Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport ADR
Inzake het onderzoek van de Belastingdienst informatiebeveiliging programma Broedkamer en voorlopers

definitief

Colofon

Titel	Onderzoek ADR inzake het onderzoek van de Belastingdienst informatiebeveiliging programma Broedkamer en voorlopers
Uitgebracht aan	Secretaris-generaal van Financiën, mw. M.R. Leijten
Datum	27 september 2017
Kenmerk	2017-0000191453

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Aanleiding opdracht

Naar aanleiding van een TV-uitzending op 1 februari 2017 over de informatiebeveiliging bij het onderdeel Data & Analytics van de Belastingdienst, heeft de Staatssecretaris van Financiën naar aanleiding van het Kamerdebat op 9 februari 2017 aan de Tweede Kamer een aantal door de Belastingdienst uit te voeren onderzoeken en acties toegezegd. Voor een tweetal van deze onderzoeken en één actie is door de Secretaris-Generaal Financiën aan de ADR opdracht gegeven om onderzoek te doen naar de objectiviteit en degelijkheid in de aanpak, de uitvoering en de rapportage van de volgende door de Belastingdienst uit te voeren onderzoeken en actie. Dit betreft:
1. Onderzoek gegevensgebruik bij D&A;
2. Onderzoek naar informatiebeveiliging bij de Broedkamer en voorlopers;
3. Actie naar de wijze waarop de eisen uit het Handboek Beveiliging Belastingdienst zijn geïmplementeerd in de organisatie, processen en systemen.

Dit rapport bevat de resultaten van het onderzoek door de ADR naar het onderzoek door de Belastingdienst naar de informatiebeveiliging bij de Broedkamer en voorlopers door de Belastingdienst en geeft antwoord op de twee onderzoeksvragen:
1 Is de objectiviteit van de door de Belastingdienst uit te voeren onderzoek Informatiebeveiliging programma Broedkamer en voorlopers geborgd?

2 Is de degelijkheid van het door de Belastingdienst uit te voeren onderzoek Informatiebeveiliging programma Broedkamer en voorlopers geborgd?

Over de onderzoeken naar het gegevensgebruik bij D&A en de actie HBB, wordt door de ADR afzonderlijk gerapporteerd.

Hoofdboodschap

De Belastingdienst heeft naar aanleiding van signalen over de beveiligingssituatie bij de eenheid D&A, een aantal onderzoeken in gang gezet om nader inzicht te verkrijgen. Ter borging van de objectiviteit en de degelijkheid van de door de Belastingdienst uit te voeren onderzoeken, heeft de Secretaris-Generaal Financiën de ADR opdrachtgegeven hier onderzoek naar te doen.
De ADR heeft de door de Belastingdienst getroffen maatregelen die toezien op de borging van de objectiviteit en degelijkheid van het onderzoek van de Belastingdienst geïnventariseerd en onderzocht. Vanwege de aard van de opdracht, kan door de ADR geen zekerheid worden verstrekt.

De naar aanleiding van ons onderzoek samengevatte antwoorden op de twee onderzoeksvragen bij het onderzoek van de Belastingdienst "Onderzoek informatiebeveiliging programma Broedkamer en voorlopers", zijn:

1 Is de objectiviteit van de door de Belastingdienst uit te voeren onderzoek Informatiebeveiliging programma Broedkamer en voorlopers geborgd?

- De aansturing en uitvoering van het onderzoek is geschied door medewerkers die functioneel onafhankelijk zijn van het programma Broedkamer en voorlopers.

2 Is de degelijkheid van het door de Belastingdienst uit te voeren onderzoek Informatiebeveiliging programma Broedkamer en voorlopers geborgd?

- Het onderzoek (inclusief rapportage) Informatiebeveiliging programma Broedkamer is uitgevoerd door gekwalificeerde medewerkers onder toepassing van de algemene kwaliteitseisen van de beroepsorganisatie NOREA en de specifieke eisen van de NOREA-richtlijn 4401.

Onze bevindingen bij het door de Belastingdienst uitgevoerde onderzoek zijn in hoofdstukken 1 en 2 van dit rapport uitgewerkt.

1 Borging objectiviteit van uitvoering van het onderzoek naar informatiebeveiliging bij het programma Broedkamer en voorlopers

De Belastingdienst heeft een aantal maatregelen getroffen die zich richten op de objectiviteit van de uitvoering van het onderzoek Informatiebeveiliging Broedkamer en voorlopers. Deze maatregelen zijn in onderstaande paragrafen beschreven.

1.1 Uitvoering van het onderzoek door medewerkers Belastingdienst, die functioneel onafhankelijk zijn van het programma Broedkamer en voorlopers

Het onderzoek naar informatiebeveiliging bij het programma Broedkamer en voorlopers, is in opdracht van de Directeur-Generaal Belastingdienst uitgevoerd door Belastingdienstmedewerkers, onder verantwoordelijkheid van de hoofddirecteur Informatievoorziening. Het onderzoek is uitgevoerd over de periode 2012 tot februari 2016.
In het begin van deze periode is de Belastingdienst gestart met het in projectverband ontwikkelen van data-analyse modellen en het opzetten van de daarvoor benodigde omgevingen. Vervolgens heeft zich dit ontwikkeld tot het programma Broedkamer. Het programma Broedkamer is in februari 2016 opgegaan in het dienstonderdeel D&A.
Het in het onderzoek betrokken programma Broedkamer en voorlopers viel in de onderzoeksperiode niet onder de verantwoordelijkheid van de hoofddirecteur Informatievoorziening, maar werd aangestuurd door de directeur Belastingdienst. De directeur Bedrijfsvoering IV is de opdrachtnemer van het onderzoek.
Het onderzoek is uitgevoerd door medewerkers van de IV-organisatie van de Belastingdienst, aangevuld met een drietal ingeleende medewerkers van andere onderdelen van de Belastingdienst. Geen van de bij het onderzoek betrokken medewerkers heeft deel uitgemaakt van het programma Broedkamer of zijn voorlopers. Vastgesteld is dat alle bij het onderzoek betrokken medewerkers functioneel onafhankelijk zijn van het programma Broedkamer en voorlopers.

1.2 Deskundigheid medewerkers onderzoeksteam

Het onderzoeksteam bestaat uit acht medewerkers. Hiervan zijn drie medewerkers ingeschreven in het NOREA-register1 en hebben twee medewerkers de post-doctorale EDP-auditopleiding afgerond. De leden van het onderzoeksteam beschikken over een ruime werkervaring.

1 NOREA is de beroepsorganisatie van IT-auditors in Nederland

2 Borging van de degelijkheid van het onderzoek naar informatiebeveiliging bij het programma Broedkamer en voorlopers

De Belastingdienst heeft een aantal maatregelen getroffen die zich richten op de degelijkheid van de uitvoering van het onderzoek Informatiebeveiliging Broedkamer en voorlopers. Deze maatregelen zijn in onderstaande paragrafen beschreven.

2.1 Uitwerking opdracht volgens NOREA – richtlijn 4401

Het vertrekpunt voor de opdracht aan de Belastingdienst om een onderzoek te doen is de toezegging door de Staatssecretaris aan de Tweede Kamer. Binnen de Belastingdienst zijn een opdrachtgever en een opdrachtnemer benoemd en is een onderzoeksteam samengesteld, met inachtneming van eisen op het gebied van onafhankelijkheid en deskundigheid (zie hiervoor hoofdstuk 1). Gekozen is om de opdracht uit te voeren volgens de NOREA-richtlijn 4401. Dit betreft opdrachten tot het verrichten van overeengekomen specifieke werkzaamheden met betrekking tot informatie-technologie.

De NOREA-richtlijn 4401 is een passende richtlijn voor het onderhavige type onderzoek. In de NOREA 4401-richtlijn is onder andere opgenomen dat de EDP-auditor uitsluitend verslag doet van de uitgevoerde werkzaamheden en de feitelijke bevindingen. In het rapport wordt geen conclusie gegeven. De gebruikers van het rapport dienen zich zelf een oordeel te vormen aan de hand van de werkzaamheden en bevindingen die door de EDP-auditor in het rapport zijn weergegeven.

2.2 Doel van de opdracht, het object van onderzoek en periode van uitvoering

Het doel van het onderzoek naar de informatiebeveiliging bij het programma Broedkamer en voorlopers is als volgt omschreven in het door de onderzoekers van de Belastingdienst opgestelde plan van aanpak : *'dit onderzoek richt zich op het programma Broedkamer en de voorlopers daarvan en beslaat de periode van 2012 tot februari 2016. Het doel van dit onderzoek is drieledig:*
a. aan de hand van in elk geval beschikbare of reconstrueerbare loggegevens over gebruik van systemen, applicaties en data vaststellen of in genoemde periode gegevens van belastingplichtigen, belastingschuldigen of toeslaggerechtigden[3] buiten de Belastingdienst zijn gebracht dan wel oneigenlijk[4] zijn gebruikt; b. in kaart brengen welke informatiebeveiligingsmaatregelen in de genoemde periode van kracht waren en hoe deze hebben gewerkt en op basis daarvan vaststellen welke risico's hebben bestaan en c. in relatie tot geconstateerde risico's en/of feiten omtrent daadwerkelijk oneigenlijk gegevensgebruik of het buiten de Belastingdienst brengen van gegevens, signalen inventariseren en bekijken wat daarmee is gedaan.'

De uitvoering van het onderzoek heeft plaatsgevonden in de periode maart 2017 t/m september 2017.

2.3 Plan van aanpak

De opdracht is door het onderzoeksteam van de Belastingdienst uitgewerkt in een plan van aanpak. Dit plan van aanpak "Onderzoek Broedkamer" van 13 april 2017, is op 14 april 2017 ondertekend door de opdrachtnemer en op 19 april 2017 door de gedelegeerd opdrachtgever. In het plan van aanpak is de volgende inhoudsopgave opgenomen:

INHOUD

In het plan van aanpak zijn de volgende onderwerpen uitgewerkt:

- De aard van de opdracht en dat de uitvoering zal plaatsvinden onder toepassing van Richtlijn 4401 van de NOREA waardoor de IT-auditor geen conclusie zal trekken en daarmee geen sprake zal zijn van een Assurance-opdracht;
- De omschreven doelstelling van de opdracht;
- De reikwijdte (scope) van de opdracht;
- Een opsomming van de uit te voeren specifieke werkzaamheden zoals die met gebruikers zijn overeengekomen;
- De aanduiding van het object van onderzoek waarop de overeengekomen specifieke werkzaamheden uitgevoerd zullen worden;
- De aard, de tijdsfasering en de omvang van de uit te voeren specifieke werkzaamheden;
- De te verwachten vorm van het rapport van feitelijke bevindingen en andere vormen van communicatie over de bevindingen inzake de opdracht, voor zover van toepassing;
- Naam projectleider;
- Verantwoordelijkheden projectleider en opdrachtgever;
- De waarborg voor de vrije toegang tot alle personen, informatiesystemen, vastleggingen, documentatie en andere informatie die in het kader van de opdracht wordt gevraagd;
- De afspraken over de planning;
- Een verzoek aan de opdrachtgever de acceptatie van de opdrachtvoorwaarden te bevestigen door het terugsturen van een getekend exemplaar van de opdrachtbevestiging;
- Vertrouwelijkheid en geheimhouding;
- Wederzijdse ondertekening.

De voor het onderzoek relevante aspecten worden behandeld in het plan van aanpak. Het opgestelde referentiekader past bij de doel van het onderzoek.

2.4 Uitvoering werkprogramma

In paragraaf 2.6 van het plan van aanpak Onderzoek Broedkamer is de aanpak van het onderzoek informatiebeveiliging programma Broedkamer en voorgangers beschreven. De verschillende uit te voeren werkzaamheden zijn benoemd en vervolgens verdeeld over de teamleden. Hierbij is rekening gehouden met de voor de uitvoering van de werkzaamheden benodigde kennis en ervaring.
Van elk afgenomen interview is een verslag opgesteld, welke is afgestemd met de geïnterviewde. De voor het onderzoek bestudeerde documenten zijn evenals de bij de uitvoering van het onderdeel naar de loggegevens gebruikte correspondentie, lijstwerk en opgevraagde documentatie opgenomen in het dossier.
Vanwege onvolledigheid van de beschikbare logging is een beperkt deel van de periode 2012-feb 2016 onderzocht.
De vereiste werkzaamheden zijn uitgevoerd en op 21 september 2017 afgerond, het dossier is op dezelfde datum afgesloten.

2.5 Analyse

Bij de uitvoering van het onderzoek is gebruik gemaakt van een bevindingenmatrix. In de bevindingenmatrix zijn van elke onderzochte norm de aangetroffen bevindingen, de bijbehorende bron en het onderliggende document systematisch vastgelegd.
De aangetroffen bevindingen zijn in een overzicht opgenomen. Dit overzicht is afgestemd met het verantwoordelijk management.

2.6 Dossiervorming

Het onderzoek heeft binnen de Belastingdienst als werknaam :"Onderzoek Broedkamer". De archivering van het dossier vindt plaats op een hiervoor specifiek gereserveerde ruimte. De toegang tot deze ruimte en de mogelijkheid voor uitvoeren van werkzaamheden is verstrekt aan een beperkt aantal belastingdienstmedewerkers die betrokken zijn bij de uitvoering van het onderzoek en aan een beperkt aantal ADR-medewerkers betrokken bij de uitvoering van het onderzoek van de ADR.

De door het onderzoeksteam gedane bevindingen zijn afgestemd met het verantwoordelijke management en in het dossier te herleiden naar de bron.

De relevante documenten zijn aangetroffen in het dossier. De relatie tussen planning, uitvoering, analyse en rapportage is zichtbaar in verschillende documenten.

2.7 Afwegingsproces voor opname van bevindingen in de rapportage

De relatie tussen het bevindingenoverzicht en de rapportage (en de afweging daartussen) is opgenomen in*: "Wegingstabel bevindingen in rapportage".*
Het onderzoeksteam heeft in een afwegingsproces keuzes gemaakt wat betreft het opnemen van bevindingen in de rapportage. Zo zijn bevindingen met een vertrouwelijk karakter niet in detail in de rapportage opgenomen. In voorkomende gevallen is ervoor gekozen om bevindingen samenvattend op een hoger abstractieniveau weer te geven. De relevante bevindingen zijn in de rapportage opgenomen.

2.8 Rapportage

Over de uitkomsten van het onderzoek is op 21 september 2017 het definitieve rapport:*"Rapport van bevindingen onderzoek informatiebeveiliging programma Broedkamer en voorlopers"* uitgebracht. Het concept van het rapport is besproken met de opdrachtgever.
De volgende formeel vereiste onderwerpen zijn op juiste wijze opgenomen in de rapportage:

- een beschrijving van het doel en van de overeengekomen werkzaamheden;
- een opschrift dat duidelijk aangeeft dat dit een rapport van bevindingen betreft;
- de identificatie van de specifieke objecten waarop de overeengekomen specifieke werkzaamheden toegepast zijn;
- de vermelding dat de met de ontvanger overeengekomen werkzaamheden zijn uitgevoerd;
- de vermelding dat de opdracht is uitgevoerd overeenkomstig NOREA Richtlijn 4401: Opdrachten tot het verrichten van overeengekomen specifieke werkzaamheden met betrekking tot informatietechnologie;
- de beschrijving van de uitgevoerde specifieke werkzaamheden;
- de beschrijving van de feitelijke bevindingen van de IT-auditor, waaronder voldoende details van de gevonden fouten en afwijkingen;
- de vermelding dat geen assurance-opdracht is uitgevoerd en dat derhalve geen zekerheid over het object van onderzoek wordt verstrekt;
- de vermelding dat, indien de auditor andere aanvullende werkzaamheden of een assurance-opdracht zou hebben uitgevoerd, wellicht andere onderwerpen zouden zijn geconstateerd en gerapporteerd;
- eigenaarschap rapport;
- datum van het rapport;
- ondertekening.
- In het rapport zijn feitelijke bevindingen opgenomen en wordt geen zekerheid verschaft en geen conclusie getrokken. In het rapport worden geen aanbevelingen gedaan. Dit is overeenkomstig de NOREA richtlijn 4401.

3 Verantwoording onderzoek ADR

3.1 Werkzaamheden en afbakening

De ADR heeft de opdracht uitgevoerd gedurende de uitvoering van het onderzoek informatiebeveiliging Broedkamer en voorlopers te weten van april 2017 tot en met 21 september 2017.

Onze overeengekomen werkzaamheden zijn conform het plan van aanpak uitgevoerd. De onderzoeksvragen hebben wij beantwoord door het opgestelde en in de bijlage opgenomen referentiekader in te vullen aan de hand van het door de Belastingdienst opgestelde dossier en rapportage van het onderzoek informatiebeveiliging Broedkamer en voorlopers van de Belastingdienst.
Het concept van dit rapport is voor hoor en weder hoor met de hoofd directeur Informatievoorziening Belastingdienst afgestemd op feitelijke juistheid en is op 27 september 2017 besproken met de gedelegeerd opdrachtgever..

3.2 Gehanteerde standaard

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing.
In dit rapport wordt geen zekerheid verschaft, omdat er geen assurance-opdracht is uitgevoerd.

Het door ons opgestelde referentiekader is opgesteld onder gebruikmaking van de aspecten van de Interne Kwaliteitstoetsing, die de ADR hanteert voor als 'opdrachten tot het verrichten van overeengekomen specifieke werkzaamheden met betrekking tot informatietechnologie'. Deze aspecten zijn gebaseerd op:

- Handboek Auditing Rijksoverheid (HARo) hoofdstuk A2
- HARo hoofdstuk E3
- Gedragscode NOREA richtlijnen 210, 230 en 4401. Tevens zijn nuttige aanwijzingen ontleend aan de NV COS 4400.

De in het referentiekader onder hoofdstuk 2 opgenomen eisen, richten zich met name op het aspect "objectiviteit" van het onderzoek van de Belastingdienst. De overige hoofdstukken richten zich op de "degelijkheid" van het onderzoek.

3.3 Verspreiding rapport

De opdrachtgever, Secretaris-Generaal Financiën mevr. M.R. Leijten, is eigenaar van dit rapport.
De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de ADR een rapport heeft geschreven, het rapport binnen zes weken op de website van de rijksoverheid plaatst, tenzij daarvoor een uitzondering geldt. De minister van Financiën stuurt elk halfjaar een overzicht naar de Tweede Kamer met de titels van door de ADR uitgebrachte rapporten en plaatst dit overzicht op de website.

4 Ondertekening

Den Haag, 27 september 2017

Auditmanager
Auditdienst Rijk

Bijlage 1: Managementreactie

De Belastingdienst heeft naar aanleiding van signalen over de beveiligingssituatie bij de eenheid Data&Analytics, een aantal onderzoeken in gang gezet om nader inzicht te verkrijgen. De ADR is gevraagd om onderzoek te doen naar de objectiviteit en degelijkheid van de door Belastingdienst uitgevoerde onderzoeken. De antwoorden op de twee onderzoeksvragen van de ADR op het "Onderzoek informatiebeveiliging programma Broedkamer en voorlopers", luiden dat:

- De aansturing en uitvoering van het onderzoek is geschied door medewerkers die functioneel onafhankelijk zijn van het programma Broedkamer en voorlopers;
- Het onderzoek (inclusief rapportage) Informatiebeveiliging programma Broedkamer is uitgevoerd door gekwalificeerde medewerkers onder toepassing van de algemene kwaliteitseisen van de beroepsorganisatie NOREA en de specifieke eisen van de NOREA-richtlijn 4401.

Ik onderschrijf de beschreven aanpak, werkwijze en bevindingen van de ADR. De Belastingdienst zal separaat een managementreactie verzorgen op het onderzoek informatiebeveiliging programma Broedkamer en voorlopers en daar vervolg aan geven.

Hoogachtend,

drs. M.R. Leijten
Secretaris-generaal Financiën

Bijlage 2: Referentiekader

Dit referentiekader is opgesteld onder gebruikmaking van de aspecten van de Interne Kwaliteitstoetsing, die de ADR hanteert voor vergelijkbare onderzoeksopdrachten.

Identificatie

Dossiernaam:	
Dossier gearchiveerd op:	
Verantwoordelijk onderzoeker (projectleider):	
Periode uitvoering opdracht:	
Object van onderzoek:	
Doel van opdracht:	

Intake

1a. Heeft de onderzoeker tijdens de intake de relevante onderwerpen met de opdrachtgever besproken en vastgelegd? Hierbij is er onder meer aandacht voor of met de opdracht een rationeel doel wordt gediend.
1 b. Past de keuze voor een onderzoeksopdracht bij de doelstelling van de opdracht?

Aanvaarding onderzoeksopdracht

2a. Blijkt uit het dossier dat de onderzoeker expliciet heeft vastgesteld dat hij en het team voldoen aan de eis van onafhankelijkheid?
2b. Heeft de onderzoeker zo nodig maatregelen getroffen? Zo ja, is daarbij de bedreiging, de beoordeling, de toegepaste maatregel en conclusie vastgelegd?
2c. Blijkt uit het dossier dat de onderzoeker expliciet heeft afgewogen of hij en het team bij het uitvoeren van de opdracht aan alle fundamentele beginselen kunnen voldoen?
Professionaliteit:
Integriteit:
Objectiviteit:
Vakbekwaamheid en zorgvuldigheid:
Vertrouwelijkheid:
2d. Heeft de onderziooeker zo nodig maatregelen getroffen? Zo ja, is daarbij de bedreiging, de beoordeling, de toegepaste maatregel en conclusie vastgelegd?

Plan van aanpak en bevestiging van de opdracht

3a. Heeft de opdrachtnemer de opdracht bevestigd aan de opdrachtgever?

3b. Heeft de auditor in de opdrachtbevestiging in ieder geval de volgende onderwerpen opgenomen:

- ☐ De aard van de opdracht en een verwijzing dat deze zal worden uitgevoerd met inachtneming van Richtlijn 4401, dat derhalve de IT-auditor geen conclusie zal trekken en daarmee geen sprake is van een assurance-opdracht.
- ☐ De omschreven doelstelling van de opdracht.
- ☐ De reikwijdte (scope) van de opdracht.
- ☐ Een opsomming van de uit te voeren specifieke werkzaamheden zoals die met gebruikers zijn overeengekomen.
- ☐ De aanduiding van het object van onderzoek waarop de overeengekomen specifieke werkzaamheden uitgevoerd zullen worden.
- ☐ De aard, de tijdsfasering en de omvang van de uit te voeren specifieke werkzaamheden.
- ☐ De te verwachten vorm van het rapport van feitelijke bevindingen en andere vormen van communicatie over de bevindingen inzake de opdracht, voor zover van toepassing.
- ☐ Naam projectleider
- ☐ Verantwoordelijkheden projectleider en opdrachtgever
- ☐ De waarborg voor de vrije toegang tot alle personen, informatiesystemen, vastleggingen, documentatie en andere informatie die in het kader van de opdracht wordt gevraagd.
- ☐ De afspraken over de planning.
- ☐ Een verzoek aan de opdrachtgever de acceptatie van de opdrachtvoorwaarden te bevestigen door het terugsturen van een getekend exemplaar van de opdrachtbevestiging.
- ☐ Vertrouwelijkheid en geheimhouding
- ☐ Wederzijdse ondertekening.

3c. Hebben de auditor (projectleider) en de opdrachtgever beiden de opdrachtbevestiging ondertekend?

3d. Heeft de auditor een plan van aanpak opgesteld in overeenstemming met de uitgangspunten in HARo : Uit het plan van aanpak moet onder meer blijken dat voor de opdracht voldoende menskracht beschikbaar is en dat de werkzaamheden worden toegewezen aan medewerkers die beschikken over de juiste kennis en vaardigheden, gegeven de aard van de opdracht en de omstandigheden waarin deze moet worden uitgevoerd.

3e. Heeft de auditor eventuele wijzigingen in de opdracht afgestemd met de opdrachtgever?

Veldwerk

4a. Heeft de auditor een werkprogramma opgesteld met daarin de uit te voeren werkzaamheden?

4b. Blijkt de zichtbare betrokkenheid van de projectleider uit het dossier?

4c. Heeft de auditor in het werkprogramma bepaald door welke teamleden de verschillende werkzaamheden worden uitgevoerd en sluiten de specialistische kennis en vaardigheden van de teamleden aan bij de uit te voeren werkzaamheden?

4d. Heeft de auditor alle overeengekomen werkzaamheden afgerond (indien nee: is dit gemotiveerd vastgelegd)?

4e. Heeft de auditor de verzamelde informatie op een overzichtelijke wijze

vastgelegd?

Analyse

5a. Heeft de auditor de wijze van en de uitkomsten van de analyse vastgelegd (bijv. datamatrix)?

5b. Zijn de uitkomsten van de analyse (de voorlopige c.q. concept bevindingen van het onderzoek) voorgelegd aan de auditee en is diens reactie vastgelegd?

5c. Is de informatie die is verkregen uit de uitgevoerde overeengekomen specifieke werkzaamheden als basis gebruikt voor het rapport van feitelijke bevindingen?

Rapportage

6a. Geeft het rapport voldoende gedetailleerd een beschrijving van het doel en van de overeengekomen werkzaamheden, zodat de lezer in staat is de aard en de reikwijdte van de uitgevoerde werkzaamheden te begrijpen?

6b. Heeft de auditor in ieder geval de volgende onderwerpen opgenomen in de definitieve rapportage:

- ☐ een opschrift dat duidelijk aangeeft dat dit een rapport van bevindingen betreft;
- ☐ de geadresseerde (dit zal doorgaans de opdrachtgever zijn die de auditor heeft aangetrokken om de overeengekomen specifieke werkzaamheden uit te voeren);
- ☐ de identificatie van de specifieke objecten waarop de overeengekomen specifieke werkzaamheden toegepast zijn;
- ☐ de vermelding dat de met de ontvanger overeengekomen werkzaamheden zijn uitgevoerd;
- ☐ de vermelding dat de opdracht is uitgevoerd overeenkomstig NOREA Richtlijn 4401: Opdrachten tot het verrichten van overeengekomen specifieke werkzaamheden met betrekking tot informatietechnologie;
- ☐ de beschrijving van het doel waarvoor de overeengekomen specifieke werkzaamheden zijn uitgevoerd;
- ☐ de beschrijving van de uitgevoerde specifieke werkzaamheden;
- ☐ de beschrijving van de feitelijke bevindingen van de IT-auditor, waaronder voldoende details van de gevonden fouten en afwijkingen;
- ☐ de vermelding dat geen assurance-opdracht is uitgevoerd en dat derhalve geen zekerheid over het object van onderzoek wordt verstrekt;
- ☐ de vermelding dat, indien de auditor andere aanvullende werkzaamheden of een assurance-opdracht zou hebben uitgevoerd, wellicht andere onderwerpen zouden zijn geconstateerd en gerapporteerd;
- ☐ eigenaarschap rapport (zie par. 12 audit charter);
- ☐ datum van het rapport;
- ☐ ondertekening.

6c. Zijn de resultaten in het rapport te onderbouwen met de verzamelde informatie in het dossier (audittrail)?

6d. Zijn eventuele aanbevelingen uit hoofde van de *natuurlijke adviesfunctie* kort en bondig opgenomen in de aanbiedingsbrief bij het rapport? NB. Aanbevelingen c.q. adviezen mogen **niet** worden opgenomen in het rapport.

6e. Wordt met de rapportage geen zekerheid verschaft (geen oordeel of overall conclusie opgenomen) en zijn termen als "zekerheid", "conclusie", "controle" of "beoordeling" vermeden in de rapportage? En zijn geen smileys of kleuren gebruikt?

6f. Heeft de auditor het rapport in concept besproken met de opdrachtgever en is diens reactie vastgelegd in het dossier?

6g. Is het rapport ondertekend?

Dossiervorming

7a. Heeft het dossier een duidelijke audittrail waardoor de relatie tussen planning – uitvoering – analyse - rapportage goed te leggen is en zitten alle relevante documenten in het dossier?

7b. Datum dossier onderzoek:

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