Ministerie van Justitie

Eindrapport Audit CIOT 2009

Een follow-up audit naar de opvolging van de aanbevelingen uit de audit 2008 door de telecommunicatieaanbieders, de BOID's en het CIOT.

Versie 1.0

Datum	19 april 2010
Status	definitief

Colofon

Afzendgegevens	**Departementale Auditdienst** Kalvermarkt 53 2511 CB Den Haag Postbus 20301 2500 EH Den Haag www.justitie.nl
Contactpersoon	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 Follow-upCIOT 2009
Ons kenmerk	DDS/5651078/10
Bijlage(n)	-
Auteurs	dhr. drs. J. van Luttikhuizen RE RA dhr. mr. drs. J. Roodnat RE RA

Inhoud

Managementsamenvatting en Conclusies

Aanleiding
Recentelijk heeft de Directeur Instrumentatie Rechtspleging en Rechtshandhaving van het Ministerie van Justitie, tevens voorzitter van de Commissie van Advies Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT), ons gevraagd een follow-up audit te doen naar de mate waarin de aanbevelingen uit de audit over 2008 zijn opgevolgd.

In de periode van 1 december 2009 tot en met 28 februari 2010 zijn zes aanbieders van telecommunicatiediensten, acht (Bijzondere) Opsporings- en Inlichtingendiensten en het Centraal Informatiepunt Onderzoek Telecommunicatie bezocht. Bij het onderzoek is getoetst of er – gemeten naar de situatie eind 2009 - in voldoende mate acties zijn ondernomen op die punten, die bij de betreffende aanbieders onvoldoende waren én tevens concrete aanbevelingen ter verbetering waren gegeven. Voor de individuele actoren hebben wij daarbij de gespreksverslagen 2008 inclusief bijlagen als uitgangspunt genomen. In zijn algemeenheid constateren wij daarbij overigens wel dat niet alle aanbevelingen zoals opgenomen in het “Overzicht van aanbevelingen uit de audits” in het eindrapport 2008 als zodanig in de gespreksverslagen en bijbehorende bijlagen aan de orde kwamen.

Wij willen alle betrokkenen bedanken voor een prettige samenwerking.
Hierna treft u onze samenvattende conclusies aan.

Conclusie onderzoek aanbieders telecommunicatie
De aanbevelingen uit de audit 2008 waarvan de follow–up is onderzocht hadden met name betrekking op de getroffen algemene organisatorische maatregelen en procedures en de kwaliteit van de met het CIOT uitgewisselde gegevensbestanden.

Bij de audit 2009 hebben wij vastgesteld dat de in 2008 bij de bestandsanalyses – door de toenmalige auditor - gesignaleerde afwijkingen door de betreffende aanbieders zijn opgepakt en onderzocht. Waarnodig hebben herstelacties en aanpassingen plaatsgevonden. Voor het overige was geen sprake van een fundamenteel gewijzigde situatie ten opzichte van 2008.

Periodieke visitatie van bestanden op een structurele wijze door de aanbieders zelf vindt niet plaats, omdat daartoe intern geen directe noodzaak wordt gevoeld. Verder stellen wij vast dat ook de aanbevelingen tot het meer specifiek maken van de algemeen organisatorische procedures en richtlijnen geen follow-up krijgen. Vanuit de providers komt het signaal dat men dat als overbodig ziet, tenzij daar vanuit bedrijfsvoering en risicoafwegingen specifiek aanleiding toe is. Er is sprake van een vrijwel volledig geautomatiseerd proces waar relatief weinig wijzigingen in plaatsvinden en de normale bedrijfsbreed geldende procedures gericht op betrouwbare werking en beveiliging worden toereikend geacht.

Op zich kunnen wij ons in de gegeven argumentatie vinden, maar wij vinden het wel belangrijk dat in ieder geval voorzien wordt in een adequate centrale registratie van no-hits. No-hits geven een kwaliteitsindicatie voor wat betreft aangeleverde bestanden. Wanneer deze no-hits bij aanbieders (relatief) vaker voorkomen respectievelijk wanneer zij een bepaald nader vast te stellen percentage overschrijden, dan kan (gezamenlijk) nader analyse en onderzoek plaatsvinden.

Conclusie onderzoek BOID's

Bij de BOID's hebben wij een zeer wisselend beeld over de mate van follow-up. Aanbevelingen zijn in verschillende mate opgepakt en er bestaan in verschillende mate intenties omdat (alsnog) te doen.
Voor drie belangrijke punten waarop aanbevelingen zijn gedaan naar aanleiding van de audit 2008, te weten het delegeren van bevoegdheden en de formele autorisatie, de rechtsgrondslagen en de rechtmatigheid van bevragingen en de documentatie van de werkwijze en de instructies, is de situatie voor 2009 bij het merendeel van de BOID' s (vrijwel) ongewijzigd. De aanbevelingen op deze punten blijven dan ook nog onverkort van kracht. Aanvullend bevelen wij aan om nadere handreikingen te doen met betrekking tot het interpreteren van en omgaan met het begrip rechtmatigheid gezien de behoefte die op dit punt van de zijde van de BOID's is geuit.

Voor wat betreft de overige aanbevelingen is het beeld over de mate waarin zaken zijn opgepakt en verbeterd meer gevarieerd. Voor al die aanbevelingen geldt echter dat zij vrijwel allen voor meerdere BOID 's van toepassing blijven.

Conclusie onderzoek CIOT

De overall conclusie in het eindrapport over 2008 was dat het CIOT en het ondersteunende CIOT Informatiesysteem CIS voldeden aan de daaraan te stellen eisen. Desalniettemin zijn een aantal aanbevelingen gedaan om identificatie en autorisatie, de controles ten aanzien van de integriteit van aangeleverde gegevens en de beschikbaarheid en continuïteit te verbeteren. Ook de actualisatie van de afspraken met gebruikers van data verdiende aandacht.
Bij de audit 2009 hebben wij vastgesteld dat ten aanzien van de eerste twee punten een redelijke mate van follow-up heeft plaatsgevonden. Aan een aantal mogelijke verbeteringen is concreet invulling gegeven. De aanbevelingen inzake beschikbaarheid en continuïteit (uitwijk in geval van calamiteiten) en het actualiseren van afspraken met gebruikers zijn nog niet (volledig) gerealiseerd en blijven nog van toepassing.

Toekomstige audits

Om de administratieve lasten zoveel mogelijk te beperken is door het college van Advies de intentie uitgesproken om over een aantal jaren zoveel mogelijk gebruik te maken van de werkzaamheden van interne auditdiensten. Daarvoor moeten echter de relevante processen in het kader van het Besluit verstrekking gegevens telecommunicatie wel specifiek en structureel object van onderzoek zijn. Verder dient de scope van de werkzaamheden toereikend te zijn en moeten uitkomsten ook schriftelijk worden vastgelegd. In de huidige situatie is dit bij geen der onderzochte actoren het geval. Indien er brede ondersteuning is om op termijn tot de "gewenste" situatie te komen, dan zullen daarover met de onderscheiden actoren (aanbieders van data, CIOT en gebruikers van data) nadere (concrete afspraken moeten worden gemaakt. Daarbij zal naar onze mening een zekere differentiatie nodig zijn op grond van nadere risicoanalyse. De genoemde actoren hebben in het proces immers een geheel verschillende positie en rol met een eigen context en eigen accenten als het gaat om belangrijke risico's en het afleggen van verantwoording.

Wel blijft het naar onze mening belangrijk invulling te geven aan de aanbevelingen uit 2008 om nadere afspraken tussen partijen te maken en vast te leggen in de Auditovereenkomst over de wijze van uitvoering van de audits, het visiteren van bestanden en het creëren van randvoorwaarden waaronder bewijsmateriaal over het rechtmatig handelen kan worden verzameld en de rechtmatigheid ook feitelijk kan worden vastgesteld rekening houdend met de geldende wet- en regelgeving.

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.

Naar aanleiding van het eindrapport over 2008 en de in dat rapport opgenomen aanbevelingen heeft de opdrachtgever aan de Rijksauditdienst verzocht om een follow-up onderzoek in de stellen. Bij dit onderzoek dient te worden vastgesteld in welke mate door de onderscheiden actoren de diverse aanbevelingen zijn opgevolgd, uiteraard voor zover die aanbevelingen op hen van toepassing waren.

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 ((B) OID's)

Het opvragen van gegevens met betrekking tot diensten telecommunicatie 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 Inlichtingen – en veiligheidsdiensten (WIV);
- Artikel 10.10 van de Telecommunicatie Wet (TW).

1.4 Centraal Informatiepunt Onderzoek Telecommunicatie

Het Centraal Informatiepunt Onderzoek telecommunicatie (CIOT) is een onafhankelijk onderdeel van het Ministerie van Justitie en draagt er voor zorg dat de gegevens van de aanbieders van telecommunicatiediensten worden doorgeleid naar de (B)IOD's. Hierbij worden alleen die gegevens aan de (B)IOD's verstrekt die expliciet zijn opgevraagd.

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.

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

1.5 Autorisaties van de Officier van Justitie

De artikelen 126n en 126u geven de Officier de mogelijkheid te “bevelen”, te “vorderen”, etc. dat gegevens met betrekking tot telecommunicatie beschikbaar worden gesteld voor opsporingsdoeleinden. Deze “bevelen” en “vorderingen” worden bij opsporingsdiensten vrij algemeen geduid met “machtiging van de Officier van Justitie”.

Aangezien de termen “vordering”, “bevel” en “machtiging” een juridische betekenis hebben, kan het gebruik van de term “machtiging” mogelijk een verkeerde indruk oproepen. In de context van deze rapportage maken wij daarom gebruik van de term “autorisatie van de Officier van Justitie” voor het document waarmee de Officier van Justitie (mede) het opvragen van gegevens van telecommunicatievoorzieningen ex artikel 126n en 126u WvS goedkeurt.

2 UITVOERING

2.1 Audit

In overleg met de opdrachtgever van deze audit, de Directeur Instrumentatie Rechtspleging en Rechtshandhaving van het Ministerie van Justitie, tevens voorzitter van de Commissie van Advies CIOT, is besloten de audit 2009 te beperken tot de 6 providers en 8 opsporingsdiensten onderzocht in 2008 en het CIOT. Verder is de reikwijdte van de audit 2009 beperkt tot de follow-up van de aanbevelingen ter verbetering, zoals die gegeven zijn door de toenmalige auditor

In de periode van 1 december tot en met 28 februari 2010 zijn 6 aanbieders van telecommunicatiediensten, 8 (bijzondere) opsporingsdiensten en het CIOT bezocht. Aangezien de audit betrekking heeft op het jaar 2009 is de stand van zaken bij de onderscheiden actoren eind december 2009 als uitgangspunt gehanteerd.
De audit heeft zich in principe beperkt tot interviews en dossierreview. Gegevensbestanden van aanbieders op of rond de datum van het bezoek zijn alleen onderzocht indien dat op dat moment technisch mogelijk was en relevant werd geacht voor het vormen van een oordeel over de mate van follow-up van de aanbeveling(en).

2.2 Rapportage

In de Auditovereenkomst Staat Aanbieders 2006 is in artikel 3, lid 1, bepaald dat de rapportage van de audit wordt uitgebracht aan de Minister van Justitie. De rapportage bestaat uit een rapport op hoofdlijnen met conclusies en aanbevelingen. Daarnaast zijn voor de opdrachtgever afzonderlijke notities van bevindingen per onderzocht object/ betrokken partij beschikbaar.

In lijn met artikel 3 lid 2 zijn de notities van bevindingen met daarin opgenomen de conclusies en aanbevelingen uitsluitend met de betreffende onderzochte partij besproken. Dit rapport vormt het hiervoor bedoelde rapport op hoofdlijnen. De bevindingen en aanbevelingen zijn niet herleidbaar naar een specifieke partij, met uitzondering van de bevindingen en aanbevelingen ten aanzien van het CIOT. Dit rapport is derhalve zodanig opgesteld en geformuleerd dat dit in beginsel ook geschikt is om te publiceren en derhalve bekend te maken aan derden.

3 AANPAK

3.1 Normenkader

Door ons is het bij de audit over 2008 toegepaste normenkader gehanteerd. Uitgangspunt bij dit normenkader is geweest het voldoen aan de geldende wet – en regelgeving, de Service Level Agreements (SLA) en verder vastgelegde afspraken. Het normenkader bestaat uit 3 afzonderlijke onderdelen, te weten een onderdeel voor de aanbieders van telecommunicatiediensten, voor de (B)IOD's, en voor het CIOT. In het normenkader zijn verwijzingen naar de gebruikte documentatie opgenomen.

3.2 Aanbieders van telecommunicatiediensten

In 2008 is een audit uitgevoerd naar de naleving door de aanbieders van hun verplichtingen over de periode 1 januari 2008 tot en met 31 augustus 2008. Bij die audit zijn aan de hand van een vastgesteld generiek normenkader de volgende beheersmaatregelen getoetst:

- Beheersmaatregelen rondom aanleverproces richting CIOT (gericht op de kwaliteitsaspecten betrouwbaarheid, integriteit, exclusiviteit en non repudiation);
- Logische toegangsbeveiliging tot de omgeving waar de extractie uit de bedrijfsgegevens plaatsvindt. Ongeautoriseerde medewerkers dienen de gegevensverstrekking aan het CIOT niet (on)opzettelijk te kunnen raadplegen, muteren en/of verstoren;
- Aanwezigheid van onafhankelijke auditrapporten en de uitkomsten hiervan.

Voor deze follow-up audit zijn slechts die normen uit het voor 2008 goedgekeurde en toegepaste normenkader in het onderzoek betrokken die bij de audit 2008 niet of slechts gedeeltelijk aan de gestelde norm voldeden én ten aanzien waarvan één of meer aanbevelingen zijn gedaan.

Onderzoek naar bestanden bij telecommunicatieaanbieders heeft slechts plaatsgevonden in die situatie waarbij dit relevant en noodzakelijk werd geacht om de effecten van de doorgevoerde verbeteringen naar aanleiding van de gedane aanbevelingen te kunnen beoordelen. In die laatste situatie zijn 3 tot 5 bestanden van op of rond de datum van het bezoek aan die aanbieder op ons verzoek veiliggesteld en nader onderzocht.

3.3 (Bijzondere) Opsporings- en Inlichtingendiensten

In de audit 2008 is onderzoek uitgevoerd naar de naleving door afnemers van telecommunicatiegegevens van hun verplichtingen. Daarbij is onderzocht of het opvragen van gegevens via het CIOT Informatiesysteem (CIS) is gebeurt op de juiste wijze en met de juiste rechtsgrondslag.

Bij het onderzoek 2008 is door de auditor de volgende aanpak gehanteerd:

- Vaststellen van de aanwezigheid van lokale procedures voor het bevragen van het CIS;
- Vaststellen dat deze procedures ook worden opgevolgd;
- Steekproefsgewijs vaststellen dat het bevragen conform de procedure en rechtmatig heeft plaatsgevonden.

Daarbij is als toetsingskader gehanteerd een minimale set aan beheersingsmaatregelen zoals in de "Blauwdruk bevragingen via het CIOT-systeem" en "Referentie procesbeschrijving Bevraging met behulp van CIOT" welke elke (B) OID moet implementeren.

Op die punten waar bij de audit over 2008 verbeteringen noodzakelijk werden geacht en aanbevelingen zijn gedaan aan de individuele (B)IOD's hebben wij bij die betreffende (B)OID's waar deze punten aan de orde waren in de follow-up audit 2009 nader onderzoek verricht.

3.4 Centraal Informatiepunt Onderzoek Telecommunicatie

In de audit CIOT over 2008 is onderzoek uitgevoerd naar het voldoen van het CIOT aan de wet –en regelgeving, zoals Besluit Verstrekking Gegevens Telecommunicatie, VIR, VIR/BI en de WBP. Verder is onderzocht hoe het CIOT zorgt voor een juiste, tijdige, en volledige afhandeling van het vraag – en antwoordverkeer, alsmede de beveiliging van de omgeving van waaruit de opvraging uit het CIS plaatsvindt.

De audit over 2009 heeft zich uitsluitend gericht op die punten uit die audit 2008 waarop verbetering nodig werd geacht en aanbevelingen zijn gedaan.

4 Resultaten van de follow-up audit bij de aanbieders van telecommunicatiediensten

4.1 Nakoming Besluit Verstrekking Gegevens Telecommunicatie

Sinds 2008 dienen de aanbieders van telecommunicatie hun gegevens in een XML bestand aan te leveren. Door middel van het gebruik van XML kunnen een aantal restricties ten aanzien van de vorm en in te voeren waarden toegepast worden en kan een zekere toetsing van de plausibiliteit van gegevens plaatsvinden. Bij de visitatie van de bestanden over 2008 door de betreffende auditor zijn onder meer lege velden, onjuiste velden, dubbele records en niet plausibele waarden geconstateerd, alsmede afwijkingen tussen gegevens in het CIOT –bestand en gegevens in de bedrijfsvoeringssystemen van de verstrekker van de gegevens. Op grond daarvan is op dat moment geconcludeerd dat niet altijd even zorgvuldig met het genereren van gegevensbestanden werd omgegaan.

Op grond van de constateringen en conclusies naar aanleiding van de bestandsvisitatie is aan de aanbieders van telecommunicatiediensten geadviseerd om:

1. Met een analysetool periodiek een bestandsanalyse uit te voeren op het gegevensbestand ter controle van de inhoud van dit bestand;
2. Bestanden voorafgaand aan de overdracht te controleren aan de hand van de XSD schema's;
3. Analyses uit te voeren naar de oorzaak van no-hits en eventueel daarin gevonden structurele fouten op te lossen.

Bij de follow-up audit hebben wij geconstateerd dat aan deze aanbevelingen door de telecommunicatieaanbieders - voor zover deze voor hen van toepassing waren - geen verdere invulling is gegeven. Vanuit de aanbieders komt het signaal dat zij twijfelen aan toegevoegde waarde en noodzaak, gezien de aard, omvang en oorzaken van het bij de visitaties geconstateerde. Daarbij worden onder meer de volgende belangrijke afwegingen/overwegingen genoemd:

1. Aanmaken CIOT -bestanden is een volledig geautomatiseerd proces waarop de normaal geldende procedures en maatregelen ter borging van de kwaliteit van toepassing zijn;
2. De zaken die geconstateerd zijn, zijn grotendeels verklaarbaar en niet van een zodanige omvang dat gestructureerde preventieve actie in de vorm van periodieke bestandsonderzoeken noodzakelijk worden geacht. Wel adequaat snel oplossen van (structurele) zaken wanneer die geconstateerd worden;
3. Ook gestructureerde analyses naar oorzaken van no -hits worden niet noodzakelijk geacht. Adequaat reageren op interne dan wel externe signalen ten aanzien van onjuiste/ onvolledige gegevens acht men gezien de omvang van de problematiek meer gepast.

Voor wat betreft de eerste twee afwegingen/overwegingen kunnen wij de redenering en aangevoerde argumentatie in principe onderschrijven. Wel achten wij het van belang dat no-hits (bij voorkeur ook centraal) worden vastgelegd zodat inzicht wordt verkregen in de (relatieve) omvang per provider. Dit geeft een indicatie omtrent de kwaliteit van de aangeleverde bestanden.
Wanneer deze no-hits (een) aanbieder(s) (relatief) vaker voorkomen respectievelijk wanneer zij een bepaald nader vast te stellen percentage overschrijden, dan kan (eventueel gezamenlijk) nader analyse en onderzoek plaatsvinden.

4.2 Integriteitcontroles van de bestandsuitwisseling tussen telecommunicatieaanbieders en CIOT

Naar aanleiding van de bevindingen bij de audits 2008 zijn richting sommige aanbieders aanbevelingen gedaan om plausibiliteitstesten met behulp van de door CIOT beschikbaar gestelde XSD- schema's uit te voeren. Zoals hiervoor al opgemerkt wordt hieraan -bij die aanbieders waar deze aanbeveling van toepassing is - geen verdere invulling gegeven om genoemde redenen. Verder zijn aanbevelingen gedaan om de integriteit van de uitwisseling van gegevens te verbeteren en ook te kunnen vaststellen.
Van de zijde van het CIOT is op dat punt in maatregelen voorzien (zie 6.1).

4.3 Algemeen organisatorische maatregelen aan de zijde van de aanbieders

Algemene organisatorische procedures en beheersmaatregelen moeten garanderen dat de bestanden conform SLA juiste, volledige en tijdige gegevens uit de bedrijfsvoeringssystemen van de aanbieder in continuïteit en tijdig aan het CIOT worden aangeleverd. Naar aanleiding van de bevindingen tijdens de audit 2008 werd daarbij specifiek aandacht gevraagd voor het installeren van actuele antivirus- programmatuur en het tijdig vooraf melden aan het CIOT van wijzigingen in de infrastructuur en de programmatuur voor de generatie van het CIOT- bestand. Deze aspecten waren echter in de gespreksverslagen 2008 van de bezochte providers geen issue.

De relevante algemene organisatorische procedures en beheersmaatregelen zijn algemeen en bedrijfsbreed geldend. Zij vallen onder de reguliere intern en/of extern uitgevoerde bedrijfsaudits (IT-audits, SOx-compliance audits etc.), indien die worden uitgevoerd, gezien de omvang van de provider. Er wordt zeker niet door alle providers een noodzaak gevoeld tot het opstellen van specifieke procedures en richtlijnen ten aanzien van de verstrekking van gegevens aan het CIOT of het uitvoeren van specifieke intern gerichte dan wel externe audits ten aanzien van het CIOT -proces. Dit omdat het een verregaand geautomatiseerd proces betreft met relatief weinig wijzigingen, dat verder in de ogen van de providers behoort te voldoen en voldoet aan eigen bedrijfsbrede procedures en richtlijnen als het gaat om aspecten als vertrouwelijkheid en beveiliging.

4.4 Conclusie aanbieders van telecommunicatiediensten

Op basis van de bevindingen uit onze follow-up audit concluderen wij, dat de bij de verschillende aanbieders bij de visitatie van de gegevensbestanden met IDEA in 2008 geconstateerde afwijkingen/verschillen adequaat aandacht hebben gekregen. Daarbij zijn in het algemeen waarnodig correcties doorgevoerd en aanpassingen gedaan. Voor de overige concrete aanbevelingen 2008 constateren wij dat er geen sprake is van een fundamenteel gewijzigde situatie. Daarbij tekenen wij aan dat op diverse openstaande punten (gearceerd en rood gekleurd in het overzicht) de noodzaak tot wijzigen en verbeteren van werkwijze niet algemeen gevoeld en onderschreven wordt. Redenering en aangevoerde argumentatie kunnen wij in principe onderschrijven. Wel vinden wij centraal inzicht in aantallen no-hits relevant als indicatie van de kwaliteit van aangeleverde bestanden. Wanneer het aantal no-hits een bepaald percentage overschrijdt dan wel de relatieve omvang van het aantal no-hits per provider daartoe aanleiding geeft dan kan desgewenst (gezamenlijk) actie worden ondernomen en nader analyse en onderzoek plaatsvinden. Op de betreffende punten is dan ook nadere dialoog en besluitvorming in de Commissie van Advies gewenst, zodat beargumenteerd en rekeninghoudend met administratieve lasten, nut en eventuele risico's, een standpunt kan worden ingenomen.

5 Resultaten van de follow-up audit bij de BOID's

5.1 Delegatie van bevoegdheden en formele autorisaties

Bij de audits 2008 is geconstateerd dat medewerkers belast met CIOT bevragingen formeel niet waren aangewezen als "bevoegde autoriteit". Bij de audit 2009 hebben wij geconstateerd dat bij enkele BOID's deze formele aanwijzing inmiddels heeft plaatsgevonden en nu op orde is. Bij andere BOID's moet dit aspect nog steeds worden geregeld zodat dit een punt van aandacht blijft.

Voor wat betreft de autorisatie van CIOT- bevraging ex 126n en 126u WvS zijn aanbevelingen gedaan om de juiste werkwijze inzake het verkrijgen van deze autorisaties onder de aandacht van de medewerkers te brengen en een meer eenduidig gebruik te bevorderen. Bij de audit 2009 hebben wij op dit punt een situatie aangetroffen vergelijkbaar met 2008 zodat voor de meeste BOID's deze aanbevelingen eveneens nog onverkort van toepassing blijven.

5.2 Rechtsgrondslagen en rechtmatigheid van bevragingen

Het is van essentieel belang dat het doen van CIOT bevragingen door de geautoriseerde ambtenaar rechtmatig plaatsvinden. Op dat punt zijn naar aanleiding van de audit als aandachtspunten geformuleerd:

- het zorg dragen voor voldoende inzicht in de geldende wet – en regelgeving bij de betreffende ambtenaren;
- het gebruik van de juiste rechtsgrondslagen bij bevraging van data door het CIOT;
- het zodanig vastleggen en documenteren van de bevragingen dat die rechtmatigheid ook achteraf kan worden aangetoond.

Een complicatie ten aanzien van het achteraf kunnen vaststellen van de rechtmatigheid op basis van vastleggingen en documenten is dat dit in de meeste gevallen niet centraal zal kunnen geschieden maar dat bewaking en toetsing decentraal zal moeten plaatsvinden. Naar onze mening is het creëren van een situatie waarin bewaking en toetsing te allen tijde centraal kan plaatsvinden gewenst. Er zijn voorbeelden van opsporingsdiensten waar een (centrale) 100% (interne) controle wordt gerealiseerd.

Bij de audit in 2009 hebben wij vastgesteld dat bij sommige BOID's op het punt van het gebruik van de juiste rechtsgrondslagen de situatie is verbeterd en aanbevelingen zijn opgevolgd. Wel zou geautoriseerd en juist gebruik verdergaand geautomatiseerd kunnen worden afgedwongen. Over de gehele linie genomen constateren wij bij de BOID's een situatie vergelijkbaar met 2008.

De aanbevelingen blijven dus onverkort van kracht en dienen naar onze mening met hoge prioriteit te worden aangepakt.

Wij constateren dat er geen eenduidigheid bestaat over het begrip rechtmatigheid en dat sprake is van verschillende beelden/interpretaties. Vanuit de BOID's is dan ook de behoefte kenbaar gemaakt aan een nadere concrete invulling van dit begrip en aan richtlijnen hoe zij dit kunnen vaststellen.

5.3 Documentatie van werkwijze en instructie

Een goede documentatie van werkwijze en instructie van medewerkers moet waarborgen dat een juiste werkwijze wordt gehanteerd bij het doen van CIOT bevragingen. Bij enkele BOID's zijn naar aanleiding van de audit 2008 aanbevelingen gedaan om dit te verbeteren.

Bij de audit over 2009 hebben wij geconstateerd dat de situatie nog voor het overgrote deel ongewijzigd is en dat dit aandachtspunt bij de betreffende BOID's nog de nodige follow-up dient te krijgen.

5.4 Overige aanbevelingen

Voor de overige aanbevelingen 2008 hebben wij een zeer wisselend beeld omtrent de mate van follow-up. Bij sommige BOID's hebben wij een voldoende mate van follow-up en verbetering kunnen constateren. Bij andere BOID's daarentegen moet dit nog gebeuren en is de situatie grosso modo nog ongewijzigd.
Ook ten aanzien van die aanbevelingen geldt echter dat zij vrijwel allen voor meerdere BOID 's van toepassing blijven.

5.5 Conclusie (Bijzondere) Opsporings- en Inlichtingendiensten

Bij ons onderzoek over 2009 hebben wij geconstateerd dat sommige BOID's de aanbevelingen duidelijk hebben opgepakt en zaken substantieel hebben verbeterd. Tevens hebben wij echter moeten vaststellen dat bij andere BOID's dit nog moet gebeuren waarbij er in meer dan wel mindere mate (concrete) voornemens zijn om dat in 2010 te doen. Het eenvoudig kunnen vaststellen van de rechtmatigheid van de CIOT bevragingen, documentatie van werkwijze en instructie van medewerkers, juist gebruik van rechtsgrondslagen en het ontdoen van het proces van overbodige documenten blijven dan ook zaken die bij meerdere BOID"s de nodige aandacht verdienen. Verder komt vanuit de BOID's het signaal dat behoefte bestaat aan een concrete invulling van het begrip rechtmatigheid en richtlijnen hoe dit vast te stellen.

6 Resultaten van de follow-up audit bij het CIOT

6.1 Controle integriteit aangeleverde bestanden

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.

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 van de zijde van het CIOT wijzigingen in technische infrastructuur en systeem tijdig en goed worden gecommuniceerd richting aanbieders.

Om geheel zeker te zijn van de integriteit van de ontvangen bestanden adviseren wij om naast de encryptie ook het signen te overwegen. Hierbij dient wel rekening te worden gehouden met een extra beheerlast door het CIOT in de vorm van het bijhouden van alle Public Keys van de aanbieders. Door het activeren van het signen is het mogelijk dat de beschikbaarheid negatief wordt beïnvloed door het niet up-to-date hebben van alle public keys. Dit is niet ondenkbaar gezien de mutaties van aanbieders. Indien niet voor signen wordt gekozen dient expliciet het geringe restrisico geaccepteerd te worden.

De mate van volledigheid en de juistheid van de gegevens in de CIOT bestanden in de zin van het overeenkomen van deze gegevens met de in de bedrijfsvoering bij de aanbieders aanwezige gegevens zal alleen op basis van random steekproeven kunnen worden vastgesteld voor die aanbieders die in de periodieke audit dan wel de review van de interne audit vallen.

6.2 Logging en monitoring

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.

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 maar een en ander is nog niet (volledig) afgerond. Derhalve blijven de aanbevelingen uit 2008 nog deels relevant.

6.3 Calamiteiten- en uitwijkplan

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 deze is nog niet operationeel en gereed voor uitwijk.

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

6.4 Service Level Agreements

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 die nog niet beschreven zijn in de SLA’s worden gecommuniceerd.

De aanbeveling uit 2008 om de SLA zelf te actualiseren blijft derhalve van kracht.

6.5 Overige aanbevelingen 2008

De aanbevelingen vermeld in het overzicht 2008 vermeld onder 7. 8, 7.10 en 7.14 met betrekking tot het gebruik van kenmerken en rechtsgrondslagen, testbevragingen en administratieve lasten zijn tijdens deze audit niet aan de orde geweest omdat zij in het gedetailleerde verslag van bevindingen niet waren opgenomen. De overige aanbevelingen inzake het aanvragen van gebruikersnamen en -certificaten, intrekken van gebruikersaccounts en handtekeningenlijsten lokaal beheerders hebben voldoende follow-up gekregen. De gesignaleerde risico’s tijdens de audit op deze punten zijn inmiddels geheel dan wel voor een groot deel weggenomen.

6.6 Conclusie CIOT

De overall conclusie in het eindrapport over 2008 was dat het CIOT en het ondersteunende CIOT Informatiesysteem CIS voldeden aan de daaraan te stellen eisen. De aanbevelingen uit de audit 2008 waren met name aanbevelingen bedoeld ter verdere verbetering.
Bij deze follow-up audit hebben wij vastgesteld dat ten aanzien van een aantal mogelijke verbeteringen invulling is gegeven. Voor andere aanbevelingen geldt dat er inmiddels lopende activiteiten zijn om tot verbetering te komen of in 2010 gepland staan. Er is in zijn algemeenheid sprake geweest van een redelijke follow-up zij het dat wij een per aanbeveling een wisselend beeld hebben van de mate waarin dat is gebeurd. Een aantal aanbevelingen blijft dan ook voor 2010 nog relevant.

7 Toekomstige audits

Jaarlijks dient door de Minister van Justitie een verslag te worden opgesteld van een audit naar de goede uitvoering van het Besluit verstrekking gegevens telecommunicatie door de aanbieders van openbare telecommunicatiediensten of van openbare telecommunicatienetwerken, het informatiepunt, de arrondissementsparketten en de politiekorpsen of ander opsporingsdiensten. Daarbij dient tenminste aan de orde te komen de werking van het systeem, de kwaliteit van de verstrekking van gegevens en de bevraging van gegevens (artikel 8 lid 2 van het Besluit verstrekking gegevens telecommunicatie).
Om de administratieve lasten te beperken is in 2009 in de Commissie van Advies CIOT afgesproken om de administratieve en controlelast voor de organisaties te verminderen door niet jaarlijks de controle “opnieuw” te doen, maar te gaan kijken naar de follow-up van de aanbevelingen en partieel roulerend de audits uit te voeren bij de aanbieders en de BOID’s. Verder is het voornemen uitgesproken om over een aantal jaren zoveel mogelijk te steunen op onderzoeken van interne auditdiensten naar aanleiding van een voorstel van deze strekking ingebracht in de Commissie van Avies in maart 2009.

Gegeven dit uitgangspunt hebben wij op basis van onze bevindingen en ervaringen bij de follow-up audit 2009 de volgende kanttekeningen:

- Indien het de wens is om in de toekomst bij partieel roulerende audits zoveel mogelijk gebruik te maken van de onderzoeken van interne auditdiensten dan zullen de relevante processen in het kader van de uitvoering van het Besluit verstrekking gegevens telecommunicatie specifiek en structureel object van onderzoek zijn voor de betreffende interne auditdiensten. Ook zullen in dat geval de uitkomsten schriftelijk moeten worden vastgelegd en voorzien van een oordeel. Het ligt verder voor de hand om de verschillende categorieën van actoren op grond van verschillen in belang en risicoafweging verschillend te benaderen en ook gedifferentieerde afspraken te maken. Voor de aanbieders geldt immers dat het aanleveren van bestanden geautomatiseerd geschied en dat slechts beperkt sprake zal zijn van wijzigingen in die processen. Daarbij zullen zij vanuit een eigen perspectief en belang zonder meer zorgvuldig en met voldoende mate van beveiliging met de eigen gegevens omgaan en daarbij (willen) handelen conform de intern bedrijfsbreed geldende procedures. Het CIOT zal daarentegen een zorgvuldig beheer conform het afgesproken beveiligingsniveau moeten realiseren en dat ook moeten aantonen zowel richting de aanbieders die de gegevens verstrekt hebben als richting de samenleving in het algemeen. De gebruikers (BOID’s) zullen zich ten slotte naast het zorgvuldig omgaan met de verkregen gegevens vooral moeten kunnen verantwoorden over het (rechtmatig) verkrijgen en gebruik van die gegevens.

- Indien en voor zover gebruik wordt gemaakt van de werkzaamheden van interne auditdiensten zal:

    1. de scope van de werkzaamheden bij de aanbieders zowel betrekking moeten hebben op de processen zelf als op de kwaliteit van de uitgewisselde gegevensbestanden. Dit laatste kan bijvoorbeeld worden vastgesteld door middel van periodieke visitatie van die bestanden.
       In de huidige situatie is dit nog geenszins het geval.
       Interne audits worden zeker bij de grotere dan wel hele grote organisaties (aanbieders) wel uitgevoerd maar deze (IT)audits hebben dan veelal een organisatiebreed karakter gericht op algemene maatregelen en procedures onder andere in het kader van SOx-compliancy of mogelijk ook audits in het kader van

ISO-certificering. Structurele audits op de kwaliteit van uitgewisselde gegevensbestanden vinden bij de door ons bezochte organisaties niet plaats.
2. voor de BOID's zal de scope van de werkzaamheden zowel betrekking moeten hebben op de kwaliteit van de processen bij bevraging van data als ook de vastleggingen en documentatie daarvan en het (steekproefsgewijs) (kunnen) vaststellen van de feitelijke rechtmatigheid van de individuele bevraging.

- Ook in de situatie dat gebruik kan worden gemaakt van de uitkomsten van interne audits blijft het van belang om conform de aanbevelingen 2008:

    1. in een auditprotocol nadere afspraken vast te leggen omtrent de wijze waarop de visitatie van de CIOT bestanden en het vaststellen van het overeenkomen van deze gegevens met de gegevens in de bedrijfsvoeringssystemen van de aanbieder kan plaatsvinden.
    2. voor de toekomstige periodieke onderzoeken bij de BIOD's randvoorwaarden te creëren waaronder bewijsmateriaal voor de rechtmatigheid kan worden verzameld en de rechtmatigheid van de bevraging ook feitelijk door de auditor kan worden vastgesteld, rekening houdend met wet- en regelgeving op het gebied van informatiebeveiliging.

Het verdient voorts aanbeveling om in de Commissie van Advies nadere afspraken te maken omtrent de periodiciteit van de uit te voeren audits. Aard en omvang van de organisatie alsmede het al dan niet verrichten van specifieke interne en/of externe audits door de betreffende betrokken actor kunnen daarbij van belangzijnde specifieke criteria zijn. Concreet betekent dit het nader uitwerken van een auditprotocol voor de onderscheiden categorieën van actoren ook als follow-up van het voorstel inzake de inrichting van de audit zoals ingebracht in de Commissie van Advies in maart 2009. Daarbij tekenen wij overigens aan dat de periodieke audits dienen plaats te vinden naast het uitvoeren van eventuele follow-up audits omdat follow-up audits noch inzicht kunnen geven in opzet en implementatie van proceswijzigingen en effecten daarvan op de kwaliteit noch inzicht bieden in de feitelijke werking van de processen gedurende het onderzochte jaar.

Tenslotte verdient het ook aanbeveling om afspraken te maken over de maximaal te accepteren afwijkingen als het gaat om de kwaliteit van bestanden en de minimaal vereiste kwaliteit als het gaat om de processen. De eis ten aanzien van de uitgewisselde gegevensbestanden in de in de SLA vastgelegde afspraken is op dit moment dat gegevens 100% overeenstemmen met de gegevens die de aanbieder gebruikt voor zijn bedrijfsvoering en dat deze voor 100% in het geleverde bestand zijn opgenomen. Hoewel het streven naar een hoge kwaliteit bij de onderzochte aanbieders aanwezig is en realisatie van een zeer hoge kwaliteit ook mogelijk door de vrijwel volledig geautomatiseerde processen zal het feitelijk foutloos zijn van bestanden waarschijnlijk een utopie zijn en blijven. Een centrale signalering en een "piepsysteem" ten aanzien van afwijkingen/omissie lijkt in deze situatie voor de hand te liggen. De vraag is dan welke afwijking acceptabel is alvorens tot nadere actie wordt overgegaan/ verplicht wordt gesteld.
Voor de processen geldt een min of meer gelijke principiële vraag als het gaat om aanbrengen van verdere kwaliteitsverbetering in die situatie waarin tevens is geconcludeerd dat proces/systeem aan de daaraan te stellen eisen voldoet zoals in het eindrapport audit CIOT 2008 verwoord in de conclusie over het CIOT proces/systeem. Het verder verbeteren van het proces komt dan in een ander perspectief te staan met een nadrukkelijker afweging van kosten/baten en risico's als het gaat om het doorvoeren van verbeteringen en het geven van follow-up aan aanbevelingen.

8 Stand van zaken aanbevelingen 2008 ultimo 2009

§	Overzicht aanbevelingen uit de audits 2008	Status eind 2009
	Aanbieders van telecommunicatiediensten	
5.1	**In het kader van de audit te onderzoeken objecten en aspecten**	
	De wijze waarop de visitatie van de CIOT bestanden door de auditor plaats kan vinden in de Auditovereenkomst vastleggen.	**4**
	Alternatief: de visitatie met de (interne) accountant van de aanbieder uitvoeren	**4**
5.2	**Gebruik XSD schema's**	
	Bestanden voorafgaand aan de overdracht te controleren aan de hand van de XSD schema's	**1**
5.3	**Afwikkeling no-hit faxen**	
	De no-hit procedure strikt naleven en onvolledige faxberichten retourneren naar de afzender zonder de gevraagde gegevens.	**4**
5.4	**Integriteit verzonden gegevensbestand**	
	De bestanden voor verzending voorzien van een checksum om te kunnen vaststellen of het bestand inhoudelijk andere informatie bevat dan de aanbieder heeft verzonden.	**3**
5.5	**Analyse en opvolging import logbestand**	
	Zowel bij de aanbieder als het CIOT analyse op het import logbestand uitvoeren om de aard en de impact van de foutmeldingen te kunnen vaststellen.	**1**
5.6	**Bestandanalyse en inhoudelijke juistheid bestanden**	
	Door de aanbieders periodiek uitvoeren van bestandsanalyse, door middel van een analysetool, op het gegevensbestand ter controle van de inhoud van dit bestand.	**1**
5.7	**Controle op besmetting met computervirussen**	
	Op de server waar de CIOT bestanden worden gegenereerd en verzonden actuele antivirus programmatuur installeren.	**4**
5.8	**Afwikkeling no –hits**	
	Analyseren van de oorzaak van no-hits en eventueel daarin gevonden structurele fouten oplossen.	**1**
5.9	**Melding wijziging infrastructuur aan het CIOT**	
	Iedere wijziging in de infrastructuur en de programmatuur voor de generatie van het CIOT- bestand vooraf melden aan het CIOT	**4**

§	Overzicht aanbevelingen uit de audits 2008	Status eind 2009
	Bijzondere Opsporings- en InlichtingenDiensten	
7.1	**In het kader van de audit te onderzoeken objecten en aspecten**	
	Landelijke richtlijnen te (laten) formuleren met betrekking tot meervoudige autorisaties ex artikel 126n WvS, zodat deze niet leiden tot formeel onrechtmatige bevragingen.	**4**
7.2	**Gegevens benodigd voor het verkrijgen van een autorisatie van de Officier van Justitie**	
	De juiste werkwijze ten aanzien van het verkrijgen van een autorisatie van de Officier van Justitie ex artikel 126n 126u WvS onder de aandacht van de betreffende opsporingsambtenaren brengen.	**1**
7.3	**Documentatie van de werkwijze rond bevragingen CIOT**	
	De BOID dient zijn lokale werkwijze rond bevragingen CIOT te documenteren en onder de aandacht van de gebruikers te brengen opdat de juiste werkwijze wordt gehanteerd.	**1**
7.4	**Controle op rechtmatigheid door de geautoriseerde ambtenaar**	
	De rechtmatigheidscontrole door de geautoriseerde ambtenaar laten uitvoeren, c.q. op andere wijze in het proces waarborgen dat bevragingen alleen op rechtmatige gronden kunnen worden uitgevoerd.	**1**
7.5	**Gebruik UserID's en certificaten**	
	De medewerkers instrueren dat een gebruikers -ID voor het netwerk als ook voor de CIOT webtoepassing, strikt persoonlijk is en dat deze nimmer aan andere personen mag worden verstrekt.	**2**
7.6	**Gebruik van CIOT accounts**	
	Het aantal medewerkers met toegang tot de CIOT webtoepassing beperken tot diegenen die daadwerkelijk regelmatig bevragingen uitvoeren.	**2**
7.7	**Aanvragen en activeren –certificaten**	
	De lokale beheerders attenderen op de noodzaak bij het activeren van het certificaat het "vinkje" te plaatsen voor het hoge beveiligingsniveau.	3
7.8	**Gebruik kenmerken en rechtmatigheidsgrondslagen**	
	Bij de bevragingen zorgvuldig omgaan met de keuze van de combinatie van rechtsgrondslagen en kenmerk.	**2**
7.9	**Identificerend kenmerk spoedprocedure**	
	Elke spoedbevraging voorzien van een uniek identificerend kenmerk.	**2**
7.10	**Testbevragingen**	
	Bevragingen die niet zijn gebaseerd op de daarvoor geldende rechtsgrondslagen separaat laten autoriseren door een daartoe aangewezen en bevoegde persoon.	**1**
	Gebruik voor training reguliere bevragingen	

§	Overzicht aanbevelingen uit de audits 2008	Status eind 2009
7.11	**Kennis wet – en regelgeving**	
	De medewerkers belast met het uitvoeren van bevragingen goed op de hoogte stellen en houden van de geldende wet- en regelgeving.	**1**
7.12	**Verstrekte autorisaties artikel 126n en 126u WvS**	
	Het landelijk op dezelfde wijze autoriseren van CIOT bevragingen in de door de OvJ verstrekte autorisaties ex artikel 126n en 126u WvS door het plaatsen van het daarvoor bedoelde kruisje.	**4**
7.13	**Administratieve lasten voor de BOID's**	
	Daar waar mogelijk het proces van het verstrekken van telecommunicatiegegevens ontdoen van onnodige documenten teneinde de administratieve last te verminderen.	**4**
	Centraal Informatiepunt Onderzoek Telecommunicatie	
7.8	**Gebruik kenmerken en rechtmatigheidgrondslagen**	
	In de webtoepassing de keuze voor onmogelijke combinaties van kenmerken en rechtsgrondslagen blokkeren.	**4**
7.10	**Testbevragingen**	
	In het CIOT systeem een aparte "pseudo" rechtsgrondslag aanmaken voor testbevragingen (indien wordt besloten dat dit moet worden toegestaan).	**4**
7.14	**Administratieve lasten voor de BOID's**	
	Administratieve ondersteuning van het proces door CIS de benodigde documenten in de vorm van een Proces Verbaal laten genereren.	**4**
8.1	**Controle op integriteit aangeleverde bestanden**	
	Controle van de integriteit van de ontvangen bestanden met behulp van een (MD5) hashtotal.	**3**
	Invoeren van verplichte encryptie van de bestanden bij de verzending via FTP	**3**
8.2	**Importvalidaties**	
	Controleren op het formaat zoals beschreven in de overeengekomen XSD-schema's bij het inlezen van de bestanden.	**2**
8.3	**Calamiteiten - /uitwijkplan**	
	Uitvoeren van een risicoanalyse om te komen tot een actueel en toereikend calamiteiten - en uitwijkplan.	**1**
9.1	**Logging en monitoring aanlevering**	
	De logging ten aanzien van de aanlevering en het importeren van de bestanden beter inzichtelijk maken naar de aanbieders.	**1**

§	Overzicht aanbevelingen uit de audits 2008	Status eind 2009
9.2	**Aanvragen gebruikersnamen en -certificaten**	
	Technisch afdwingen dat bij het aanvragen van een certificaat alleen een hoog beveiligingsniveau kan worden geselecteerd.	3
9.3	**Logging certificate servers**	
	Op de certificate servers de logging activeren zodat inzicht ontstaat in de door beheerders gemaakte wijzigingen en aanpassingen aan de PKI-structuur.	3
	Deze logging periodiek, bijvoorbeeld wekelijks, beoordelen op bijzonderheden, zodat tijdig gehandeld kan worden.	1
9.4	**Intrekken gebruikersaccounts**	
	Bij het intrekken van een gebruikersaccount de Lokale Beheerder schriftelijk inlichten indien de aanvraag in de systemen is verwerkt.	3
9.5	**Handtekeningenlijsten lokaal beheerders**	
	Periodiek de handtekeningenlijst evalueren en actualiseren.	2
9.6	**Service Level management**	
	De SLA's met de BOID's actualiseren en de afspraken over de aanmaak van nieuwe gebruikers in de webtoepassing en bevraging formeel vast te leggen.	1
	Aanbevelingen voor volgende audits	
10.1	**Bewijsmateriaal voor de auditor van de opsporingsdiensten**	
	Voor de toekomstige audits randvoorwaarden creëren waaronder bewijsmateriaal voor de rechtmatigheid kan worden verzameld, rekening houdend met wet- en regelgeving op het gebied van informatiebeveiliging.	1
10.2	**Onderzoek bestanden aanbieders van telecommunicatiediensten**	
	Met de aanbieders van telecommunicatiediensten afspraken maken over het geautomatiseerd visiteren van de bestanden met behulp van een data-analyse tool.	1

8.1 Legenda

1	=	aanbeveling is niet of onvoldoende opgevolgd of afgerond; indien gearceerd dan wordt de aanbeveling ook in verschillende mate door de betrokken actoren onderschreven c.q. het nut en/of noodzaak wordt verschillend ingezien.
2	=	de aanbeveling is deels dan wel slechts door één of enkele maar niet alle betrokken actoren opgevolgd.
3	=	de aanbeveling is door de betrokken actoren onverkort opgevolgd. Indien gearceerd is, dan heeft de aanbeveling op een andere wijze voldoende invulling gekregen waardoor het over 2008 gesignaleerde risico is geheel of in voldoende mate is weggenomen.
4	=	De aanbeveling is bij geen van de audits aan de orde geweest. Bij het onderzoek zijn de definitieve individuele gespreksverslagen 2008 het uitgangspunt geweest en de betreffende aanbeveling kwam in geen van die verslagen aan de orde.