden uitgezet in de organisatie of bij de ketenpartner. Monitoring vindt plaats door de Compliance Manager en Security Officer. Afwijkingen worden opgenomen in de standaard rapportages en besproken in de Quality Board en/of de periodieke overleggen met ketenpartners. Door de externe toezichthouders zijn geen ernstige tekortkomingen geconstateerd en verbeteracties worden in opzet in voldoende mate opgevolgd.

6.3 Interne audits

Er zijn in totaal vijf auditoren: drie bij de afdeling Compliance behorend bij Unit product management en Compliance en twee bij afdeling Kwaliteitstoetsing, een onderdeel van de unit Operations. De kwaliteitstoetsers doen voornamelijk productaudits.

Het auditjaarplan wordt in opzet jaarlijks als onderdeel van het driejarenplan opgesteld door de Compliance manager, Security officer en Kwaliteitstoetsing (Operations) en vastgesteld door het Q-board. ISO onderwerpen en processen worden afhankelijk van risico-profiel binnen een driejarencyclus jaarlijks, tweejaarlijks of driejaarlijks geaudit.

Interne auditbevindingen zoals tekortkomingen en opmerkingen worden vastgelegd door de interne auditoren in Excel. Hier wordt op gemonitord door de Compliance manager en de afdeling Kwaliteitstoetsing.

Aanbevelingen worden opgenomen in het auditrapport; de desbetreffende afdeling maakt hierin een keuze deze wel of niet op te volgen; bij aanbevelingen is geen sprake van verplichte opvolging zoals bij tekortkomingen.

De interne audits worden systematisch uitgevoerd conform een vooraf opgesteld jaarplan. Hierbij worden relevante tekortkomingen gerapporteerd. Tekortkomingen worden regelmatig niet onderzocht op root cause, de geconstateerde fout wordt dan hersteld door een correctieve actie maar de kans op herhaling wordt hierdoor niet kleiner. Een voorbeeld is role based access control en verwijderen van bevoegdheden bij uitdiensttreding (ref 4.2.9).

Uit de auditrapportages blijkt verder dat pas bij een volgende audit de opvolging van een geconstateerde tekortkoming wordt beoordeeld. In die gevallen blijkt regelmatig dat er geen of niet voldoende voortgang is geboekt (zie b.v. ref 4.1.4).

De Excel (ref 1.9.1 C3) waarin alle tekortkomingen worden geregistreerd wordt niet volledig ingevuld. De kolom "analyse van de grondoorzaak en de omvang van het probleem" wordt bijvoorbeeld nauwelijks ingevuld, hetzelfde geldt voor de kolom "verificatiedatum (uiterlijk) of status". De kolom "resterende looptijd bevat regelmatig een negatief getal, wat betekent dat de verbeteracties op achterstand staan. Acties dienen binnen 90 dagen te worden opgelost. Ongeveer 2/3 van de acties staat op een achterstand van 80 tot 127 dagen. Ook is gebleken dat in elk geval enkele kritische tekortkomingen niet in de Excel zijn opgenomen (KT-21-03-01, KT-21-03-02 en KT-21-03-03 uit ref 4.2.5).

Er wordt gerapporteerd aan de Q-board d.m.v. de "Dashboard Compliance" (ref 2.6.1, 2.6.2, 2.6.3) maar hierin wordt niet gerapporteerd over de status van de in de Excel opgenomen acties.

2021B4:

Ons is niet gebleken dat root cause analyses in alle gevallen waar nodig worden uitgevoerd.

2021B5:

Ons is niet gebleken dat de monitoring op acties voortkomend uit interne audits, effectief is. O.a.:

- *acties om tekortkomingen op te lossen staan regelmatig te lang open en;*
- *niet alle tekortkomingen zijn opgenomen in de Excel die wordt gebruikt om de voortgang te monitoren.*

2021B6:

Ons is niet gebleken dat expliciet wordt geaudit op opzet bestaan en werking van risico mitigerende maatregelen. Er wordt door Kiwa zwaar gesteund op de collegiale toetsing (CT's) en op eindtoetsen (ET's) die voor de verschillende productiestraten zijn beschreven (opzet). Het ligt voor de hand om op bestaan en werking van deze maatregelen te auditen.

6.4 Kwaliteitsmanagement

De documentatie van het kwaliteitsmanagement bestaat uit het Topdocument en de documentatie van de kernprocessen en sub-processen. In documentatie van de sub-processen staan verwijzingen naar ondersteunende documenten zoals Werkinstructies. De werkinstructie zijn deels bij de audit betrokken.

De scope en de diepgang van de door BSI uitgevoerde ISO 9001 certificering verschilt met de scope van ILT. Hierdoor kan slechts in beperkte mate gebruik gemaakt worden van de resultaten van de uitgevoerde ISO 9001 certificering. De door BSI gerapporteerde toetsing wordt daarom onvoldoende geacht om op te kunnen steunen voor deze audit.

Kiwa heeft de gevraagde documentatie niet of niet tijdig aangeleverd waardoor de opzet van het kwaliteitsmanagement slechts in beperkte mate kon worden beoordeeld.

6.4.1 Compliance management

In de aangeleverde documentatie is compliance management als proces niet beschreven. Daarnaast is niet alle gevraagde documentatie aangeleverd en zijn de aldaar gestelde vragen niet beantwoord.

Conclusie

Wij kunnen niet beoordelen of Kiwa inzichtelijk heeft aan welke wetgeving dient te worden voldaan en of Kiwa (in opzet) compliant is met deze wetgeving.

Met name kunnen wij niet beoordelen of Kiwa voldoet aan de archiefwet en de AVG. Onder andere hebben wij de volgende vragen niet kunnen beantwoorden:

1. Worden de juiste bewaartermijnen gehanteerd en wordt daarin rekening gehouden met eventuele beroepszaken?
2. Welke informatie wordt gearchiveerd in overeenstemming met de archiefwet (archiveren of verwijderen doe je na verstrijken van de bewaartermijn).
3. Welke informatie over personen wordt wel/niet gearchiveerd vanwege de AVG?
4. Wie is eigenaar van de betrokken gegevens en wie is eventueel verwerker? Eigenaarschap van de vergunning(houder) database is van belang voor de taakverdeling met betrekking tot de AVG en Archiefwet.

2021B7:

Compliance Management is niet als apart proces beschreven. Het is daarnaast niet duidelijk op welke wijze Kiwa voldoet aan de wettelijke eisen. Het is met andere woorden niet duidelijk hoe non-compliance risico's worden beheerst.

6.4.2 Kennis en competentie management

In de aangeleverde documentatie is kennis/competentiemanagement als proces niet beschreven. Daarnaast is de gevraagde documentatie niet of niet tijdig aangeleverd en zijn de aldaar gestelde vragen niet of niet tijdig beantwoord.

In de audit-heatmap Q4 (ref 4.2.16) wordt gesteld dat Operations & IT een competentie-matrix heeft opgesteld maar dat deze echter nog niet volledig is ingevuld.

Er zijn functiebeschrijvingen beschikbaar met bijbehorende competenties voor medewerker vergunningverlening (deze geldt voor bijna alle af te geven vergunningen) en voor specialist producten en processen (ref 5.2.2.2 en 5.2.2.1).

Conclusie:

Wij kunnen niet beoordelen of Kiwa te allen tijde over noodzakelijke capaciteit, kennis en deskundigheid beschikt voor een juiste uitvoering van de taken en voor zover toepasselijk aan deskundigheids- en opleidingsvereisten uit wet- en regelgeving en internationale verdragen voldoet (ref. 5.1.4). Dit omdat het proces voor het maken van functiebeschrijvingen met competenties niet beschikbaar is en omdat de functiebeschrijving hiervoor te algemeen zijn opgesteld.

6.4.3 Risicomanagement, met focus op ILT-gerelateerde producten

Er zijn twee maatregelen van interne controle beschreven, de collegiale toetsing die in verschillende processen is geïmplementeerd (als steekproef of als 100% controle) en de zogenaamde eindtoets. Er is echter geen koppeling aangetroffen tussen de onderkende risico's en de daar bijbehorende mitigerende maatregelen. Het is daarom niet vast te stellen of alle risico's zijn onderkend (en dus) of alle noodzakelijke maatregelen zijn genomen en wat de restrisico's zijn.

Fraudebeheersing is één van de kernprocessen (ref 1.4.3). Dit proces beschrijft voornamelijk welke handelingen moeten worden verricht nadat een fraude is geconstateerd. Preventieve maatregelen die zijn beschreven, zijn van algemene aard (b.v. VOG, fysieke beveiliging en dergelijke). Expliciete maatregelen om fraude te voorkomen of te detecteren zijn niet aangetroffen (zoals bijvoorbeeld verbandscontroles op de voorraad waarde documenten of integriteitscontroles op het verwerkingsproces).

Er is documentatie beschikbaar (ref. 1.4.8.x) waarin Risicofactoren en Beheersmaatregelen zijn beschreven. Deze documenten zijn niet gedateerd en het is niet duidelijk op welke wijze deze tot stand zijn gekomen. Het is m.a.w. niet duidelijk of en zo ja welk risicoanalyse methode is toegepast. Verder zijn van de risico's de kans en impact niet bepaald.

Conclusie

Risicobeheer of risicomangement is een *continu proces* dat ten aanzien van de (strategische) doelstelling risico's identificeert, beoordeelt en vervolgstappen definieert. Een vervolgstap kan zijn het implementeren van een risico mitigerende maatregel maar ook het accepteren van het risico.

Het is niet mogelijk om te beoordelen of afdoende mitigerende maatregelen zijn getroffen om relevante risico's te beheersen. Omdat kennelijk geen gebruik is gemaakt van een standaardrisicoanalyse methode is evenmin geborgd dat alle relevante risico's zijn onderkend

Bijlage A Virtual Vaults- Index

INDEX	TITLE	DATE VISIBLE
1	Algemene documenten	03-Dec-2021 12:36 CET
1.1	Topdocument QMS Kiwa Register V2	03-Dec-2021 12:36 CET
1.2	ISMS KIWA-Register 2021-01 V1.2	03-Dec-2021 12:36 CET
1.3	Antwoorden Kiwa Toezichtsprogramma 2021v1	10-Dec-2021 10:50 CET
1.4	Kernproces	13-Dec-2021 10:13 CET
1.4.1	Kernproces Register versie 29102021_part1a	03-Dec-2021 12:36 CET
1.4.2	Kernproces Register versie 29102021_part1b	03-Dec-2021 12:36 CET
1.4.3	Kernproces Register versie 29102021_part2a	03-Dec-2021 12:36 CET
1.4.4	Kernproces Register versie 29102021_part2b	03-Dec-2021 12:36 CET
1.4.5	Kernproces Register versie 29102021_part3	03-Dec-2021 12:36 CET
1.4.6	Kernproces Register versie 29102021_part4	03-Dec-2021 12:36 CET
1.4.7	Processchema's	14-Dec-2021 12:06 CET
1.4.7.1	1.1 Boordcomputerkaarten regulier proces	14-Dec-2021 12:06 CET
1.4.7.2	1.1 Boordcomputerkaarten intrekking	14-Dec-2021 12:06 CET
1.4.7.3	1.3 Smart Tachograafkaarten proces	14-Dec-2021 12:12 CET
1.4.7.4	1.4 Scheepvaart proces	14-Dec-2021 12:13 CET
1.4.7.5	1.7 Express Service	14-Dec-2021 12:44 CET
1.4.7.6	2.1 Bezwaar en beroep	14-Dec-2021 12:47 CET
1.4.7.7	2.2 Klachten en claims	14-Dec-2021 12:49 CET
1.4.7.8	2.5 Wettelijke wijz vern verbt P&P	14-Dec-2021 12:55 CET
1.4.7.9	2.6.1 Buiten beh stelling	14-Dec-2021 13:03 CET
1.4.7.10	2.6.2 Afwijzen	14-Dec-2021 13:08 CET
1.4.7.11	2.6.3 Intrekken	14-Dec-2021 13:08 CET
1.4.7.12	3.5 Projectmanagement	14-Dec-2021 13:12 CET
1.4.7.13	4.2 Gebruikersondersteuning	14-Dec-2021 13:19 CET
1.4.7.14	4.3 Muteren autorisaties	14-Dec-2021 13:26 CET
1.4.7.15	4.1.1. Wensenproces_RegisterApplicaties	14-Dec-2021 13:39 CET
1.4.7.16	4.1.2. Wijzigingenproces_RegisterApplicaties	14-Dec-2021 13:39 CET
1.4.7.17	4.1.3. Releaseproces_RegisterApplicaties	14-Dec-2021 13:39 CET
1.4.7.18	4.10 Procedure uitgifte tags	14-Dec-2021 13:52 CET
1.4.8	KPI's en risico's per proces	21-Dec-2021 16:10 CET
1.4.8.1	KPI, risico's 2.5 WWWPP	21-Dec-2021 16:13 CET
1.4.8.2	KPI, risico's 2.2 K&C	21-Dec-2021 16:13 CET
1.4.8.3	KPI, risico's 2.1 B&B	21-Dec-2021 16:13 CET
1.4.8.4	KPI, risico's 1.8 DK	21-Dec-2021 16:13 CET
1.4.8.5	KPI, risico's 1.7 ES	21-Dec-2021 16:13 CET
1.4.8.6	KPI, risico's 1.6 BGvv	21-Dec-2021 16:13 CET
1.4.8.7	KPI, risico's 1.5.1 IV	21-Dec-2021 16:13 CET
1.4.8.8	KPI, risico's 1.5 OV	21-Dec-2021 16:13 CET
1.4.8.9	KPI, risico's 1.4.1. BV	21-Dec-2021 16:13 CET
1.4.8.10	KPI, risico's 1.4 SV	21-Dec-2021 16:13 CET
1.4.8.11	KPI, risico's 1.3 DTST	21-Dec-2021 16:13 CET

INDEX	TITLE	DATE VISIBLE
1.4.8.12	KPI, risico's 1.2 LV	21-Dec-2021 16:13 CET
1.4.8.13	KPI, risico's 1.1 BCT	21-Dec-2021 16:13 CET
1.5	Werkinstructies	13-Dec-2021 10:14 CET
1.5.1	Land	13-Dec-2021 10:14 CET
1.5.1.1	W-G 1.0 Werkinstructie en gebruikersinstructie Land	13-Dec-2021 10:20 CET
1.5.2	Luchtvaart	13-Dec-2021 10:15 CET
1.5.2.1	W 1.2.1-01 Werkinstructie Luchtvaart	13-Dec-2021 10:20 CET
1.5.3	Binnenvaart	13-Dec-2021 10:15 CET
1.5.3.1	Jump W 14-8 Rijnvaartverklaring Concept versie 0.11	13-Dec-2021 10:21 CET
1.5.4	Scheepvaart	13-Dec-2021 10:15 CET
1.5.4.1	Punten ter controle bij het Collegiale Toetsen van aanvragen Scheepvaart	13-Dec-2021 11:22 CET
1.5.5	DCP document	14-Dec-2021 15:39 CET
2	Opvolging auditbevindingen 2018	03-Dec-2021 12:36 CET
2.1	A1	03-Dec-2021 12:36 CET
2.1.1	211106_Beleid verificatie Part-66 v1.2	10-Dec-2021 09:45 CET
2.1.2	210624_Aannamebeleid aanvragen Part-66 v1.0	10-Dec-2021 09:45 CET
2.1.3	210420_StaVaZa Afdwingen Controle Stappen JUMP	10-Dec-2021 09:45 CET
2.1.4	200528_Onderzoek_nav_reality_check_LV	10-Dec-2021 09:45 CET
2.1.5	190924_Teamoverleg_Luchtvaart	10-Dec-2021 09:45 CET
2.2	A2	03-Dec-2021 12:36 CET
2.2.1	zie map Externe toezichthouders	10-Dec-2021 09:46 CET
2.3	A3	10-Dec-2021 09:45 CET
2.3.1	210504_Evaluatie_DTG2	10-Dec-2021 09:48 CET
2.4	B1	10-Dec-2021 09:49 CET
2.4.1	Zie map Externe toezichthouders	10-Dec-2021 09:50 CET
2.5	B2	10-Dec-2021 09:50 CET
2.5.1	B2_Voortgang_CAP (Kiwa en Ketenpartners) (Let op! 3 tabbladen)	10-Dec-2021 10:13 CET
2.6	B3	10-Dec-2021 10:13 CET
2.6.1	B3_maandrapportage QBoard september 2021	10-Dec-2021 10:15 CET
2.6.2	B3_Dashboard_Compliance_sep_2021	10-Dec-2021 10:15 CET
2.6.3	B3_Dashboard_Compliance_aug_2021	10-Dec-2021 10:15 CET
2.6.4	B3_211118_Notulen_PKIo-overleg_TSP	10-Dec-2021 10:15 CET
2.6.5	B3_211028_Notulen ketenoverleg	10-Dec-2021 10:15 CET
2.7	C1	10-Dec-2021 10:16 CET
2.7.1	C1_W 20-1 Werkinstructie Interne audits 091221	10-Dec-2021 09:38 CET
2.7.2	C1_Besluitenlijst_Q-Board	10-Dec-2021 10:28 CET
2.8	C2	10-Dec-2021 10:21 CET
2.8.1	Zie map Interne audits	10-Dec-2021 10:29 CET
2.9	C3	10-Dec-2021 10:21 CET
2.9.1	C3_Openstaande_bevindingen	10-Dec-2021 09:38 CET
2.10	C4	10-Dec-2021 10:30 CET
2.10.1	Zie C1 W20-1 Werkinstructie Interne audits	10-Dec-2021 10:31 CET
3	Audits door Externe Toezichthouders	03-Dec-2021 12:36 CET
3.1	ETSI BSI BCT	03-Dec-2021 12:36 CET
3.1.1	PKI-ETSI_Notitie_CAP_opvolging	03-Dec-2021 12:36 CET
3.1.2	PKI-ETSI_CAP_sep21_AKK_LA	03-Dec-2021 12:36 CET
3.1.3	PKI-ETSI_BSI_Auditrapport_sep21_v10_FINAL	03-Dec-2021 12:36 CET
3.1.4	PKI-ETSI_BSI_Auditrapport_mar21_NCR_v1.0	03-Dec-2021 12:36 CET

INDEX	TITLE	DATE VISIBLE
3.1.5	Mail BSI inzake re-issue certificate 2021-2023	03-Dec-2021 12:36 CET
3.1.6	Certificaat_BSI_ETSI-411-2_2019-2021	03-Dec-2021 12:36 CET
3.1.7	Certificaat_BSI_ETSI-411-1_2019-2021	03-Dec-2021 12:36 CET
3.1.8	Ecertificate - ETS 017 - 2021-2023	20-Dec-2021 09:41 CET
3.1.9	Ecertificate - ETS 040- 2021-2023	20-Dec-2021 09:41 CET
3.2	ISO 27001	03-Dec-2021 12:36 CET
3.2.1	ISO27001_Statement_of_Applicablitiy_v2	03-Dec-2021 12:36 CET
3.2.2	ISO27001_CAP_v1_Input Ismail_WB_20210621_update	03-Dec-2021 12:36 CET
3.2.3	ISO27001_BSI_Certificaat_2021_2024	03-Dec-2021 12:36 CET
3.2.4	ISO27001_BSI_Auditrapport_20201218	03-Dec-2021 12:36 CET
3.3	ISO 9001	03-Dec-2021 12:36 CET
3.3.1	ISO9001_Certificaat_2018_2021	03-Dec-2021 12:36 CET
3.3.2	ISO9001_BSI_Auditplan_2021	03-Dec-2021 12:36 CET
3.3.3	ISO9001_BSI_Auditrapport_20210216	03-Dec-2021 12:36 CET
3.4	Voorbeeld opvolging CAP	03-Dec-2021 12:36 CET
4	Interne audits	03-Dec-2021 12:36 CET
4.1	2020	03-Dec-2021 12:36 CET
4.1.1	Auditplanning_2020	03-Dec-2021 12:36 CET
4.1.2	2020-101 BCT Regulier Product Proces	03-Dec-2021 12:36 CET
4.1.3	2020-102 2020-02 BCT Intrekkingen	03-Dec-2021 12:36 CET
4.1.4	2020-103 Auditrapport FCL	03-Dec-2021 12:36 CET
4.1.5	2020-104 Auditrapport BCT Product	03-Dec-2021 12:36 CET
4.1.6	2020-105 Auditrapport BCT Intrekkingen	03-Dec-2021 12:36 CET
4.1.7	2020-03 Auditrapport QMS Systeemaudit ISO 9001	03-Dec-2021 12:36 CET
4.1.8	2020-04 II-III Verslag Follow up audit CAP ERCA 2019 20200729 v1	03-Dec-2021 12:36 CET
4.1.9	2020-04 Auditrapport DT-ST	03-Dec-2021 12:36 CET
4.1.10	2020-05 Auditrapport TWS PKI-ETSI	03-Dec-2021 12:36 CET
4.1.11	2020-06 TWS auditrapport augustus 2020 v1.1	03-Dec-2021 12:36 CET
4.1.12	2020-07 Auditrapport Wensen wijzigingen releases	03-Dec-2021 12:36 CET
4.1.13	2020-08 Auditrapport Projectmanagement	03-Dec-2021 12:36 CET
4.1.14	2020-12 Auditrapport Leveranciersmanagement	03-Dec-2021 12:36 CET
4.1.15	2020-15 Auditrapport Self-serviceportal	03-Dec-2021 12:36 CET
4.1.16	2020-16 Auditrapport Topicaudit ISMS v1.0	03-Dec-2021 12:36 CET
4.2	2021	03-Dec-2021 12:36 CET
4.2.1	Auditplanning_2021 (1)	03-Dec-2021 12:36 CET
4.2.2	2021-01 QMS9001 systeemaudit	03-Dec-2021 12:36 CET
4.2.3	2021-02 BCT Proces	03-Dec-2021 12:36 CET
4.2.4	2021-03 Axians Compliance	03-Dec-2021 12:36 CET
4.2.5	2021-05 Auditrapport AML go live JUMP	03-Dec-2021 12:36 CET
4.2.6	2021-06 BCT Intrekkingen	03-Dec-2021 12:36 CET
4.2.7	2021-12 BCM	03-Dec-2021 12:36 CET
4.2.8	2021-13 TWS auditrapport juni 2021 V1.0 signed	03-Dec-2021 12:36 CET
4.2.9	2021-15 Vierkantstelling_2021Q1	03-Dec-2021 12:36 CET
4.2.10	2021-18 Vierkantstelling_2021Q2	03-Dec-2021 12:36 CET
4.2.11	2021-19 Vierkantstelling_2021Q3	03-Dec-2021 12:36 CET
4.2.12	2021-20 Mandatering BCT kaarten	03-Dec-2021 12:36 CET
4.2.13	2021-101 BCT Product	03-Dec-2021 12:36 CET
4.2.14	2020-106 ONV-B Product rapportage - definitief	03-Dec-2021 12:36 CET

INDEX	TITLE	DATE VISIBLE
4.2.15	2020-106 ONV-T Product rapportage - definitief	03-Dec-2021 12:36 CET
4.2.16	Audit-heatmap 2021 Q4	03-Dec-2021 12:36 CET
4.2.17	2021-02 Auditrapport BCT Proces_Collegiale Toets	22-Dec-2021 18:37 CET
5	Kwaliteitsmanagement en compliance	03-Dec-2021 12:36 CET
5.1	Compliance management	03-Dec-2021 12:36 CET
5.1.1	Archiefwet - AVG	03-Dec-2021 12:36 CET
5.1.1.1	Privacy Statement Kiwa Register def 2.0	22-Dec-2021 18:44 CET
5.1.1.2	211222_Kiwa_Register_Processen APQCc023456	22-Dec-2021 18:44 CET
5.1.1.3	19-31 Auditrapport topicaudit Beh. persoonsgegevens definitief incl. CAR	22-Dec-2021 18:44 CET
5.1.1.4	Informatiebeveiligingsbeleid v.3.1. vastgesteld	22-Dec-2021 18:44 CET
5.1.1.5	PIA Kiwa Register_AML C0.1_122020	22-Dec-2021 18:44 CET
5.1.1.6	PIA Kiwa Register_Rijnvaart concept v.0.1_072020	22-Dec-2021 18:44 CET
5.1.1.7	Contractregister Kiwa Register V1.0	22-Dec-2021 18:44 CET
5.1.1.8	210709_Besluit 36 Privacy Officer	22-Dec-2021 18:44 CET
5.1.2	210909_Compliance manager definitief	22-Dec-2021 18:42 CET
5.1.3	211124_mail interim compliance manager	22-Dec-2021 18:42 CET
5.1.4	211119_Overzicht_Wet_en_Regelgeving	22-Dec-2021 18:42 CET
5.1.5	201214_Roadmap_Wetswijzigingen_v05	22-Dec-2021 18:42 CET
5.1.6	201228_RE EASA 23-12-2020 Publicatie Commission Implementing Regulation (EU) 20202193 Flight crew competence and training methods	22-Dec-2021 18:42 CET
5.1.7	171026_W 25-1 Werkinstructie actiepunten wijziging wetgeving	22-Dec-2021 18:42 CET
5.2	Kennismanagement	03-Dec-2021 12:36 CET
5.2.1	Handboeken en productbronboeken	03-Dec-2021 12:36 CET
5.2.2	Inwerktraject onboardingsproces	03-Dec-2021 12:36 CET
5.2.2.1	Medewerker Vergunningverlening fube met competenties	22-Dec-2021 18:48 CET
5.2.2.2	Specialist Producten en Processen fube met competenties	22-Dec-2021 18:48 CET
5.2.3	Opleidingsplan	03-Dec-2021 12:36 CET
5.2.3.1	211101_Overzicht_Opleidingsplan 2021 - anoniem	22-Dec-2021 18:46 CET
5.2.3.2	Kiwa_Performance_Management versie januari 2019	22-Dec-2021 18:47 CET
5.2.3.3	KIWA academy	22-Dec-2021 18:47 CET
5.2.3.4	KIWA security opleiding	22-Dec-2021 18:47 CET
5.2.3.5	Rapport 9001 hercertificering 2021	22-Dec-2021 18:47 CET
5.3	Risicomanagement	03-Dec-2021 12:36 CET
5.4	211222_Antwoorden Kiwa Toezichtsprogramma 2021v1	22-Dec-2021 18:55 CET

Bijlage B Terugkoppeling Kiwa op conceptrapportage

Hst/paragraaf	Feitelijke onjuistheden (te corrigeren tekst)	Argumentatie/onderbouwing van uw reactie	Toelichting ILT
2.1 Conclusie	Vaststelling ontbreekt dat Kiwa gesteld staat voor de opgedragen taken en dat de kwaliteit en de continuïteit van de taakuitvoering involdoende mate geborgd zijn	Vorige audit heeft ILT geoordeeld dat Kiwa gesteld staat voor de opgedragen taken en dat de kwaliteit en de continuïteit van de taakuitvoering in voldoende mate geborgd zijn, ondanks bevindingen. Kiwa Register is inmiddels extra gecertificeerd (conform ISO 27001) en toch onthoudt ILT zich nu van die vaststelling. Er zijn geen kritieke bevindingen gerapporteerd. Kiwa is van mening dat de huidige conceptrapportage onterecht het beeld wekt dat Kiwa een slechtere kwaliteit levert dan in 2018/2019. Of zijn de normen veranderd?	KIWA is van mening dat het concept rapport het beeld wekt dat KIWA slechtere kwaliteit levert dan in 2018/2019. ILT zegt in de conclusie van 2.1 dat voor de taakuitvoering door KIWA op een aantal punten verbetering behoeft. In de voorbereiding en tijdens de audit is gebleken dat niet alle relevante documentatie tijdig voorhanden was om in het kader van de audit een beoordeling te kunnen uitvoeren. Voor meerdere documentatie was de versie datum niet te achterhalen. Wanneer er sprake is van een goed werkend kwaliteitssysteem verwacht ILT dat op vrij korte termijn de relevante documenten kunnen worden aangeleverd. <u>De reactie van KIWA geeft geen aanleiding om de tekst aan te passen.</u>
2.6 Samenwerking Kiwa; 3.3 Informatieverstrekking door Kiwa	De beperkingen die het gebruik van virtual vaults (zie H3.3) met zich meebrengt heeft een negatief effect gehad op de efficiëntie van het uitgevoerde onderzoek.	ILT geeft aan dat de beperkingen die het gebruik van virtual vaults met zich meebrengt een negatief effect hebben op de efficiëntie van het uitgevoerde onderzoek. Bij de audit over 2018, uitgevoerd in 2020, bij het begin van de coronatijd, was ILT echter wel tevreden met deze werkwijze. Ook in 2021 hadden we te maken met specifieke maatregelen (een lockdown) a.g.v. Corona. Kiwa wil benadrukken dat zij alle relevante documentatie ter beschikking heeft gesteld aan ILT voor zover de beperkte tijd strekte. Het gebruik van de Vault heeft geen gevolgen gehad voor de kwaliteit van het audit onderzoek. Kiwa is van mening dat deze opmerking derhalve niet relevant is te vermelden in het audit rapport.	Bij de aanbidding van het conceptrapport heet ILT gevraagd om een check te doen op feitelijk onjuistheden. De beschreven argumentatie is een mening van KIWA. Het is nu in het rapport opgenomen omdat ILT tot de conclusie is gekomen dat er door KIWA op verschillende manieren met externe partijen omgaat. ILT geeft alleen aan dat het een negatief effect op de efficiëntie van het uitgevoerde onderzoek heeft. <u>De reactie van KIWA geeft geen aanleiding om de tekst aan te passen.</u>
2.5 Bevindingen; 6.1 Wob	Het is onduidelijk waarom Kiwa van mening is dat ze niet onder de werking van de Wob valt. Een juridische onderbouwing hiervan ontbreekt	Het Topdocument dat gehanteerd is door ILT voor het opnemen van deze bevinding, is niet een document waar toepasselijke wetgeving uitgebreid beschreven wordt dan wel dient te	De bevinding wordt uit het definitieve rapport verwijderd. Het onderwerp "Wet openbaarheid van bestuur" moet nog tussen ILT en KIWA besproken worden. Het is van belang

Hst/paragraaf	Feitelijke onjuistheden (te corrigeren tekst)	Argumentatie/onderbouwing van uw reactie	Toelichting ILT
		worden. Het is daarom onduidelijk waarom ILT dit opneemt als bevinding.	dat KIWA die informatie levert welke nodig is, om op een bij ILT ontvangen WOB verzoek te kunnen reageren.
2.4 Risk management; 6.5.3 Risicomanagement	Omdat kennelijk geen gebruik is gemaakt van een standaardrisicoanalyse methode is evenmin geborgd dat alle relevant risico's zijn onderkend.	ILT stelt in haar rapport: Het is niet mogelijk om te beoordelen of afdoende mitigerende maatregelen zijn getroffen om relevante risico's te beheersen. Hoe komt ILT vervolgens tot haar oordeel dat kennelijk geen gebruik is gemaakt van een standaard risicoanalyse methode en evenmin geborgd is dat alle relevante risico's zijn onderkend? Vanwege tijdsgebrek heeft Kiwa de risicomanagement vragen niet kunnen beantwoorden en is geen risicomanagement documentatie overhandigd. Kiwa is van mening dat ILT zich had dienen te beperken tot de vaststelling dat het niet mogelijk (was) om te beoordelen of afdoende mitigerende maatregelen zijn getroffen om relevante risico's te beheersen.	<p>Tijdens de voorbereiding is door ILT aangegeven:</p> <ul style="list-style-type: none"> • ILT stelt voor dat KIWA aangeeft welke van de gevraagde documenten nog niet geleverd kunnen worden omdat deze nog niet zijn opgesteld en/of in conceptfase zijn. → geen reactie KIWA; • ILT geeft in de mail van d.d. 24-11-2021 aan punt D (toezichtsplan) af te handelen o.b.v. de op 10 december beschikbaar gestelde informatie. Het is niet meer mogelijk om alle toegevoegde documenten mee te nemen in de eindrapportage omdat dit niet past in het schema (rapportage voor eind dit jaar gereed). Tussen 24 november en 10 december had de informatie, waarvan kan worden verondersteld dat deze zonder meer voor handen is, kunnen worden aangeleverd; <p>Het is niet te achterhalen waarom de gevraagde informatie niet op tijd is geleverd. Bij een goed werkend kwaliteitssysteem, moet de beschikbare informatie over het risicomanagement proces snel verstrekt kunnen worden.</p> <p><u>De reactie van KIWA geeft geen aanleiding om de tekst aan te passen.</u></p>

Hst/paragraaf	Feitelijke onjuistheden (te corrigeren tekst)	Argumentatie/onderbouwing van uw reactie	Toelichting ILT
6.5 Kwaliteitsmanagement	De scope en de diepgang van de door BSI uitgevoerde ISO 9001 certificering is beperkt. Geen enkel primair proces valt aantoonbaar binnen de scope van de BSI certificering. De door BSI gerapporteerde toetsing wordt daarom onvoldoende geacht om op te kunnen steunen voor deze audit.	<p>Kiwa wil benadrukken dat de scope van ISO 9001 ook de Uitvoering omvat. Dit blijkt uit de in de Vault ter beschikking gestelde audit documentatie. Op basis van het auditprogramma kan worden vastgesteld dat het primaire proces Scheepvaar is geauditeerd. In het audit rapport op p7 staat het volgende: Doorgenomen: Het behandelen van aanvragen, het uitgeven en beheer van (waarde)documenten en vergunningen Proces van aanvraag tot uitgifte Rijnvaartverklaring (34073) Proces van aanvraag tot uitgifte Vaarbevoegdheidsbewijs Koopvaardij (A-743098-T9N9).</p> <p>In het auditrapport 2018 gaf ILT aan dat relevante bevindingen uit externe audits zoals die van BSI in de auditrapportage waren opgenomen. Derhalve steunde ILT in de 2018 rapportage op auditrapportages van BSI. Hoe komt ILT tot het oordeel dat primaire processen geen onderdeel zijn en het BSI rapportonvoldoende is?</p>	<p>Voor ILT is het belangrijk om vast te stellen dat KIWA voldoet aan wettelijke normen en aan de afspraken tussen KIWA – ILT. De rapportage van BSI geeft ILT niet voldoende informatie om iets te kunnen zeggen over de in de scope opgenomen onderwerpen.</p> <p><u>De reactie van Kiwa geeft aanleiding om de tekst als volgt aan te passen:</u></p> <p>De scope en de diepgang van de door BSI uitgevoerde ISO 9001 certificering verschilt met de scope van ILT. Hierdoor kan slechts in beperkte mate gebruik gemaakt worden van de resultaten van de uitgevoerde ISO 9001 certificering. De door BSI gerapporteerde toetsing wordt daarom onvoldoende geacht om op te kunnen steunen voor deze audit.</p>
2.5 Bevindingen; 6.5.1 Compliance management	Het is daarnaast niet duidelijk op welke wijze Kiwa voldoet aan de wettelijke eisen.	<p>In het document Kernproces, procedure 2.5 Wettelijkewijziging, verbetering en vernieuwing product en proces wordt beschreven hoe Kiwa voldoet aan de wettelijke eisen. Daarnaast zijn werkinstructies beschikbaar welke zijn opgesteld volgens COPAFIJT beginselen. Werkinstructie Actiepunten Wijziging Wetgeving W25-1 geeft een overzicht van alle benodigde activiteiten waaronder het opstellen van een plan van aanpak, handhavings- en uitvoeringstoets.</p>	<p>Bij de aanbieding van het conceptrapport heet ILT gevraagd een om check te doen op feitelijk onjuistheden. De beschreven argumentatie is een mening van KIWA waarbij deze niet onderbouwd is met nieuwe feitelijkheden.</p> <p><u>De reactie van KIWA geeft geen aanleiding om de tekst aan te passen.</u></p>

Hst/paragraaf	Feitelijke onjuistheden (te corrigeren tekst)	Argumentatie/onderbouwing van uw reactie	Toelichting ILT
		Vanuit de ISO 27001 certificeringsaudit zijn bevindingen geconstateerd m.b.t. wet en regelgeving, deze zijn opgelost zoals inzichtelijk gemaakt in het overzicht van wet- en regelgeving dat bij de audit ter beschikking is gesteld; daarmee heeft Kiwa nu inzicht in wet en regelgeving.	
6.4 Interne audits	Tekortkomingen worden vaak niet onderzocht op root cause, de geconstateerde fout wordt dan hersteld door een correctieve actie maar de kans op herhaling wordt hierdoor niet kleiner.	ILT geeft aan dat tekortkomingen vaak niet worden onderzocht op root cause. Kiwa is van mening dat de kwalificatie 'vaak' nadere omschrijving verdient.	Door de beperkingen die het gebruik van virtual vaults met zich meebrengt is niet goed te monitoren hoe vaak dit heeft plaats gevonden. <u>De reactie van Kiwa geeft aanleiding om de tekst als volgt aan te passen:</u> Vaak zal worden veranderd in regelmatig, echter de essentie van het hoofdstuk is hierdoor overigens niet veranderd.
2 Managementsamenvatting en conclusie; 6.4 Interne audits	Ons is niet gebleken dat root cause analyses in alle gevallen waar nodig worden uitgevoerd Tekortkomingen worden vaak niet onderzocht op root cause, de geconstateerde fout wordt dan hersteld door een correctieve actie maar de kans op herhaling wordt hierdoor niet kleiner.	Kan ILT de samenvatting meer op één lijn brengen met de detailtekst in de paragrafen? Bijvoorbeeld samenvatting 2021B4: niet (...) in alle gevallen, tegenover detailtekst: vaak.	<u>De reactie van Kiwa geeft aanleiding om de tekst aan te passen.</u>
2.2 Compliance management	Daarnaast is niet alle gevraagde documentatie aangeleverd en zijn niet alle gestelde vragen over dit onderwerp beantwoord	Daarnaast is niet alle gevraagde documentatie aangeleverd en zijn niet alle gestelde vragen over dit onderwerp beantwoord" moet zijn: binnen het door ILT gestelde tijdsbestek kon de benodigde informatie niet aangeleverd worden. Hierover is tijdig gecommuniceerd naar de auditoren.	Tijdens de voorbereiding is door ILT aangegeven: <ul style="list-style-type: none"> • ILT stelt voor dat KIWA aangeeft welke van de gevraagde documenten nog niet geleverd kunnen worden omdat deze nog niet zijn opgesteld en/of in conceptfase zijn. → geen reactie KIWA; • ILT geeft in de mail van d.d. 24-11-2021 aan punt D (toezichtsplan) af te handelen o.b.v. de op 10 december beschikbaar gestelde informatie.

Hst/paragraaf	Feitelijke onjuistheden (te corrigeren tekst)	Argumentatie/onderbouwing van uw reactie	Toelichting ILT
			<p>Het is niet meer mogelijk om alle toegevoegde documenten mee te wegen in de eindrapportage omdat dit niet past in het schema (rapportage voor eind dit jaar gereed). Tussen 24 november en 10 december had de informatie, waarvan kan worden verondersteld dat deze zonder meer voor handen is, kunnen worden aangeleverd.</p> <p>Het is niet te achterhalen waarom de gevraagde informatie niet op tijd is geleverd. Bij een goed werkend kwaliteitssysteem, moet de beschikbare informatie over compliance management proces snel verstrekt kunnen worden.</p> <p><u>De reactie van KIWA geeft geen aanleiding om de tekst aan te passen.</u></p>
2.3 Kennis en competentie management	"Dit omdat het proces voor het maken van functiebeschrijvingen met competenties niet beschikbaar is en omdat de functiebeschrijvingen hiervoor te algemeen zijn opgesteld"	Een proces voor het maken van functiebeschrijvingen is geen voorwaarde voor de vaststelling door ILT of "Kiwa te allen tijde over noodzakelijke capaciteit, kennis en deskundigheid beschikt voor een juiste uitvoering van de taken en voor zover toepasselijk aandeskundigheids- en opleidingsvereisten uit wet- en regelgeving en internationale verdragen voldoet"	<p>De beschreven argumentatie is een mening van KIWA. De daadwerkelijke scope is tijdens het onderzoek beperkt omdat vragen over compliance management, kennismanagement en risicomanagement niet of niet tijdig zijn beantwoord en de hierover gevraagde documentatie niet of niet tijdig is aangeleverd.</p> <p>Binnen KIWA is er om dit moment alleen een algemene functie beschrijving van iemand die bij vergunningverlening werkt→ (verschillende waarde documenten, vliegbrevetten, monsterboekjes ,taxi, tacho vergunning voor taxi en bus)</p> <p><u>De reactie van KIWA geeft geen aanleiding om de tekst aan te passen.</u></p>
6.2 Opvolging bevindingenvoorgaande audit	2021B2: Het Kiwa onderzoek wijst uit dat de kwaliteit van het aanvraag en afgifte proces voor AML's en FCL's nog niet optimaal is geborgd. Een root cause analyse van de bevindingen uit 2018 heeft niet plaatsgevonden.	Kiwa wil benadrukken dat de analyses en maatregelen zijn uitgevoerd conform het aan ILT toegezonden corrective action report (CAR) waarin derhalve ook besproken het al dan niet uitvoeren van root cause analyses.	<p>De beschreven argumentatie is een mening van KIWA waarbij deze niet onderbouwd is met nieuwe feitelijkheden.</p> <p><u>De reactie van KIWA geeft geen aanleiding om de tekst aan te passen.</u></p>

Hst/paragraaf	Feitelijke onjuistheden (te corrigeren tekst)	Argumentatie/onderbouwing van uw reactie	Toelichting ILT
6.2 Opvolging bevindingen voorgaande audit	2021B3: Wat ontbreekt aan de evaluatie van het project "G2 implementatie tachograafkaarten" is een hoofdstuk "lessons learned". Het risico bestaat nu dat bij een volgend project gelijksoortige fouten worden gemaakt.	Kiwa wil benadrukken dat weliswaar een apart hoofdstuk "Lessons Learned" ontbreekt, maar dat de verschillende aanbevelingen in de projectevaluatie als zodanig beschouwd dienen te worden waarmee het risico op gelijksoortige fouten in een volgend project aanzienlijk kleiner geacht wordt.	Hoofdstuk 6.2 is niet in tegenspraak met het hier gegeven commentaar. <u>De reactie van KIWA geeft geen aanleiding om de tekst aan te passen.</u>
6.4 Interne audits	2021B5: Ons is niet gebleken dat de monitoring op acties voortkomend uit interne audits, effectief is.	Kiwa wil benadrukken dat maandelijks in het Q Board overleg de status van audits inclusief de opvolging van geconstateerde tekortkomingen wordt gerapporteerd en besproken met leidinggevendenden van de afdelingen Compliance, Productmanagement, Innovatie & Ontwikkeling en Operations. Indien nodig volgen aanmaningen.	De beschreven argumentatie is een mening van KIWA waarbij deze niet onderbouwd is met nieuwe feitelijkheden. ILT geeft aan: Er wordt gerapporteerd aan de Q-board d.m.v. de "Dashboard Compliance" (ref 2.6.1, 2.6.2, 2.6.3) maar hierin wordt niet gerapporteerd over de status van de in de Excel opgenomen acties. <u>De reactie van KIWA geeft geen aanleiding om de tekst aan te passen.</u>
4 Interne audits	Ons is niet gebleken dat door Kiwa expliciet wordt geaudit op opzet bestaande en werking van risico mitigerende maatregelen. Er wordt door Kiwa zwaar gesteund op de collegiale toetsing (CT's) en op eindtoetsen (ET's) die voor de verschillende productiestraten zijn beschreven (opzet). Het ligt voor de hand om op bestaan en werking van deze maatregelen te auditen.	CT en ET zijn integraal onderdeel van de primaire processen die periodiek worden geaudit op bestaan en werking. Ook heeft Kiwa een Dynamisch Controle Programma waarbij de resultaten uit de CT en ET binnen de teams worden geanalyseerd en besproken in bijzijn van een van de kwaliteitsmedewerkers. Derhalve vindt een dergelijke audit zoals in de bevinding gesuggereerd, reeds plaats.	De beschreven argumentatie is een mening van KIWA waarbij deze niet onderbouwd is met nieuwe feitelijkheden. <u>De reactie van KIWA geeft geen aanleiding om de tekst aan te passen.</u>
4.1 Auditscope; 4.2 Audit diepgang; 6.5 Kwaliteitsmanagement	In paragraaf 4.1 staat het volgende: De daadwerkelijke scope is tijdens het onderzoek beperkt omdat vragen over compliance management, kennismanagement en risicomanagement niet of niet tijdig zijn beantwoord en de hierover gevraagde documentatie niet of niet	Kiwa wil benadrukken dat de audit onder grote tijdsdruk, vlak voor Kerst, heeft plaatsgevonden. Dit geldt zowel voor ILT waar de lead auditor de organisatie ging verlaten als voor Kiwa waarin de eindejaar periode altijd het afronden van vele werkzaamheden speelt. Kiwa heeft in mailwisseling duidelijk de beperkingen van de tijd	Tijdens de voorbereiding is door ILT aangegeven: <ul style="list-style-type: none"> • ILT stelt voor dat KIWA aangeeft welke van de gevraagde documenten nog niet geleverd kunnen worden omdat deze nog niet zijn opgesteld en/of in conceptfase zijn. → geen reactie KIWA; • ILT geeft in de mail van d.d. 24-11-2021 aan punt D (toezichtsplan) af te handelen o.b.v. de op 10

Hst/paragraaf	Feitelijke onjuistheden (te corrigeren tekst)	Argumentatie/onderbouwing van uw reactie	Toelichting ILT
	<p>tijdig is aangeleverd.</p>	<p>aangegeven en een alternatief, haalbaar tijdschema voorgesteld. Dit tijdschema is slechts deels overgenomen. Derhalve is de scope niet zozeer beperkt als wel dat door tijdsdruk zaken niet vastgesteld konden worden.</p>	<p>december beschikbaar gestelde informatie. Het is niet meer mogelijk om alle toegevoegde documenten mee te nemen in de eindrapportage omdat dit niet past in het schema (rapportage voor eind dit jaar gereed). Tussen 24 november en 10 december had de informatie, waarvan kan worden verondersteld dat deze zonder meer voor handen is, kunnen worden aangeleverd.</p> <p>Het is niet te achterhalen waarom de gevraagde informatie niet op tijd is geleverd. Bij een goed werkend kwaliteitssysteem, moet de beschikbare informatie over management proces snel verstrekt kunnen worden.</p> <p>De laatste zin is een mening van KIWA</p> <p><u>De reactie van KIWA geeft geen aanleiding om de tekst aan te passen.</u></p>

