Ministerie van Veiligheid en Justitie

Eindrapport audit CIOT 2010

Een audit naar de opvolging door het CIOT van de aanbevelingen uit de audit 2008 en 2009

Datum	23 juni 2011
Status	definitief

Colofon

Afzendgegevens	**Departementale Auditdienst** Kalvermarkt 53 2511 CB Den Haag Postbus 20301 2500 EH Den Haag www.rijksoverheid.nl/venj
Contactpersoon	ing. A.H.J. Huijbers RA RE RO *Senior Auditor* T 070 370 65 60 F 070 370 48 47 a.huijbers@minjus.nl
Projectnaam	Eindrapport audit CIOT 2010
Ons kenmerk	DDS/5698812

Inhoud

Managementsamenvatting

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 een audit uit te voeren bij het CIOT.
De scope van de audit is de CIOT organisatie. In tegenstelling tot voorgaande jaren vallen de bijzondere opsporings- en inlichtingendiensten [(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 uitgevoerde audit bestaat uit de volgende drie onderdelen:
1. Follow-up van de aanbevelingen uit de audit over 2009 die het CIOT betreffen;
2. Herevaluatie van een selectie van normen waaraan het CIOT in 2008 voldeed;
3. Onderzoek naar het totstandkomingsproces van de gerapporteerde jaarcijfers.

Belangrijkste bevindingen
De belangrijkste bevindingen per onderdeel van de audit worden hieronder behandeld:

Follow-up
Van de zes aanbevelingen zijn er drie in voldoende mate opgevolgd. De volgende drie aanbevelingen zijn niet of niet volledig opgevolgd:
1. De Service Level Agreement (SLA) voor de BOID's dateert van maart 2004 en is niet geactualiseerd naar de nieuwe situatie van de CIS applicatie.
2. Aanbeveling uit 2008 was om de back-up en recovery procedure te beschrijven. Wij hebben een concept versie aangetroffen die nog geformaliseerd dient te worden.

Tijdens de audit 2008 is de aanbeveling gedaan om periodiek vast te stellen of de in de productie aanwezige programmatuurversie actueel conform de laatst goedgekeurde versie is. Deze controle is nog niet aantoonbaar uitgevoerd.

Herevaluatie
De belangrijkste bevindingen ten aanzien van de herevaluatie van geselecteerde normen zijn:
1. Om de beschikbaarheid van het interne CIOT netwerk te monitoren wordt de tool Microsoft Operations Manager (MOM) gebruikt. Deze tool is nog niet formeel in productie genomen. Wij bevelen aan deze verder in te richten en te testen.
2. Naast incidenten worden ook problemen geregistreerd in de helpdesktool Topdesk. Wij bevelen aan ook de status en oplossing van een probleem in Topdesk op te nemen. Hierdoor kan de opvolging van problemen beter worden getoetst en is inzichtelijk welke nog openstaan.
3. Voor het wijzigingsproces zijn de volgende bevindingen geconstateerd:
   a. De beheerafdeling hanteert een verouderde wijzigingsprocedure.
   b. Een vastgestelde spoedprocedure is niet aangetroffen.
   c. Een Technisch Ontwerp is aangetroffen maar was niet actueel.
   d. Acceptatietesten worden uitgevoerd maar testplannen, testgevallen, testresultaten en de opvolging van de testen zijn niet aantoonbaar vastgelegd.

e. De formele status van in productie genomen wijzigingen ontbreekt.

4. De virusdefinities van de virusscanner worden handmatig bijgewerkt. Door een onvolledige logging hebben wij niet vast kunnen stellen of de tijdigheid van de definities over de gehele periode geborgd is.
5. De CIOT productieomgeving is nog niet opgenomen in de autorisatiematrix.

Jaarcijfers
Uitkomst van onze audit is dat de gepubliceerde jaarcijfers met betrekking tot opvragingen overeenkomen met de jaarcijfers die het systeem genereert.
Hoewel het totstandkomingsproces van de jaarcijfers voldoet aan de eisen, plaatsen wij een kanttekening bij de juistheid en volledigheid van de rapportage vanwege de omissies geconstateerd in het testtraject.

Den Haag, 23 juni 2011

Departementale Auditdienst van het ministerie van Veiligheid en Justitie

Directeur DAD	Senior Auditor
J. C. van Praat RE RA	ing. A.H.J. Huijbers RA RE RO

1 Inleiding

1.1 Aanleiding

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.

Onze opdrachtgever, 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 bij het CIOT.

1.2 Aanbieders van telecommunicatiediensten

Conform het Besluit Verstrekking Gegevens Telecommunicatie artikel 4, lid 1 en 2, leveren alle aanbieders 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 de gegevens bij het CIOT.

1.3 (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).

1.4 Centraal Informatiepunt Onderzoek Telecommunicatie

Het CIOT is een onderdeel van het Ministerie van Veiligheid en Justitie (MVenJ) 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 volledig geautomatiseerde CIOT-informatiesysteem (CIS), waarin het vraag- en antwoordverkeer zorgvuldig en snel 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 wordt voldaan aan wettelijke voorschriften, zoals het VIR, het VIR/BI en de WBP.

1.5 Scope

De scope van deze audit is de CIOT organisatie. In tegenstelling tot voorgaande jaren vallen de (B)OID's als afnemers van de telecommunicatie-informatie en de aanbieders van openbare telecommunicatiediensten of van openbare telecommunicatienetwerken buiten de scope van dit onderzoek. Hiervoor zijn afzonderlijke trajecten gestart.

1.6 Leeswijzer

Hoofdstuk 2 van dit rapport gaat in op de aanpak van de audit. Voordat de audit is gestart zijn de scope en normenkader van de audit vastgesteld. Daarnaast is vastgelegd hoe er gerapporteerd gaat worden. Deze drie aspecten zijn opgenomen in de paragrafen van hoofdstuk 2.
De uitkomst van de follow-up audit is opgenomen in hoofdstuk 3. Dit hoofdstuk beschrijft in hoeverre het CIOT de aanbevelingen uit de voorgaande audit heeft overgenomen.
Hoofdstuk 4 behandelt de bevindingen van de herevaluatie van normen die eerder zijn getoetst en waaraan het CIOT voldeed.
Het laatste hoofdstuk gaat in op het totstandkomingsproces van de gepubliceerde jaarcijfers CIOT.

2 Aanpak

2.1 Scope van de audit

In overleg met de opdrachtgever van deze audit is besloten de audit 2010 te beperken tot de CIOT organisatie. Redenen voor deze beperkte scope zijn de volgende:

- Bij de (B)OID's zijn diverse afzonderlijke trajecten gestart om de kwaliteit van opvragen te verbeteren en te onderzoeken.
- Uit de onderzoeken van voorgaande jaren is gebleken dat de risico's bij de aanbieders van telecommunicatiediensten beperkt zijn. Dit wordt ook bevestigd door de onderzoeken van voorgaande jaren

Verder is de reikwijdte van de audit 2010 uitgebreid ten opzichte van 2009. In 2009 is een audit uitgevoerd naar de follow-up van de aanbevelingen ter verbetering, zoals die gegeven zijn door de toenmalige auditor. In 2010 is naast de follow-up van de aanbeveling ter verbetering ook een selectie van normen getoetst waaraan het CIOT in voorgaande jaren aan voldeed.

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 april 2011.

2.2 Normenkader

Voor de audit hebben wij ons gebaseerd op een deel van het, over 2008 toegepaste, normenkader. Uitgangspunt bij dit normenkader 2008 is het voldoen aan de geldende wet – en regelgeving, zoals Besluit Verstrekking Gegevens Telecommunicatie, Voorschrift Informatiebeveiliging rijksoverheid (VIR), Voorschrift Informatiebeveiliging rijksoverheid bijzondere Informatie (VIR/BI) en de Wet Bescherming Persoonsgegevens (WBP) , de Service Level Agreements (SLA) en verder vastgelegde afspraken. Dit normenkader bestaat uit drie afzonderlijke onderdelen, te weten een onderdeel voor de aanbieders van telecommunicatiediensten, voor de (B)IOD's, en voor het CIOT.
Wij hebben in onze audit gebruik gemaakt van het onderdeel voor het CIOT. Omdat in de voorgaande audit over 2009 een follow-up op de aanbevelingen bij het CIOT is uitgevoerd is besloten om over 2010 naast een follow-up ook een selectie van normen te toetsen waaraan het CIOT in 2008 voldeed.

Het in deze audit toegepaste normenkader bevat twee onderdelen:

1. Follow-up op de aanbevelingen uit de audit over 2009. Deze aanbevelingen zijn afgeleid van twaalf normen uit het normenkader.

2. Selectie van normen waaraan het CIOT in 2008 voldeed Het complete CIOT onderdeel van het normenkader bevat 165 normen. Van dit onderdeel zijn de normen geselecteerd die een hoge bijdrage leveren aan het mitigeren van de onderkende risico's. Deze selectie bevat in totaal 69 normen.

Naast de geselecteerde normen hebben wij ook het totstandkomingsproces van de gerapporteerde jaarcijfers onderzocht. 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. Wij hebben geverifieerd of de gerapporteerde verantwoording door het CIOT over de

bevragingen overeenkomt met de rapportages uit het CIS en de gepubliceerde jaarcijfers aansluiten op de rapportages.

2.3 Rapportage

In tegenstelling tot artikel 3, lid 1 Auditovereenkomst Staat Aanbieders 2006 wordt de rapportage van de audit uitgebracht aan de voorzitter van de Commissie van Advies CIOT, tevens directeur JustID. De eindrapportage van deze audit bestaat uit een rapport van bevindingen.

3 Resultaat follow-up audit

Dit hoofdstuk behandelt de follow-up van de aanbevelingen zoals die in het rapport van de audit 2009 zijn opgenomen. In deze audit zijn wij nagegaan in hoeverre de aanbevelingen zijn geïmplementeerd. Van de zes openstaande aanbevelingen uit 2009 hebben wij vastgesteld dat de helft hiervan in voldoende mate is opgevolgd.

3.1 Controle integriteit aangeleverde bestanden

Aanbeveling 2008
Op basis van de bevindingen tijdens de audit 2008 is geadviseerd om aanvullende maatregelen te treffen om de integriteit van de importbestanden en de data-uitwisseling beter te borgen. Een voorbeeld van een aanvullende maatregel is het vaststellen van de integriteit van de data-uitwisseling met behulp van bijvoorbeeld een MD5 hash.

Follow-up 2009
Bij de audit 2009 hebben wij vastgesteld dat:

- Het CIOT is gestart met het activeren van de validatie voor alle blackboxen. Deze validatie heeft echter nog een beperkt karakter. Het verder aanscherpen van de validatie kan de kwaliteit van de in te lezen bestanden verhogen. Centrale signalering van mogelijke omissies vinden wij een essentieel aspect;
- Het CIOT maatregelen heeft geïmplementeerd om de vertrouwelijkheid en de technische integriteit van de data-uitwisseling in voldoende mate te borgen door middel van het toepassen van encryptie in combinatie met aanvullende maatregelen zoals SSL en de validatie met de XSD. Het is wel van belang dat ook aan de zijde van het CIOT wijzigingen in de technische infrastructuur en het systeem tijdig en goed worden gecommuniceerd richting aanbieders.

Follow-up 2010
Middels waarneming ter plekke is vastgesteld dat het CIOT de controle op het juiste formaat van de aangeleverde gegevens inmiddels op alle blackboxen heeft geactiveerd. Volgens het CIOT blijft controle op de inhoud van de gegevens een verantwoordelijkheid van de aanbieder zelf.
Wij hebben aan de hand van overzichtsrapportages uit het CIS vastgesteld dat inzichtelijk gemaakt kan worden wat het resultaat is van een import. Daarnaast wordt in de rapportage aangegeven in hoeverre een inleesfout heeft geleid tot een geweigerde import van gegevens.

De aanbeveling is opgevolgd.

3.2 Logging en monitoring

Aanbeveling 2008
Naar aanleiding van de audits 2008 is de aanbeveling gedaan om de aanbieder een meer volledig inzicht te geven in de verwerking van de bestandsaanlevering en het importeren van bestanden om eventuele inhoudelijke fouten tijdig te kunnen oplossen en herstellen. Verder is geadviseerd om voor certificate servers de logging te activeren om tijdig fouten te kunnen ontdekken en nagaan.

Follow-up 2009
Om het aanleverproces zelf beter te kunnen beheersen is het CIOT gestart met de implementatie van aanvullende maatregelen op het punt van logging en monitoring.

Om de aanleveringen te kunnen monitoren en de rapportage geautomatiseerd te kunnen genereren is het CIOT gestart met de bouw van een "Log Service Module". Deze module verzamelt gegevens uit ondermeer de logbestanden van diverse systeemonderdelen.
Voordeel van de module is dat de loggegevens op één plek beschikbaar zijn en snel geanalyseerd kunnen worden aangezien alleen de belangrijkste gegevens worden verzameld. De module was op het moment van audit nog niet in productie.

Verder heeft het CIOT een functioneel ontwerp opgesteld van de "Aanlevering monitor" en de bouw daarvan vastgelegd in een RFC. Met de "Aanlevering monitor" kan de CIOT beheerder in één oogopslag de status van aanlevering op een bepaald tijdstip bekijken. De loggegevens en de functionaliteit van de "Aanlevering monitor" zijn niet beschikbaar voor de aanbieder. Wel kan de CIOT beheerder sneller actie ondernemen op geconstateerde fouten in het aanleverproces.
Tenslotte heeft het CIOT een RFC aangemaakt voor haar informatiesysteem om de rapportage van de aanleveringen geautomatiseerd af te kunnen drukken. Hierdoor kan de rapportage (die nu nog voor een vijftal aanbieders handmatig wordt opgesteld) geautomatiseerd afgedrukt worden voor alle aanbieders.
Voor de certificate servers is de logging inmiddels geactiveerd maar er wordt nog wel aanbevolen om nog nader in te regelen welke informatie met welke periodiciteit relevant is voor de logging en door wie die logging moet worden gecontroleerd.

Er lopen op betreffende punten derhalve activiteiten. Een en ander is nog niet (volledig) afgerond. Derhalve blijven de aanbevelingen uit 2008 nog deels relevant.

Follow-up 2010
Door middel van een waarneming ter plekke is vastgesteld dat in de rapportagemodule wordt bijgehouden of een aanbieder het dagelijkse bestand heeft aangeboden. Afhankelijk van het type provider wordt de aanbieder na 1 of 2 keer het bestand niet actualiseren geattendeerd op het toezenden.
Het CIOT heeft in 2010 een nieuw component voor gegevenstransport naar de blackbox in gebruik genomen. Een onderdeel hiervan is de logservice. Op basis van de logservice kan het CIOT in het CIS een rapport aanroepen die de status van de aanbiedingen toont.

De aanbeveling een meer volledig inzicht te geven in de verwerking en het importeren van de bestandsaanlevering is opgevolgd. De aanbeveling om logging op de certificate servers te activeren is ook opgevolgd.

3.3 Calamiteiten- en uitwijkplan
Aanbeveling 2008
Bij de audit 2008 bleek dat uit het calamiteitenplan van het CIOT, deels steunend op het calamiteitenplan van de Gemeenschappelijke beheerorganisatie (GBO) onvoldoende kon worden afgeleid welke prioriteiten de activiteiten van het CIOT kregen indien zich een calamiteit zou voordoen. Tevens ontbrak (nog) een uitwijkplan.
Inmiddels draait de CIOT productieomgeving bij een andere verwerkingsorganisatie op een andere locatie. Ook is een uitwijklocatie ingericht, maar nog niet operationeel en gereed voor uitwijk.

Follow-up 2009
De aanbeveling uit de audit 2008 om te komen tot een actueel en toereikend calamiteiten- en uitwijkplan blijft van toepassing.

Follow-up 2010

Het CIOT heeft inmiddels opvolging gegeven aan de aanbeveling een calamiteiten- en uitwijkprocedure te beschrijven en te implementeren. Op 27-5-2010 heeft het CIOT een uitwijkoefening uitgevoerd en nadien geëvalueerd. De beschreven en uitgevoerde uitwijk was gericht op de productieomgeving. Het CIOT geeft aan zich bezig te blijven houden met het bepalen van de scope van een uitwijk, waarbij aandacht wordt gegeven aan welke organisatorische en technische zaken bij een uitwijk moeten worden afgedekt.

De aanbeveling is opgevolgd.

3.4 Service Level Agreements

Aanbeveling 2008
De Service Level Agreement voor de BOID's dateert van maart 2004 en is niet geactualiseerd naar de nieuwe situatie van de CIS applicatie. Aanvullend op de SLA's wordt aan de BOID's wel een informatiepakket gestuurd waarin aanvullende procedures worden gecommuniceerd die nog niet beschreven zijn in de SLA's.

Follow-up 2009
De aanbeveling uit 2008 om de SLA zelf te actualiseren blijft van kracht.
Follow-up 2010
De aanbeveling uit 2008 om de SLA's periodiek te evalueren en daar waar nodig bij te stellen is in 2010 als actie door het CIOT opgestart en wordt in 2011 gecontinueerd. Het CIOT heeft een Project Initiatie Document (PID) opgesteld om aan deze actie invulling te geven.

De aanbeveling blijft actueel.

3.5 Back-up en recovery

Aanbeveling 2008
Naar aanleiding van de audits 2008 is de aanbeveling gedaan een back-up procedure op stellen waarin wordt aangegeven op welke wijze de diverse systemen worden geback-upt. Daarbij is ook geadviseerd onderscheid te maken tussen de eigen CISPROD omgeving en de CISDMZ omgeving en blackboxen. Verder is de aanbeveling gedaan een beschrijving op te stellen van de gehanteerde taperoulatie, de wijze waarop de back-ups binnen en buiten het pand worden bewaard.

Follow-up 2009
Het CIOT heeft een werkgroep opgericht die de procedures omtrent back-up en recovery gaat beschrijven. Ten tijde van de audit was er nog geen procedure ter review beschikbaar.

Follow-up 2010
Van de CIS-programmatuur en relevante gegevens wordt dagelijks een back-up gemaakt. De aanbeveling 2009 om deze procedure te formaliseren en vast te leggen in een document is als actiepunt opgepakt. Ten tijde van de audit was een (concept)versie van de procedure beschikbaar.

De aanbeveling blijft actueel totdat de procedure formeel is goedgekeurd.

3.6 Programmaversies

Aanbeveling 2008
Op basis van de bevindingen tijdens de audit 2008 is de aanbeveling gedaan om periodiek vast te stellen of de in de productie aanwezige versie(s) van de CIS modules conform de laatste bevroren en overgedragen programmaversie zijn,

inclusief eventuele (spoed) patches. Bijvoorbeeld door controlegetallen, bijvoorbeeld een MD5 hash op de relevante modules.
Verder is geadviseerd het periodiek uitvoeren van een controle op de programmaversies in te plannen in de activiteiten van de beheerafdeling, waarbij van de uitkomsten van deze controle een vastlegging wordt gemaakt.

Follow-up 2009
Alle systeemonderdelen van het CIS-systeem zijn voorzien van een versienummer. Het CIOT heeft aangegeven dat op de versienummers een periodieke controle plaats vindt, waarbij een beperkt aantal medewerkers onderdelen overdraagt naar productie.
Spoed wijzigingen worden net als gewone wijzigingen afgehandeld middels een RFC en via de OTAP procedure. Bij spoed wijzigingen worden gegevens met betrekking tot een wijziging soms achteraf ingevoerd. Het CIOT heeft op de geïmplementeerde versienummers inmiddels een inventarisatie uitgevoerd. Een periodieke controle is echter nog niet uitgevoerd en opgenomen in een procedure.

Follow-up 2010
Het CIOT heeft de beheertaak om te controleren op versienummers van de actuele CIS-programmatuur in de ontwikkel- en productieomgeving belegd in het proces Configuratiebeheer. Per kwartaal wordt onderzocht of de juiste programmaversies aanwezig zijn. Dit proces is echter niet aantoonbaar gerealiseerd. Het CIOT heeft plannen om het OTAP proces verder te automatiseren, waarbij programmatuur vanuit de ontwikkelomgeving beheerst (geautomatiseerd) wordt overgezet naar de productieomgeving. Hierdoor wordt betere controle op de meest actuele programmatuur mogelijk.

Doordat niet is aangetoond dat de controle periodiek heeft plaatsgevonden blijft de aanbeveling actueel.

4 Herevaluatie geselecteerde normen

Dit hoofdstuk gaat in op de bevindingen die wij hebben geconstateerd tijdens het toetsen van 69 geselecteerde normen. In 2008 voldeed het CIOT aan deze geselecteerde normen en over 2010 heeft er voor deze normen een herevaluatie plaatsgevonden. De normen zijn geselecteerd uit een normenset van in totaal 165 normen op basis van de hoge bijdrage die de normen leveren aan het mitigeren van de onderkende risico's.
Met bevinding wordt in dit rapport een afwijking van de norm bedoeld. Indien in dit rapport over een norm geen bevinding is opgenomen betekent dit dat het CIOT aan de norm voldoet.

4.1 Signalering uitval verbindingen

Norm
Bij het uitvallen van een verbinding, wordt (automatisch) een beheerder gewaarschuwd.

Bevinding
Bij de audit is onderscheid gemaakt tussen interne en externe verbindingen.

Intern CIOT netwerk
Voor het monitoren van interne verbindingen binnen het CISPROD domein gebruikt het CIOT Microsoft Operations Manager (MOM). Deze tool is in de fase van inrichting en testen en nog niet formeel in productie.

Extern netwerk
Bij uitval van een (externe Tele2) verbinding, waarmee o.a. het FTP proces wordt gefaciliteerd, worden de CIOT beheerders door Tele2 op de hoogte gebracht van de storingen. Tele2 neemt telefonisch contact op met de beheerafdeling van het CIOT en daarnaast registreert Tele2 incidenten op een voor het CIOT toegankelijk serviceportaal. Aan de norm met betrekking tot de externe verbindingen wordt voldaan.

Aanbeveling
Wij bevelen aan om de tool Microsoft Operations Manager (MOM) verder in te richten en te testen. Hierdoor wordt het risico beperkt dat bij (gedeeltelijke) storing of uitval van het interne CIOT-netwerk onvoldoende inzicht is welke componenten hierbij zijn betrokken.

4.2 Probleemregistratie

Norm
Een geïdentificeerd probleem wordt geregistreerd.

Bevinding
Wij hebben middels interview en deelwaarneming vastgesteld dat dit het geval is. Incidenten worden geregistreerd in de helpdesktool Topdesk. Indien een probleem wordt onderkend, wordt dit ook geregistreerd. Overigens worden problemen vaak als project gedefinieerd, waarbinnen een oplossing geformuleerd zal worden. Hierbij schenkt men in mindere mate aandacht aan het kunnen volgen van de status en oplossingen in de helpdesktool Topdesk. Hierdoor kan de tracebility verbeterd worden.

Aanbeveling
Wij bevelen aan om naast de registratie van de problemen ook de status en oplossing van een probleem in de helpdesktool Topdesk op te nemen. Hierdoor kan de opvolging van problemen beter worden getoetst en is inzichtelijk welke nog openstaan.

4.3 Wijzigingsproces

Voor het wijzigingsproces zijn er voor meerdere normen bevindingen geconstateerd. Voor de leesbaarheid zijn deze bevindingen in deze paragraaf samengevoegd.

4.3.1 Wijzigingsprocedure

Norm
Als de oplossing van een probleem leidt tot een technische en/of functionele wijziging, wordt een wijzigingsvoorstel ingediend. (Het wijzigingsvoorstel volgt een vooraf gedefinieerd proces)

Bevinding
Er zijn twee procedures voor het wijzigingsproces aangetroffen. Achteraf blijkt dat de procedure uit 2003 is vervangen door de procedure uit 2008. De 2008 versie wordt toegepast door de ontwikkelafdeling. Uit navraag blijkt dat de beheerafdeling van het CIOT nog de wijzigingsprocedure uit 2003 gebruikt.

Aanbeveling
Omdat zowel de beheerafdeling als de ontwikkelafdeling activiteiten verrichten in het wijzigingsproces dienen zij dezelfde wijzigingsprocedure te volgen. Stel daarom vast welke procedure van toepassing is en borg dat alleen deze procedure wordt toegepast.

4.3.2 Spoedwijzigingen

Norm
Urgente wijzigingen worden adequaat bewaakt en eventueel later getoetst door het CAB.

Bevinding
Een vastgestelde spoedprocedure is niet aangetroffen. Gedurende de controleperiode hebben er zich geen spoedwijzigingen voor gedaan.

Aanbeveling
Beschrijf in de wijzigingsprocedure hoe spoedwijzigingen verlopen en laat de gewijzigde procedure goedkeuren door het Coördinatoren Overleg (CO). Hierdoor is vooraf duidelijk hoe deze specifieke wijzigingen lopen en welke controleslagen er voor- en achteraf worden toegepast.

4.3.3 Documentatie ontwikkelde functionaliteit

Norm
Volledige documentatie van ontwikkelde functionaliteit wordt door ontwikkelaars opgeleverd aan productie & beheer.

Bevinding
De wijzigingsprocedure geeft aan dat er voor elke wijziging een Functioneel- en Technisch Ontwerp dient te worden gemaakt. In de deelwaarneming is het Functioneel Ontwerp aangetroffen. Een Technisch Ontwerp was niet bijgewerkt met de laatste doorgevoerde wijzigingen. Het CIOT gaf als reden dat door de

verplichtingenstop er geen capaciteit beschikbaar was om deze bij te werken. Volgens de wijzigingsprocedure dienen het Functioneel Ontwerp en het Technisch Ontwerp voorafgaand aan de wijziging goedgekeurd te worden door het CO. Doordat er voorafgaand aan de ontwikkeling geen Technisch Ontwerp beschikbaar is gesteld is er een risico op onduidelijkheden tijdens het ontwikkelproces.

Aanbeveling
Maak het Technisch Ontwerp actueel en gebruik het Ontwerp voor het vooraf kunnen beoordelen van de impact van voorgestelde wijzigingen.

4.3.4 Acceptatietesten
Norm
Releases ondergaan een systeemtest en een gebruikers acceptatietest (GAT).

Bevinding
Uit deelwaarneming blijkt dat er acceptatietesten worden uitgevoerd. Dit blijkt uit onder andere het opgeleverde testrapport. Dit testrapport bevat geen informatie over de inhoud van de uitgevoerde tests. Een testplan met vooraf gedefinieerde testgevallen is niet aangetroffen.

Aanbeveling
Wij bevelen aan om een gestructureerde testmethodiek, zoals TMAP, te hanteren zodat:

- De risico afweging inzichtelijk wordt gemaakt.
- De test opzet en uitvoering controleerbaar wordt vastgelegd.
- Een onderbouwing van de testrapportage kan worden gegeven.

4.3.5 Formele goedkeuring in productie name
Norm
Het Coördinatoren overleg (CO) bepaalt, op basis van de testevaluatie van de releasecoördinator, of de release in productie kan worden genomen.

Bevinding
Het CIOT geeft aan dat de door te voeren wijzigingen in het CO worden besproken. Een aantoonbare goedkeuring voor de in productie name is niet aangetroffen.

Aanbeveling
Leg de formele goedkeuring door het CO vast. Hierdoor is het duidelijk en controleerbaar wat de formele status van een wijziging is.

4.4 Virusscanner
Norm
Alle systemen zijn voorzien van antivirus-programmatuur, die voortdurend actueel is.

Bevinding
Wij hebben vastgesteld dat op het moment van de audit de virusdefinities up tot date zijn. Vanwege het ontbreken van een volledige logging kan de tijdigheid van het update proces niet worden vastgesteld. Uit interview blijkt dat de procedure is dat de definities op wekelijkse basis geüpdate worden. Deze update vindt manueel plaats.
Het CIOT is van plan om het update proces te automatiseren. Hiervoor is een offerte aangetroffen.

Aanbeveling
Het manueel updaten van de virusscanner brengt het risico mee dat door bijvoorbeeld de afwezigheid van een beheerder de virusscanners tijdelijk niet meer up to date zijn. Daarnaast is het door een onvolledige logging niet te controleren of het update proces het gehele jaar goed heeft gewerkt. Aanbeveling is dan ook om het proces te automatiseren en de logging zo in te richten dat het proces ook controleerbaar is.

4.5 Autorisatiematrix

Norm
CIOT verifieert periodiek de uitgegeven autorisaties aan de hand van een autorisatiematrix.

Bevinding
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 waren geen bevindingen over.
Voor de CIOT organisatie is een start gemaakt met het beschrijven van de autorisatiematrix. Tot op heden is deze er alleen voor de kantoor automatisering (KA) omgeving. Het is de bedoeling om ook de ontwikkel-, test-, acceptatie-, en productieomgeving (OTAP) hierin mee te nemen.
Het autorisatiebeheer vindt nu nog separaat plaats op de vier genoemde omgevingen (OTAP). De intentie is dat dit in de toekomst via 1 Active Directory plaatsvindt (Project inrichten OTAP)

Aanbeveling
Het CIOT is gestart met een autorisatiematrix. Met deze matrix is vooraf duidelijk welke autorisaties er bij welke functie en/of rol hoort. Daarnaast kan de matrix gebruikt worden als norm voor een periodieke controle. Aangezien de matrix nu alleen is opgesteld voor de KantoorAutomatisering-omgeving dient deze ook opgesteld te worden voor de OTAP omgeving. De werkelijk uitgegeven autorisatie dienen periodiek (per kwartaal) aantoonbaar gecontroleerd te worden aan de hand van de autorisatiematrix.

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 gerapporteerde verantwoording over de bevragingen overeenkomt met de rapportages uit het systeem. De verantwoording over de bevragingen is opgenomen in het document "Jaarverslag 2010 gebruik CIS"

In onze audit hebben wij het totstandkomingsproces van de jaarcijfers gecontroleerd aan de hand van de rapportagefunctie "Jaarverslag" van het CIS. Daarnaast hebben wij ook een controle gedaan op de maandelijkse rapportagefunctie van het systeem. Uitkomst van onze audit is dat de gepubliceerde jaarcijfers overeenkomen met de jaarcijfers die het systeem genereert.
Hoewel het totstandkomingsproces van de jaarcijfers voldoet aan de eisen, plaatsen wij een kanttekening bij de juistheid en volledigheid van de rapportage vanwege de omissies geconstateerd in het testtraject (zie 4.3.4).