Ministerie van Veiligheid en Justitie

Eindrapport audit CIOT 2011

Datum	25 september 2012
Status	definitief

Colofon

Afzendgegevens	**Departementale Auditdienst** Kalvermarkt 53 2511 CB Den Haag Postbus 20301 2500 EH Den Haag www.rijksoverheid.nl/venj
Contactpersoon	A.H.J. Huijbers T 070 370 65 60 F 070 370 48 47
Ons kenmerk	dds 5738839/12
Auteurs	ing A.H.J. Huijbers, RE RA RO

Inhoud

1 Samenvatting

Aanleiding
De voorzitter van de Commissie van Advies Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT), tevens directeur JustID, heeft de Departementale Auditdienst van het ministerie van Veiligheid en Justitie (DAD VenJ) gevraagd de jaarlijkse audit uit te voeren bij het CIOT naar de correcte uitvoering van artikel 8 van het Besluit verstrekking gegevens telecommunicatie.
Het onderzoek is binnen het CIOT uitgevoerd. In tegenstelling tot voorgaande jaren vallen de (B)OID's als afnemers en de aanbieders van openbare telecommunicatiediensten of van openbare telecommunicatienetwerken buiten de scope van de audit. Hiervoor zijn afzonderlijke trajecten opgestart.

De audit bestaat uit de volgende twee onderdelen:
1. Herevaluatie van het volledige normenkader waarop het CIOT in 2008 is getoetst.
2. Onderzoek naar het totstandkomingsproces van de jaarcijfers en de overeenkomst van deze jaarcijfers uit het CIS met de gepubliceerde jaarcijfers.

Bevindingen
De beheersmaatregelen bij het CIOT zijn toereikend om de risico's op inbreuken op beveiliging of integriteit van de informatie-uitwisseling te beperken.
Hieronder volgen bevindingen uit de herevaluatie waarvoor wij de aandacht vragen.

1. Om redenen van beveiliging wordt de logging van aangeleverde bestanden niet automatisch beschikbaar gesteld via de FTP-dienst. Het CIOT stelt deze logging in overleg met de aanbieder op verzoek beschikbaar (bij incidenten/problemen). Deze gewijzigde werkwijze is in opzet niet zodanig beschreven.
2. Voor het wijzigingsproces is de volgende bevinding geconstateerd:
   De beschrijvingen van de werkwijze ten behoeve van het accepteren van wijzigingen en het informeren van het Coördinatoren Overleg zijn niet actueel en sluiten niet aan op de huidige werkwijze.
3. Voor het service level managementproces zijn de volgende bevindingen op te maken:
   a. De Service Level Agreement (SLA) voor de (B)OID's en bijbehorende blauwdruk en normenkaders zijn niet geactualiseerd naar de nieuwe situatie van de gebruikte infrastructuur, technologie en procesafspraken.
   b. De huidige werkwijze ten aanzien van het periodiek verschaffen van inzicht in het behaalde niveau van dienstverlening aan de (B)OID's wijkt af van de afgesproken werkwijze in de SLA.
4. Een geformaliseerde autorisatiematrix voor de CIOT omgevingsdomeinen kon niet worden getoond. Een aantoonbare periodieke (per kwartaal) controle op de uitgegeven autorisaties in de omgevingsdomeinen kon eveneens niet worden getoond.
5. De aanbeveling uit vorige onderzoeken om de back-up en recovery procedure te beschrijven en te formaliseren is niet opgevolgd.

Jaarcijfers
Vastgesteld is dat de jaarcijfers uit de gepubliceerde verantwoording inzake de bevragingen overeenkomen met de jaarcijfers inzake de bevragingen die het CIS-systeem genereert.

Datum: 25 september 2012

Dhr. P. Scholte, RA
Directeur DAD

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

2 Inleiding

2.1 Aanleiding opdracht

In artikel 8 van het Besluit verstrekking gegevens telecommunicatie is vastgelegd dat jaarlijks een audit wordt uitgevoerd 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;
- Politiekorpsen;
- Andere opsporingsdiensten.

De voorzitter van de Commissie van Advies CIOT, tevens directeur JustID heeft de Departementale Auditdienst van het ministerie van Veiligheid en Justitie (DAD VenJ) gevraagd een audit uit te voeren naar de correcte uitvoering van bovengenoemd besluit.

2.2 Aanbieders van telecommunicatiediensten

Telecom- en internetaanbieders zijn wettelijk verplicht om telecom- en internetgegevens van hun klanten beschikbaar te stellen voor onderzoek naar criminele activiteiten. Dit staat in het Besluit verstrekking gegevens telecommunicatie. Conform dit besluit levert iedere aanbieder van telecommunicatiediensten tenminste iedere 24 uur gegevens aan bij het CIOT. De door de aanbieders geleverde gegevens moeten overeenstemmen met de gegevens die de aanbieder bij zijn bedrijfsvoering gebruikt. De gegevenslevering door de aanbieder dient elke keer de volledige set van alle gebruikers van telecommunicatiediensten te bevatten, er is dus geen sprake van actualiseren van bestaande gegevens bij het CIOT.

2.3 (Bijzondere) Opsporings- en Inlichtingendiensten

Het opvragen van gegevens door (Bijzondere) Opsporings- en Inlichtingendiensten ((B)OID's) met betrekking tot telecommunicatie diensten mag slechts op basis van een beperkt aantal wettelijke grondslagen geschieden. Het betreft:

- De artikelen 126n, 126na, 126u, 126ua, 126zh, 126zi, 126ii van het Wetboek van Strafvordering (WvS);
- Artikel 29 van de Wet op de inlichtingen- en veiligheidsdiensten (Wiv);
- Artikel 10.10 van de Telecommunicatie Wet (TW).

2.4 Centraal Informatiepunt Onderzoek Telecommunicatie

Het CIOT is een onderdeel van het Ministerie van Veiligheid en Justitie en draagt er zorg voor dat de gegevens van de aanbieders van telecommunicatiediensten worden doorgeleid naar de (B)OID's. Het CIOT kan worden beschouwd als een "clearinghouse", een intermediair tussen aanbieders en gebruikers van telecommunicatie-informatie over gebruikers in Nederland. Daartoe beheert het CIOT het geautomatiseerd CIOT-informatiesysteem (CIS), waarin het vraag- en antwoordverkeer wordt afgehandeld. Hierbij worden alleen die gegevens aan de (B)OID's verstrekt die expliciet zijn opgevraagd.

Het CIOT schept randvoorwaarden dat de gegevens van gebruikers van telecommunicatie met de juiste zorgvuldigheid worden behandeld en daarmee kan voldoen aan wettelijke voorschriften, zoals het VIR, het VIR/BI en de WBP.

2.5 Leeswijzer rapport

Hoofdstuk 3 van dit rapport gaat in op het doel en de aanpak van de audit.
Hoofdstuk 4 behandelt de bevindingen van de herevaluatie van de volledige normenset waarop het CIOT in 2008 is getoetst.
Het laatste hoofdstuk 5 gaat in op het totstandkomingsproces van de gepubliceerde jaarcijfers CIOT.

3 Doel, object, scope en aanpak opdracht

3.1 Doel

Het doel van deze audit was het uitvoeren van een onderzoek, in opzet en bestaan, gericht op het geven van inzicht in de kwaliteit (juist-, tijdig- en volledigheid) van het informatiemakelaarproces bij het CIOT. Hierbij is het bestaan onderzocht door middel van deelwaarnemingen die verspreid over de onderzoeksperiode in detail zijn getoetst. In dit onderzoek zijn ook de incidenten betrokken die zich in 2011 hebben voorgedaan en die effect hebben gehad op de kwaliteit van het informatiemakelaarproces.
Naast een 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 en het CIOT Informatie Systeem (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

In 2009 heeft een follow-up onderzoek plaatsgevonden bij het CIOT. In 2010 is naast een follow-up onderzoek een extra set aan normen geselecteerd afkomstig uit het volledig normenkader dat in 2008 in opdracht van de DAD VenJ is opgesteld. Voor het onderzoek 2011 is het volledige normenkader gehanteerd.
In overleg met en medewerking van de DAD VenJ en het CIOT is dit normenkader geactualiseerd. Aanleiding om het normenkader te actualiseren is geweest: gewijzigde processen en procesbeschrijvingen bij het CIOT en wijzigingen in de infrastructuur die het CIOT inzet bij het informatiemakelaarproces.
Het in deze audit toegepaste normenkader bevat in totaal 165 normen. Hiervan zijn 160 normen getoetst. Van het totale normenkader waren 5 normen niet meer actueel.
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 het bestaan is medio juni 2011.

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.

4 Herevaluatie normen

Dit hoofdstuk gaat nader in op de bevindingen op het volledige normenkader dat in 2008 in opdracht van de DAD VenJ is opgesteld. Dit normenkader bestaat in totaal uit 165 normen. Voor 160 normen heeft een herevaluatie plaatsgevonden. Van het volledige normenkader waren 5 normen niet meer actueel.
Met bevinding wordt in dit rapport een afwijking van de norm bedoeld, waarbij de norm een hoge bijdrage levert aan het mitigeren van de onderkende risico's. Indien in dit rapport over een norm geen bevinding is opgenomen betekent dit dat het CIOT aan de norm voldoet of dat het risico van het afwijken van de norm laag wordt ingeschat.

Wij hebben vastgesteld dat van de 16 aanbevelingen die in 2010 zijn gedaan het CIOT inmiddels 10 aanbevelingen heeft opgevolgd. De overige 6 aanbevelingen uit het onderzoek van 2010 behoeven op enkele punten nog opvolging.

In de hierna volgende paragrafen worden de belangrijkste bevindingen van het onderzoek 2011 behandeld.

4.1 Toegang tot de server(ruimte)

Norm
Toegang tot de server(ruimte) is beperkt tot de daartoe specifiek geautoriseerde personen.

Aangetroffen situatie
Toegangscontrole vindt plaats door middel van elektronische passen en ook zijn de serverracks afgesloten door middel van sloten. Alleen via enkele gemandateerde medewerkers van het CIOT kan toegang worden verkregen tot de servers.
Betrokken servers zijn ondergebracht in rekencentrum Maasland en worden door CIOT-beheerders beheerd.
Met de beheerder van het rekencentrum zijn er afspraken gemaakt over de informatiebeveiliging. Ook is in het contract opgenomen dat er een jaarlijkse TPM wordt opgeleverd.

Een afgegeven TPM door Maasland waarmee het bestaan van de geïmplementeerde toegangscontrole kan worden aangetoond was tijdens de audit niet beschikbaar. In de beheerraad waarin Justitie zitting heeft worden wel beheerrapportages van Maasland besproken.

De leverancier van de FTP-dienstverlening heeft over 2011 een TPM opgeleverd. Deze TPM bevatte bevindingen, waaronder een bevinding ten aanzien van de fysieke toegang tot het rekencentrum van de leverancier. Volgens verklaring van de leverancier en de TPM (die aan het eind van deze audit beschikbaar kwam) had deze bevinding over het gehele jaar 2011 geen impact op de systemen van het CIOT bij de leverancier van de FTP-dienstverlening.
Deze informatie levert voldoende evidence om het bestaan van de norm te toetsen.

4.2 Logbestand t.b.v. de aanbieder

Norm

Het logbestand t.b.v. de Aanbieder wordt geplaatst in de met de Aanbieder afgesproken upload folder die alleen voor de Aanbieder toegankelijk is.

Aangetroffen situatie

Wij hebben vastgesteld dat de logfile wordt geplaatst in een submap op de server waar de aanbieder zijn gegevens via FTP aanlevert. Dit logbestand is alleen beschikbaar voor het CIOT. De functionaliteit om de logging ter beschikking te stellen aan de aanbieder is gewijzigd. Om redenen van beveiligingsrisico's is de logging alleen t.b.v. het CIOT beschikbaar. In overleg met het CIOT is deze informatie voor de aanbieder beschikbaar. Deze gewijzigde werkwijze is in opzet niet zodanig beschreven.

Aanbeveling

Wij bevelen aan om de beschrijvingen ten aanzien van het gebruik en beschikbaar stellen van de aanbiederslogbestanden te actualiseren en aan te laten sluiten op de huidige werkwijze.

4.3 Werkwijze informeren t.a.v. wijzigingen

Norm

Het Coördinatoren overleg (CO) bepaalt, op basis van de testevaluatie van de releasecoördinator, of een release in productie kan worden genomen.

Aangetroffen situatie

Formeel worden wijzigingen in overleg met en door de wijzigingsbeheerder geaccepteerd. Het CO is met name ter kennisname van de wijzigingen en de voortgang en is betrokken bij de Gebruikers Acceptatie Test. De wijzigingsbeheerder treedt hierbij op als linking pin met het CO. Een beschrijving van deze werkwijze kon ons niet worden getoond.

Aanbeveling

Wij bevelen aan om de beschrijvingen van de werkwijze t.a.v. het accepteren van wijzigingen en het informeren van het CO te actualiseren en aan te laten sluiten op de huidige werkwijze.

4.4 Service Level Management

4.4.1 *Actualiseren Service Level Agreement (SLA)*

Norm

De SLA's worden periodiek (jaarlijks) geëvalueerd en daar waar noodzakelijk bijgesteld.

Aangetroffen situatie

Het CIOT heeft zowel met de aanbieders als met de afnemers een SLA afgesloten. Het PID zoals deze in 2010 is opgesteld om de SLA met (B)OID's te actualiseren is niet uitgevoerd. Dit betekent dat tussen het CIOT en de (B)OID's nog steeds een verouderde SLA geldt. Deze SLA is verouderd aangezien de technologie die het CIOT beschikbaar stelt inmiddels is vernieuwd. Dit is nog niet verwerkt in de SLA. Wel zijn deze vernieuwingen doorgevoerd in bijvoorbeeld cursusmateriaal. Daarnaast is de huidige SLA niet volledig en duidelijk over het bevragingsproces en de bijhorende verantwoordelijkheden voor de diverse stakeholders.

Ten tijde van de audit over 2011 is de directie Rechtshandhaving en Criminaliteitsbestrijding (DRC) gestart met het opstellen van een opdracht voor het actualiseren van een aantal documenten waaronder de SLA met de (B)OID's. De andere documenten betreffen de blauwdruk en het normenkader voor de (B)OID's.

Aanbeveling
Wij bevelen aan om de opdracht ten aanzien van het actualiseren van een aantal documenten waaronder de SLA en de blauwdruk in 2012 uit te voeren.

4.4.2 *Periodieke rapportage*
Norm
Periodieke Service Level Reports (SLR's) geven inzicht in de mate waarin aan de SLA is voldaan.

Aangetroffen situatie
In de SLA is opgenomen dat er periodiek rapportage aan de individuele opdrachtgevers plaats vindt. Wij hebben vastgesteld dat er door het CIOT geen periodieke rapportage richting opdrachtgevers plaats vindt. Dit is een afwijking ten opzichte van de opzet. Het CIOT informeert de (B)OID's op de volgende wijze:
- Beschikbaar stellen van de jaarlijkse auditrapportage.
- Beschikbaar stellen van een beheer/monitoring functionaliteit aan de (B)OID's. Deze functionaliteit verschaft de (B)OID's inzicht in de bevragingen en antwoorden.

Aanbeveling
De huidige werkwijze wijkt af van de afgesproken werkwijze in de SLA. Wij bevelen aan de SLA hierop aan te passen.

4.5 Autorisaties

4.5.1 *Autorisatiematrix*
Norm
CIOT verifieert periodiek (per kwartaal) de uitgegeven autorisaties aan de hand van een autorisatiematrix.

Aangetroffen situatie
Voor deze norm is als populatie de interne autorisaties van de CIOT medewerkers zelf onderzocht. De autorisaties van de eindgebruikers ((B)OID's) op het CIS is bij een andere norm onderzocht. Hier zijn geen afwijkingen geconstateerd.
De organisatie heeft ons geen procedurebeschrijving of evidence kunnen tonen van een controle op uitgegeven autorisaties voor de diverse omgevingsdomeinen. Wel is er voor de diverse omgevingen een nog niet goedgekeurde autorisatiematrix aangetroffen die de gewenste positie van de autorisaties op functieniveau aangeeft.

Aanbeveling
Voor de interne systemen van het CIOT bevelen wij aan een autorisatiematrix vast te stellen die de gewenste positie van de autorisaties op functieniveau aangeeft. Op basis van deze autorisatiematrix dient er periodiek (per kwartaal) aantoonbaar een vergelijking te worden uitgevoerd op de actuele situatie.

4.5.2 *Richtlijnen autorisaties*
Norm
CIOT beschikt over eenduidige richtlijnen en procedures voor het toekennen en intrekken van autorisaties.

Aangetroffen situatie
Voor het CIS hebben we een procedure aanmaken en intrekken accounts aangetroffen. De organisatie kon ons geen specifieke richtlijnen tonen ten behoeve van het aanmaken, verwijderen of muteren van autorisaties voor de verschillende omgevingsdomeinen.

Aanbeveling
Wij bevelen aan een richtlijn/werkinstructie vast te stellen voor het aanmaken, verwijderen of muteren van autorisaties voor de verschillende omgevingsdomeinen binnen het CIOT. Deze werkinstructie kan gecombineerd worden met de periodieke controle op uitgegeven autorisaties uit paragraaf 4.5.1.

4.6 Formaliseren backup-procedure

Norm
Dagelijks wordt een back-up gemaakt van programmatuur en relevante gegevens. (N.B. van de gegevens van de aanbieders wordt geen back-up gemaakt)

Aangetroffen situatie
Wij hebben vastgesteld dat van de CIS-programmatuur en relevante gegevens dagelijks een back-up wordt gemaakt. Wij hebben vastgesteld dat de aanbeveling vanuit de audits 2009 en 2010 om de backup procedure te formaliseren niet is opgevolgd. Dit betekent dat de backup procedure nog in concept is.

Aanbeveling
Wij bevelen aan de back-up procedure te formaliseren.

5 Jaarcijfers

Volgens artikel 8 van het Besluit verstrekking gegevens telecommunicatie is vereist dat de Minister jaarlijks verantwoording aflegt over de bevragingen per opsporingsdienst en per rechtsgrond.

In de audit hebben wij geverifieerd of de gepubliceerde verantwoording van de jaarcijfers 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 "Jaarverslag 2011 gebruik CIS"[1]

Om deze controle te kunnen uitvoeren hebben wij vastgesteld dat er met betrekking tot het totstandkomingsproces van de jaarcijfers binnen het CIOT 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 controle 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/2012/01/24/jaarverslag-2011-gebruik-cis.html