Auditdienst Rijk
Ministerie van Financiën

Audit Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT)

Beheeronderzoek 2013

ADR/2014/1087

Datum	16 september 2014
Status	Definitief

Colofon

Titel	Audit Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT)
Bijlage(n)	-
Inlichtingen	**Auditdienst Rijk** **Postbus 20201** **2500 EE Den Haag**

1 Inleiding

1.1 Aanleiding opdracht

In artikel 8 van het Besluit verstrekking gegevens telecommunicatie (Besluit Telecom) is opgenomen dat de Minister van Veiligheid en Justitie jaarlijks een verslag opstelt van een audit naar de correcte uitvoering van het Besluit door de volgende organisaties:

- de aanbieders van openbare telecommunicatiediensten of van openbare telecommunicatienetwerken;
- het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT);
- de arrondissementsparketten;
- de Politiekorpsen;
- andere opsporingsdiensten.

Onderwerpen die hierin tenminste behandeld moeten worden zijn de werking van het systeem, de kwaliteit van de verstrekking van gegevens en de bevraging van gegevens.
In het kader van deze jaarlijkse verplichting is de Auditdienst Rijk (ADR) door de directeur-generaal Rechtspleging en Rechtshandhaving (dgRR) gevraagd een onderzoek uit te voeren om inzicht te verschaffen in de werking van het systeem bij het CIOT.

1.2 Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT)

Het CIOT is een onderdeel van het Ministerie van Veiligheid en Justitie en is aangewezen om de informatieverzoeken van de (bijzondere) opsporingsdiensten ((B)OID's) door te geleiden naar de aanbieders van telecommunicatiediensten. Het CIOT kan worden beschouwd als een "berichtenmakelaar". Daartoe beheert het CIOT het geautomatiseerd CIOT-informatiesysteem (CIS), waarin het vraag- en antwoordverkeer van de door de(B)OID's expliciet gevraagde gegevens wordt doorgeleid.

Het CIOT schept randvoorwaarden zodat de gegevens van gebruikers van telecommunicatie met de juiste zorgvuldigheid worden behandeld en daarmee wordt voldaan aan wettelijke voorschriften, zoals het BIR, VIR, VIR/BI en de WBP.

1.3 Leeswijzer rapport

Hoofdstuk 2 geeft de belangrijkste risico's weer. In hoofdstuk 3 van dit rapport is de opdracht beschreven. De bevindingen zijn in hoofdstuk 4 geplaatst.
Het laatste hoofdstuk gaat in op het totstandkomingsproces van de gepubliceerde jaarcijfers CIOT.

2 Samenvatting

Het getoetste normenkader bevat in totaal 160 normen. Behoudens de in hoofdstuk 4 opgenomen bevindingen wordt aan de normen voldaan.

De drie risico's die wij expliciet onder de aandacht van het management willen brengen zijn:

Het structureel evalueren van wijzigingen en incidenten, alsmede de vastlegging van deze activiteit moet nadrukkelijk onderdeel zijn van het wijzigingsproces. Deze activiteiten raken de kwaliteit van de dienstverlening door CIOT en beperken de risico's van ongewenste effecten in het wijzigingsproces. Daarnaast moet de behandeling en besluitvorming van met name de releases expliciet aantoonbaar zijn.

Op controlelijsten worden van ingetrokken autorisaties van eigen medewerkers niet expliciet aangeven of de actie is uitgevoerd en of dit het gewenste resultaat heeft opgeleverd. In 2013 zijn van de medewerkers die de dienst hebben verlaten zijn autorisaties ingetrokken.

Sinds begin 2013 is het CIOT gehuisvest in het nieuwe complex aan de Turfmarkt. De locatie die het CIOT heeft toegewezen gekregen is direct naast de spoelkeuken van het restaurant. Hiermede is een groter risico voor wateroverlast aanwezig. Daarbij komt dat alle bekabelingen in het nieuwe complex in de tussen-vloeren zijn verwerkt. Om de continuïteit van de dienstverlening zeker te stellen bevelen wij aan dat het CIOT na gaat of aanvullende maatregelen nodig zijn tegen wateroverlast.

3 Opdracht

Dit hoofdstuk gaat naast het doel, het object en scope en de aanpak van de opdracht in op de verspreidingkring van het rapport.

3.1 Doel

Het doel van deze audit is om inzicht te verschaffen in de mate waarin de beheerorganisatie van het CIOT voldoet aan het Besluit verstrekking gegevens telecommunicatie. Het onderzoek is gericht op de kwaliteit (juist-, tijdig- en volledigheid) van de maatregelen, in de opzet en het bestaan, van het informatiemakelaarproces (inclusief het CIOT Informatie Systeem (CIS)) bij het CIOT.

Naast onderzoek gericht op de kwaliteit van het informatiemakelaarproces bij het CIOT is de gepubliceerde verantwoording van de jaarcijfers onderzocht en is getoetst of deze overeenkomt met de rapportages uit het CIS-systeem.

3.2 Object en scope

Het object van onderzoek betreft het informatiemakelaarproces, inclusief het CIS, zoals dat binnen het CIOT functioneert. Hierbij is onderzocht of het systeem functioneert zoals vastgelegd in de SLA's en bijbehorende procedures.
Uitgangspunten hierbij zijn de vastgestelde documenten die de functionaliteit van het systeem weergeven, de procedures en afspraken met providers en de bijzondere opsporingsdiensten.
Daarnaast zijn de generieke ICT beheerprocessen van de CIOT-organisatie onderzocht die van toepassing zijn op het informatiemakelaarproces. Dit omvat de processen: incident en problem management, change en release management, service level management, beschikbaarheids- en capaciteitsbeheer, continuïty management en access management.

Het onderzoek is uitgevoerd binnen het CIOT. Onderzoeken bij de (B)OID's als afnemers van de telecommunicatie-informatie en de aanbieders van openbare telecommunicatiediensten of van openbare telecommunicatienetwerken, alsmede de kantoorautomatisering van het CIOT, vallen buiten de scope van deze audit.

3.3 Aanpak

Aanvullend op de geldende normen voor het informatiemakelaarsproces en het CIS zijn voor het normenkader 2013 de relevante doelstelling uit de Baseline Informatiebeveiliging Rijk (BIR) geselecteerd. De BIR is met ingang van 2014 verplicht van toepassing.

Het in deze audit getoetste normenkader bevat in totaal 160 normen. De audit bij het CIOT heeft plaatsgevonden op basis van interviews, documentstudie, (deel)waarnemingen ter plaatse en dossierreview.
Peildatum van de audit naar de opzet en waar mogelijk het bestaan april 2013.

3.4 Verspreidingskring rapportage

De eindrapportage van deze audit wordt in de vorm van een rapport van bevindingen en aanbevelingen uitgebracht aan de directeur generaal Rechtspleging en Rechtshandhaving van het ministerie van Veiligheid en Justitie.

Inhoud

4 Bevindingen

Algemene IT beheer maatregelen worden in 2014 verder toegesneden.
Het CIOT is sinds 2011 onderdeel van de Justitiële Informatiedienst (JustID) en in 2013 afdeling ondergebracht bij directie Operatie. Het informatiserings -en beveiligingsbeleid van JustID is hierop niet aangepast.
De interim manager geeft aan dat een toegesneden beleid voor het CIOT zelf nadrukkelijk onderdeel zal zijn van het ontwikkelen van de organisatievisie in 2014.

Beheer en Wijzigingsproces moet verbeteren
In 2013 is niet periodiek onderzocht of programma onderdelen conform de laatste geautoriseerde programmaversie aanwezig zijn. Deze taak is na het vertrek van de configuratiebeheerder niet overgenomen en heeft het laatst plaatsgevonden in het eerste kwartaal van 2013. Het risico dat hiermee gepaard gaat is mede afhankelijk van de kwaliteit van changemanagement. Het risico is hier beperkt, omdat versiebeheer een expliciet onderdeel is van het wijzigingsproces binnen CIOT en dit door Team Foundation Server geautomatiseerd wordt bijgehouden. Echter het periodiek onderzoeken is een kwaliteitsaspect van de dienstverlening door CIOT.

Afgesloten en openstaande incidenten worden niet gestructureerd geanalyseerd. Alle leden van het beheerteam zijn belast met het oplossen van incidenten. Vraagt een specifiek incident om aanbevelingen of aanpassingen van de applicatie dan wordt hiervan melding gemaakt in de wijzigingsmodule. Verbetering van analyse van incidenten is onderdeel van het professionaliseren van het beheerproces binnen JustID.

Een release gaat pas in productie na goedkeuring van alle partijen. Door het CIOT is aangegeven dat het 'Project Einde rapport Wijzigingsronde CIOT informatiesysteem 2012' is besproken in de Coördinatieoverleg. Van het overleg waarin het besluit is genomen over het in productie nemen van release in 2013 is geen vastlegging aangetroffen. De procedure is in 2013 niet nageleefd wat zou betekenen dat de release in 2013 ongeautoriseerd in productie is genomen. De formele overdracht voor de release naar beheer is aanwezig en getekend.

Afwijkingen van standaarden worden opgenomen in het project Einderapport en worden besproken in het Coördinatieoverleg. Of er in 2013 een kwaliteitstoets en evaluatie op de release heeft plaatsgevonden is door het ontbreken van een vastlegging van het Coördinatieoverleg voor ons niet na te gaan.

Service Level Management
Service Level Management is niet ingericht, waardoor niet over alle aspecten van de service level agreement rapportages worden opgemaakt. Informatie uit het jaarverslag is niet toereikend om tegemoet te komen aan de SLA-afspraken.

Beveiliging
Lokale beheerders zijn door CIOT in mei 2013 gewezen op periodieke verificatie van uitgegeven autorisaties. De realisatie van het opstellen van kwartaal rapportages is in 2013 is niet gelukt.
Van de CIOT medewerkers die de dienst verlaten wordt bij vertrek een controlelijst gehanteerd, waarvan het intrekken van autorisatie onderdeel is. Deze checklist is bij

vertrek van medewerker in 2013 gevinkt. Niet duidelijk blijkt of daarmee ook de actie is afgerond. Vastgesteld is dat autorisatie van deze medewerker is ingetrokken.

Continuïteit – Huisvesting in Turfmarkt Noord vraagt mogelijk om specifieke maatregelen

Voor de datacenter in Maasland zijn voorzieningen getroffen tegen wateroverlast. De organisatie CIOT echter is gehuisvest in het departement Veiligheid en Justitie aan de Turfmarkt naast de spoelkeuken. Aangegeven is dat er een detectie systeem voor het detecteren van wateroverlast in het pand aanwezig is. Of deze maatregel voor CIOT toereikend is gezien de bijzonder functie en apparatuur van het CIOT is niet geanalyseerd. Mogelijk zijn er specifieke maatregelen tegen wateroverlast voor CIOT noodzakelijk.

5 Jaarcijfers

De Minister van Veiligheid en Jusitie stelt jaarlijks conform artikel 8 van het Besluit Verstrekking Gegevens Telecommunicatie een verslag op waarin voor wat betreft de opsporing van strafbare feiten melding wordt gemaakt van het aantal malen waarin door tussenkomst van het informatiepunt aan een bevoegde autoriteit informatie is verstrekt.

In de audit hebben wij geverifieerd of de gepubliceerde verantwoording van de jaarcijfers 2012 inzake de bevragingen overeenkomt met de rapportagefunctie "Jaarverslag" uit het CIS-systeem. De gepubliceerde verantwoording van de jaarcijfers inzake de bevragingen is opgenomen in het document "CIOT Jaarverslag 2012"[1]

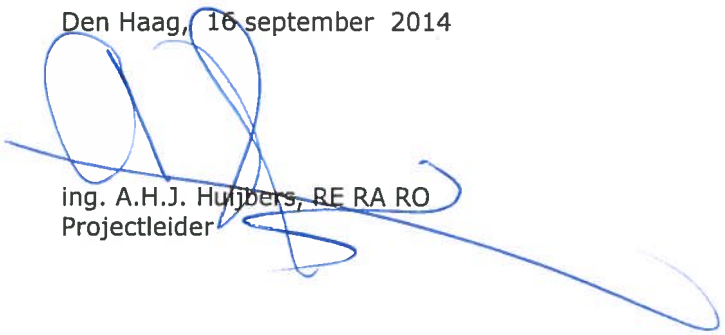
Om deze verificatie te kunnen uitvoeren hebben wij vastgesteld dat er met betrekking tot het totstandkomingsproces van de jaarcijfers binnen het CIOT in 2013 geen wijzigingen hebben plaatsgevonden in de rapportagefunctionaliteit en dat er een aantoonbaar testproces van de rapportagefunctie "Jaarverslag" aanwezig is. Op basis van deze vaststelling hebben wij bij de beantwoording van de vraag omtrent de overeenkomst van de jaarcijfers gesteund op dit totstandkomingsproces.

Uitkomst van onze verificatie is dat de gepubliceerde verantwoording van de jaarcijfers inzake de bevragingen overeenkomt met de jaarcijfers die het CIS-systeem genereert.

[1] Dit jaarverslag is gepubliceerd op de volgende locatie: http://www.rijksoverheid.nl/onderwerpen/telecomgegevens-voor-opsporing/documenten-en-publicaties/jaarverslagen/2013/01/09/ciot-jaarverslag-2012.html

Ondertekening

Den Haag, 16 september 2014



ing. A.H.J. Huijbers, RE RA RO
Projectleider