Auditdienst Rijk
*Ministerie van Financiën*

> Retouradres Postbus 20201 2500 EE Den Haag

Logius
T.a.v. [redacted], met kopie aan [redacted]
Postbus 96810
2509 JE Den Haag

**Auditdienst Rijk**
Korte Voorhout 7
2511 CW Den Haag
Postbus 20201
2500 EE Den Haag
www.rijksoverheid.nl

**Inlichtingen**
[redacted]

**Ons kenmerk**
ADR/2015/923

**Uw brief (kenmerk)**

**Bijlagen**
1

Datum 23 juni 2015
Betreft Reviewbevindingen op VKA-Assurancerapport 2014 inzake Equinix

Geachte [redacted]

Conform het overeengekomen Plan van Aanpak (document 20141124 PvA Managed Services 2013-2014 DEFINITIEF) doe ik u hierbij onze reviewbevindingen op het VKA-Assurancerapport 2014 inzake Equinix toekomen.
Ik verzoek u dit stuk intern binnen Logius beschikbaar te stellen aan de direct betrokkenen, o.a. aan [redacted]

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.
  Voor een Verantwoording over de hele keten is daarom ook inzicht in 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 2014 was nog niet voorzien in o.a. het landschapsplaatje van de technische infrastructuur(componenten). Dit is van belang om tot een goede scoping te kunnen komen ter bepaling van de aard, omvang en diepgang van de auditinspanningen bij eventuele vervolgaudits. Dit geldt m.m. ook voor EBPI;

- Met betrekking tot Equinix is het o.i. raadzaam om ook 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.

Tot het geven van een nadere toelichting op onze bevindingen zijn wij gaarne bereid.

**Auditdienst Rijk**

**Ons kenmerk**
ADR/2015/923

10,2,e

Auditdienst Rijk
*Ministerie van Financiën*

**TER INFORMATIE**
Aan
Logius, t.a.v. [redacted], met kopie aan [redacted]
Postbus 96810
2509 JE Den Haag

**Auditdienst Rijk**
**Inlichtingen**
[redacted]

**Datum**
23 juni 2015
**Notitienummer**
Bijlage bij brief ADR/2015/923
**Rubriek**
**Auteur**
[redacted]

Paraaf

**Van**
**Kopie aan**
**Bijlagen**

# notitie

Reviewbevindingen op VKA-Assurancerapport 2014 inzake Equinix
DEFINITIEF

## 1. Inleiding

Verdonck, Klooster & Associates (hierna: VKA) heeft een rapport uitgebracht, getiteld "Third Party Memorandum 2014, Assurance rapport EASI Managed Services Equinix voor Logius" (inclusief bijlage) d.d. 26 januari 2015. 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. Voor onze review hebben wij als uitgangspunt/veronderstelling gehanteerd dat Logius 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 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 2014 is de uitkomst van het onderzoek door de auditor VKA kenbaar gemaakt in het hierboven aangegeven rapport "Third Party Memorandum 2014, Assurance rapport EASI Managed Services Equinix voor Logius" (inclusief bijlage) d.d. 26 januari 2015. 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 conclusies 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.

De resultaten van onze review zijn opgenomen in voorliggende rapportage van bevindingen. Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing.

Met onze rapportage wordt geen zekerheid verschaft. Dat wil zeggen dat hierin geen (samenvattend) oordeel wordt gegeven. De rapportage wordt uitgebracht aan en is bestemd voor Logius.

## 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: 17-3-2015 en 5-6-2015). Op basis hiervan hebben wij het door ons gehanteerde Normenkader Algemene Aanpak Reviews ingevuld en zijn onze bevindingen samengevat in voorliggende notitie. Beide stukken zijn op diverse momenten, laatstelijk op 5 juni 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 ruim 200 uur begroot. In de door Equinix aan de auditor VKA verstrekte opdracht is niet voorzien in de beschrijving en beoordeling van het systeemlandschap van Equinix, voor zover relevant voor de dienstverlening aan Logius.

- *Controleconsiderans*

Er is een controleconsiderans opgesteld. Hierin is een onderscheid aangebracht naar kernprocessen (SEC, INF, ACC, CON, CHA en INC) en naar ondersteunende processen (SLM, SUP, CTY, PRO, GEN, CAP en AVA). De auditor VKA geeft aan dat dit de classificatie is die Equinix hanteert om tot een prioritering van op te lossen punten te komen.

Het is niet duidelijk in hoeverre de considerans c.q. het onderscheid is gebaseerd op een eigen risico-inschatting van de auditor VKA en welke overwegingen

inzake het controle-object hij heeft gehanteerd ter bepaling van de opzet, richting en omvang van zijn verwachte audit(inspanningen).
Ook is niet duidelijk in welke mate inzicht in het systeemlandschap van Equinix alsmede inzage in rapportages van derden ((ISO 27001 audit en pentest) hebben meegewogen in de bepaling van de audit-inspanningen.

Er is een controleprogramma ("Werkblad") opgemaakt waarin de auditor VKA de door Logius aan Equinix meegegeven normen heeft vertaald/opgenomen zoals verwoord in het "Normenset onderzoek diensten DigiD voor Burgers, OTPnieuw, Haagse Ring en EASI Managed Services, versie 1.6, d.d. 8 mei 2014". Hierin is ook het proces SUP opgenomen, met verhoging van het versienummer naar versie 1.7.

- *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 voor het Equinix-dossier niet plaatsgevonden.
In de voorgestelde aanpak van VKA was voorzien in review door een collega auditor (RE). Hiervan is in het dossier echter niet gebleken.
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.

- *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 is, waar van toepassing, een duidelijke verwijzing aangetroffen naar de onderliggende evidence in het dossier.
In het Werkblad is de werkwijze aangegeven die op voorhand voorzien was door de auditor VKA: "gevraagde documentatie" en "uit te voeren deelwaarnemingen". Hierin zijn ook de feitelijk ontvangen documenten alsmede de conclusie opgenomen per norm, op het niveau van beheerdoelstelling en op overall procesniveau. Tevens zijn, indien van toepassing, aanbevelingen geformuleerd.
In het Werkblad zijn geen bevindingen opgenomen in die zin dat er per norm geen korte recapitulatie is gegeven van de uitkomsten van de voor die norm bestudeerde documentatie, anders dan de aangetroffen documentatie en een conclusie.
Voor een adequate beeldvorming door een derde dienen derhalve alle bewijsstukken geraadpleegd te worden. De door de auditor VKA uitgevoerde deelwaarnemingen waren in een aantal gevallen beperkt.

## 6. Samenvattende bevindingen

Op basis van de review van het auditdossier van de auditor VKA en de gekregen toelichting op de uitgevoerde auditwerkzaamheden kan niet in alle gevallen worden vastgesteld welke afwegingen en overwegingen de auditor VKA heeft gemaakt bij de vertaling van zijn bevindingen naar de getrokken conclusies. Samengevat luiden onze bevindingen als volgt:

| Nr. | Proces | Conclusie auditor VKA over het proces[1] | Reviewbevinding: de ADR kan de (onderbouwing/totstandkoming van de) door VKA getrokken conclusie *wel/niet* volgen |
|---|---|---|---|
| | | | |
| 1 | Generieke beheersaspecten (GEN) | Voldoet | Wel |
| 2 | Service Level Management (SLM) | Voldoet | Wel |
| 3 | Supply Management (SUP) | Voldoet | Niet |
| 4 | Security Management (SEC) | Voldoet niet | Wel |
| 5 | Capacity Management (CAP) | Voldoet | Wel |
| 6 | Availability Management (AVA) | Voldoet | Niet |
| 7 | Continuity Management (CTY) | Voldoet | Niet |
| 8 | Infrastructure Management (INF) | Voldoet (maar voldoet deels voor 1 van de 2 beheersdoelstellingen) | Niet |
| 9 | Access Management (ACC) | Voldoet | Niet |
| 10 | Configuration Management (CON) | Voldoet (maar voldoet deels voor 1 van de 1 beheersdoelstelling) | Niet |
| 11 | Change Management (CHA) | Voldoet (maar voldoet deels voor 1 van de 3 beheersdoelstellingen) | Wel |
| 12 | Incident Management (INC) | Voldoet | Wel |
| 13 | Problem Management (PRO) | Voldoet | Wel |
| 14 | Operations Management (OPS) | Voldoet | Wel |

Het bovenstaande betekent niet dat de door de auditor VKA getrokken conclusies onjuist zouden zijn, het betekent dat wij op basis van het ons beschikbaar gestelde auditdossier en de verkregen toelichting de overwegingen en afwegingen waarlangs de auditor VKA tot zijn conclusies is gekomen niet voor alle processen kunnen reproduceren.

[1] Dit betreft de *overall* conclusie van de auditor VKA over het (gehele) proces zoals beschreven in diens rapport. Per proces kunnen namelijk meerdere beheersdoelstellingen worden onderkend waarvoor door de auditor VKA in voorkomende gevallen een andere (deel)conclusie is getrokken. Waar van toepassing zijn deze ook vermeld.