Auditdienst Rijk
Ministerie van Financiën

> Retouradres Postbus 20201 2500 EE Den Haag

10,2 e

Logius
[redacted]
2509 JE Den Haag

Auditdienst Rijk
Korte Voorhout 7
2511 CW Den Haag
Postbus 20201
2500 EE Den Haag
www.rijksoverheid.nl
Inlichtingen
[redacted]

10,2e

Ons kenmerk
ADR/U2015/445
Uw brief (kenmerk)

Bijlagen
1

Datum 6 maart 2015
Betreft Reviewbevindingen op VKA-Assurancerapport 2013 inzake Equinix

10,2e [redacted]

Conform het overeengekomen Plan van Aanpak (document 20141124 PvA Managed Services 2013-2014 DEFINITIEF) doe ik jullie hierbij onze reviewbevindingen op het VKA-Assurancerapport 2013 inzake Equinix toekomen. Ik verzoek jullie dit stuk intern binnen Logius beschikbaar te stellen aan de direct betrokkenen, o.a [redacted]. 10,2,e
Inmiddels is er een afspraak op 17 maart a.s. (i.v.m. zijn vakantie nog door [redacted]
10,2,e [redacted]te bevestigen) voor de review over het jaar 2014.

Wij geven Logius n.a.v. onze deelname aan diverse overleggen waarin de betrokken partijen (deelnemers vanuit Logius, Equinix, EBPI alsmede de externe auditors) vertegenwoordigd waren en de uitkomsten van onze reviewwerkzaamheden de volgende aandachtspunten mee voor het vervolg (niet-limitatief):

- Om tot een eventuele Verantwoording te kunnen komen over de producten die Logius aanbiedt en waarbij gebruik wordt gemaakt van de EASI Managed Services dienstverlening, spelen, behalve Equinix, ook EBPI en Logius zelf een rol. Om tot een Verantwoording over de hele keten te kunnen komen is daarom ook een beoordeling van de dienstverlening door EBPI alsmede de regiefunctie van Logius naar Equinix en EBPI toe van belang;

- In de opdrachtverstrekking van Logius aan Equinix over het jaar 2013 was nog voldoende ruimte om tot een concretere opdrachtformulering te kunnen komen voor het controlejaar 2014. Wij noemen als voorbeeld de controle-objecten (o.a. het landschapsplaatje van de technische infrastructuur(componenten)) en de scoping, de termijnen/doorlooptijden en het geven van een overall conclusie. Daarbij is het raadzaam om in toekomstige audits aandacht te schenken aan de wasstraat die bij Equinix is ingericht voor het Logius-product DigiD en aan de (overige) koppelvlakken/interfaces met de overige Logius-producten;

- Voor EBPI verdient de opdrachtverstrekking eveneens nadere aandacht;

- Het verdient aanbeveling de opdrachtformulering(en) in een beperktere setting op te pakken dan in de plenaire sessies die voorheen in een ruimere setting plaatsvonden (d.w.z. met meerdere deelnemers uit de hierna te noemen organisaties) en om hiertoe de volgende partijen uit te nodigen: Logius, Equinix en de auditor van Equinix, EBPI en de auditor van EBPI alsmede de ADR.

Alle hier aangereikte aandachtspunten zijn in een eerder stadium reeds mondeling gedaan, maar uiteraard zijn wij tot het geven van nadere een toelichting gaarne bereid.

Auditdienst Rijk
Ministerie van Financiën

TER INFORMATIE
Aan
Logius
10,2,e [redacted]

Auditdienst Rijk
Inlichtingen
10,2,e [redacted]

Datum
11 februari 2015
Notitienummer
Bijlage bij brief ADR/U2015/445
Rubriek
Auteur
10,2,e [redacted]

notitie

Reviewbevindingen op VKA-Assurancerapport 2013 inzake Equinix
DEFINITIEF

Paraaf

Van
Kopie aan
Bijlagen

1. Inleiding

Verdonck, Klooster & Associates (hierna: VKA) heeft een rapport uitgebracht, getiteld "Third Party Memorandum 2013, Assurance rapport inclusief bijlage voor Equinix, EASI Managed Services Equinix voor Logius" d.d. 24 oktober 2014 Definitief. Hierin geeft de IT Auditor van VKA [redacted] (hierna: auditor VKA), in opdracht van Equinix Inc. (hierna: Equinix) een assuranceverklaring af over de EASI Managed Services dienstverlening door Equinix aan Logius.

Logius is op enig moment voornemens de uitkomsten van onder andere het onderzoek van VKA te gebruiken in haar Verantwoording(en) over de door haar aangeboden producten, indien en voor zover deze gebruikmaken van de EASI Managed Services. Ten behoeve van het vaststellen van de bruikbaarheid van de rapportage van de auditor VKA, is de ADR door Logius gevraagd een review uit te voeren op de door de auditor VKA afgegeven assurancerapportage en -oordeel. Voor onze review hebben wij als uitgangspunt/veronderstelling gehanteerd dat Logius al over 2014 verantwoording wil afleggen, dit is in diverse plenaire sessies met Logius, Equinix, de ADR en (later aangeschoven) VKA steeds benadrukt.

2. Achtergrond

Tussen Logius en Equinix is de afspraak gemaakt dat jaarlijks door een onafhankelijke auditor met een redelijke mate van zekerheid Assurance wordt verschaft over de EASI Managed Services dienstverlening. Hiertoe zijn tussen de door Equinix te behalen beheersdoelstellingen afgesproken. Deze betreffen, naast de beheersprocessen zoals verwoord in "Normenset onderzoek diensten DigiD voor Burgers, OTPnieuw, Haagse Ring en EASI Managed Services, versie

1.6, d.d. 8 mei 2014", tevens de voor de Logius-dienstverlening relevante netwerkinfrastructuur(componenten).

Ten behoeve van de Assurance over 2013 is de uitkomst van het onderzoek door de auditor VKA kenbaar gemaakt in het hierboven aangegeven rapport "Third Party Memorandum 2013, Assurance rapport inclusief bijlage voor Equinix, EASI Managed Services Equinix voor Logius" d.d. 24 oktober 2014 Definitief. De onderzoekswerkzaamheden zijn door de auditor VKA vastgelegd in een auditdossier.

3. Doelstelling

De review van het auditdossier van de auditor VKA heeft tot doel gehad vast te stellen in welke mate het dossier een deugdelijke grondslag biedt voor de bevindingen en conclusie zoals verwoord in het rapport van de auditor VKA. Een tweede doelstelling was na te gaan in hoeverre Logius gebruik kan maken van de uitkomsten van het onderzoek van de auditor VKA. Logius heeft in dit verband aangegeven prijs te stellen op een review van het auditdossier om eventueel bij te kunnen sturen in haar opdrachtverstrekking aan Equinix tot het doen uitvoeren van een onafhankelijk onderzoek.

4. Werkwijze

Onze reviewwerkzaamheden betroffen inzage in het onderliggend auditdossier en een toelichting daarop van de auditor VKA.
In deze notitie worden de uitkomsten en opmerkingen naar aanleiding van de inzage van het auditdossier en de van de auditor VKA verkregen toelichting weergegeven (reviewmomenten: 21-11-2014 en 6-2-2015).
In verband met de audit over 2014, waarin de leerpunten naar aanleiding van de audit over 2013 zouden worden meegenomen, hebben wij de auditor aandachtspunten meegegeven die ons tijdens de review zijn gebleken. Deze zijn zowel in voorliggend stuk als in het Normenkader Algemene Aanpak Reviews dat wij hebben ingevuld verwoord. Beide stukken zijn op diverse momenten, laatstelijk op 11 februari 2015, met de auditor VKA afgestemd en zijn aan hem beschikbaar gesteld.

5. Bevindingen op hoofdlijnen

- *Algemeen*

De auditor VKA heeft in zijn offerte voor de opdracht van Equinix 60 uur begroot, de feitelijke urenbesteding bedroeg volgens mededeling van de auditor 120 uur. Zelfs indien rekening wordt gehouden met beperkte de scope van de opdracht, te weten slechts gericht op de beschreven opzet en op het bestaan van de getroffen beheersmaatregelen en niet op de werking, zijn de begrote uren dusdanig qua aantal dat afgevraagd kan worden of sprake is van een rationele opdracht(aanvaarding).
Hierbij wordt in aanmerking genomen dat sprake is van een assurance-opdracht conform Richtlijn 3000 van de Norea waarbij een redelijke mate van zekerheid dient te worden gegeven en dat sprake is van een technische complexe omgeving die essentieel is voor de dienstverlening door Logius. In de begrote uren moet worden voorzien in een beoordeling van ruim 130 normen en, volgens mededeling van de auditor VKA, van ruim 160 documenten en zouden ook de overige in Richtlijn 3000 aangegeven werkzaamheden moeten worden uitgevoerd.

Hierbij wordt voorts ook in aanmerking genomen dat de auditor VKA de keuze heeft gemaakt om de beheersmaatregelen in opzet en bestaan te toetsen aan de norm, echter onder de voorwaarde dat Equinix de opzet heeft beschreven. Dit betekent dat, als de opzet niet is beschreven, deze bij wijze van eigen actie niet alsnog is beschreven door de auditor. Naar de mening van de ADR had, zeker bij een assurance-opdracht, van de auditor verwacht mogen worden dat de maatregelen ook getoetst zouden worden, zelfs indien geen sprake zou zijn geweest van een beschreven opzet; in dat geval had het in de lijn gelegen deze opzet alsnog -al dan niet op hoofdlijnen- bij wijze van eigen actie te beschrijven.

Ons beeld is daarom dat de auditor VKA met een tamelijk beperkte inspanning zijn onderzoek heeft uitgevoerd. Een overall conclusie ontbreekt.

- *Controleconsiderans*

Er is geen controleconsiderans opgesteld, wel is er een controleprogramma opgemaakt waarin de auditor VKA de door Logius aan Equinix meegegeven normen heeft vertaald/opgenomen zoals verwoord in "Normenset onderzoek diensten DigiD voor Burgers, OTPnieuw, Haagse Ring en EASI Managed Services, versie 1.6, d.d. 8 mei 2014".
In de overwegingen bij het opzetten van zijn controleprogramma en de uit te voeren werkzaamheden heeft de auditor VKA geen gebruik gemaakt van het rapport van de vorige auditor bij Equinix (Vidar Security/Pier Nauta).

Het feitelijke systeemlandschap (de technische infrastructuur van EASI Managed Services-omgeving en de daarbinnen onderscheiden componenten) is niet in kaart gebracht, waardoor input ontbreekt om op basis van een expliciete risico-inschatting te komen tot een verdere scoping van het onderzoek voor het jaar 2014. Hierdoor is het niet mogelijk om voor het controlejaar 2014 voor alle voor de Logius-dienstverlening relevante objecten de aard, omvang en richting van de auditwerkzaamheden te kunnen vaststellen in relatie tot de beheersdoelstellingen en de netwerkinfrastructuur(componenten).

De auditor VKA heeft zich grotendeels beperkt tot de beheerprocessen. Hoewel hij heeft onderkend dat uit de plenaire besprekingen met Equinix, Logius, VKA en de ADR is gebleken dat inzicht in de *feitelijke* inrichting van de netwerkinfrastructuur(componenten) gewenst werd, heeft hij tamelijk beperkte inspanningen verricht ten aanzien van deze inrichting. Hierdoor ontbreekt een sluitend beeld over het bestaan van de netwerkinfrastructuur(componenten) in het rapport. Wel heeft de auditor VKA in zijn rapport een beschrijving opgenomen van de beoogde inrichting.

- *Kwaliteitsbewaking*

Over de interne kwaliteitsbeoordeling danwel kwaliteitssysteem zoals in het algemeen gehanteerd binnen VKA is geen informatie in het dossier opgenomen. Er is geen sprake geweest van een interne Opdrachtgerichte Kwaliteitsbeoordeling (OKB). Hoewel het stelsel van kwaliteitsborgende maatregelen binnen VKA (zoals beschreven in het Handboek Bedrijfsvoering) voorziet in het uitvoeren van een kwaliteitsaudit, heeft deze volgens mededeling van de kwaliteitsmanager VKA voor het Equinix-dossier niet plaatsgevonden. Wel constateren wij dat er binnen het controleteam een onderlinge collegiale review door de teamleden plaatsgevonden op elkaars werkzaamheden, met name inzake de uitgebrachte stukken.
Voorts heeft er een peer review plaatsgevonden door een externe register IT auditor (RE). Diens bevindingen naar aanleiding van de peer review zijn teruggekoppeld met de auditor VKA.

- *Onafhankelijkheid*

De auditor VKA is een externe auditor, dat wil zeggen dat de onafhankelijkheid van de auditor ten opzichte van de opdrachtgever Equinix is geborgd.

- *Dossier*

Tijdens de audit is een controlewerkprogramma gehanteerd waarin de tussen Logius en Equinix afgesproken normen zijn opgenomen. Per getoetste norm, waar van toepassing, is een duidelijke verwijzing aangetroffen naar de onderliggende evidence in het dossier.

6. Samenvattend beeld

Op basis van de review van het auditdossier van de auditor VKA en de gekregen toelichting op de uitgevoerde auditwerkzaamheden is ons beeld dat de auditor VKA met een tamelijk beperkte inspanning zijn onderzoek heeft uitgevoerd. Een overall conclusie ontbreekt.
Wij menen dat er ruimte is voor aandachtpunten die in een vervolgonderzoek nadere uitwerking/invulling behoeven. Deze aandachtspunten blijken uit onze bevindingen in het Normenkader Algemene Aanpak Reviews dat wij hebben ingevuld alsmede uit voorliggend document. Beide stukken zijn met de auditor VKA afgestemd en zijn aan hem beschikbaar gesteld.