Agenda **Managementteam FIOD 2012.16**
Aanvang 08 mei 2012, om 13.00-17.00 uur
Besluitvormend/Thematisch
Locatie:Utrecht, MT kamer.

		Document
13.00 uur	**Publiciteit**	
12.16.01 13.15 uur	**Verslag vorige vergadering d.d. 1 mei 2012**	**MT12-15cv**
12.16.02 13.20 uur	**Mededelingen**	
12.16.03 13.45 uur	**Structurele inbedding beheer Summ-IT**	**MT12-058**
12.16.04 14.00 uur	**Leidraad gevoelige zaken**	**MT12-059**
12.16.05 14.15 uur	**Overleg ivm voorstel pilot trendwatching**	**MT12-060**
12.16.06 14.30 uur	**Postbus / Besturingsdagen**	
16.00 uur	**Rondvraag / Sluiting** -Doornemen onderlinge MT agenda -Doornemen weekberichten	

Verslag	Managementteam FIOD d.d. 1 mei 2012 Besluitvormend/Thematisch Locatie Utrecht.
Aan	Leden MT FIOD
Van	
Kenmerk	**MT12-14cv**
Kopieën aan	Teamleiders FIOD Ondernemingsraad

MT leden:

Afwezig

MT secretaris:

Publiciteit
Diverse zaken welke in de publiciteit zijn geweest worden doorgesproken. Ook bespreekt het MT een aantal toekomstige acties welke de nodige publiciteit op zouden kunnen leveren.

12.14.01 **Verslag MT vergadering d.d. 24-04-2012** **MT12-13cv**

Het verslag wordt goedgekeurd met de opmerkingen de tekst m.b.t. agendapunt 12.12.02. Deze wordt gewijzigd in: 'er wordt nu vooralsnog gekozen voor een projectmatige aanpak'. En CBA is gewijzigd in CPA.

Afgedane actiepunten:
- Voorstel aandachtspunten PMO. Dit actiepunt volgt vandaag op de agenda.

12.14.02 **Mededelingen**
- geeft aan i.h.k.v. digitalisering, gesproken te hebben met (NMA/SZW directie opsporing). Interessant om de daar aanwezige kennis en expertise te raadplegen i.h.k.v. onze ontwikkeling digitalisering. ( )
- Voorstel om een keer te praten over de overlegvormen van het Platform BOD-en, met name over informatie uitwisselen en samenhang. In een aankomend MT een agendapunt volgen: Platform BOD-en besturingsvraagstukken. Actie .
- meldt dat er i.h.k.v. ontwerp Summ-it we 1 koers gaan varen als BOD-en, comply or explaine en dat het onderwerp is belegd bij het Informatie Platform.
- geeft aan, i.v.m. artikel 60, voorstander te zijn van de samenwerking tussen de Douane en de AIVD. verzoekt om met contact op te nemen inzake de huisvesting.

12.14.03 **Reactie beantwoording vragen MT inzake GO IDR 2.0** **MT12-056**

Stuk is duidelijk en akkoord.

12.14.04 **Inrichting organisatie Besturingsdag**

Ideen uitgewisseld en ze worden in gebracht in de vb groep besturingsdag en onderwerp komt ook terug op de agenda MT volgende week.

12.14.05 **PMO brainstorm plan van aanpak** **MT12-57**

Het onderwerp pesten verdient bespreking in de werkoverleggen. De uitkomst van het PMO maakt dat duidelijk. Het percentage van 15 ligt boven de benchmark en is daarmee hoger dan gemiddeld in organisaties en bedrijven. Qua aanpak geen heksenjacht wel bewustzijn vergroten. Zoals [ ] zegt is het grapje wel een grapje.

Bij het onderwerp BMI is het gevoeld dat we er met het stuk nog niet zijn. We ondernemen actie omdat we de gezondheid van medewerkers serieus nemen. We zoek nog naar manieren om dit onderwerp goed te geagendeerd te krijgen.

[ ] neemt bovengenoemde op met [ ]. [ ] wordt door [ ] ook uitgenodigd eens bij hem aan te komen om van gedachten te wisselen.

Rondvraag/Sluiting:

[ ] zal op 25 mei om 13.00 de afspraak: aanpak Fraude-ontwikkeling ovenemen van [ ]. Hij is afwezig i.v.m. de Roparun.

Sluiting:

[ ] sluit onder dankzegging de vergadering

ACTIEPUNTENLIJST

Datum overleg	Onderwerp	Verantwoordelijk	Datum gereed
06-06-2011	Opmaak van een draaiboek/checklist voor A-onderzoeken, de noodzaak van inzet twee projectleiders, het verder uitwerken van de rollen van M1, de projectleider(s) en de teamleiders.		7 mei
18-07-2011	M.b.t. tot de AMOK training de uitwerking van de procedure inzake de operationele inzet ( ). Na accordering, procedure afstemmen met Raad van Hoofdcommissarissen.		Juni
06-12-2011	Memo werving verder uitwerken naar compleet personeelsoverzicht. Komt een getalsmatig overzicht.		Half mei
07-02-2012	Nadere uitwerking concept notitie samenwerking met OU (incl. casusbeschrijving)		Juni
13-03-2012	M.b.t. het onderwerp trendwatching een plan van aanpak uitwerken voor een nadere verkenning van dit onderwerp.		Half mei
25-04-2012	CT-coaches gaan in gesprek met CT's over functie EDP-auditor.	MT	Half mei

MANAGEMENT TEAM

AANBIEDINGSFORMULIER

MT-nummer :MT12-058

Titel	:	Structurele inbedding beheer Summ-IT
Vergaderdatum	:	08/05/12
Afkomstig van	:	/
Verantwoordelijk MT lid	:	
Aanleiding	:	Te beleggen en te plannen actviteiten in het kader van Inrichten Beheer Summ-IT vanuit Programma GO/BOD, afbakening 'verantwoordelijkheden' en houtskoolschets
Vorige behandeling	:	n.v.t.
Relevante stukken	:	Memo Structurele inbedding beheer Summ-IT (versie 1.0, d.d. 24 april 2012) Memo 'Te beleggen en te plannen activiteiten in het dader van Inrichten Beheer Summ-IT (d.d. 30 januari 2012)
Aard bespreking	:	Besluitvormend
Gepland tijdsbeslag	:	15 min
Bevoegdheid Ondernemingsraad:		n.v.t.
Korte inhoud	:	Het memo beschrijft het voorstel tot het inrichten van het beheer van Summ-IT binnen de organisatie. Hierbij wordt onderscheid gemaakt naar de incidentele inrichting (onder verantwoordelijkheid van het project) en de structurele inrichting (onder verantwoordelijkheid van een van de stafteams). Bij de inrichting van het beheer wordt eveneens onderscheid gemaakt naar het 'niveau', te weten: strategisch / tactisch en operationeel. Bij de structurele inrichting verdient het item 'behoeftemanagement' specifieke aandacht mede in relatie tot de ontwikkeling van de 'postbus 2.0' en de 'houtskoolschets'.

Betrokken Stafonderdelen:	Voor Gezien
Bedrijfsvoering	coproductie
Beleid	n.v.t.
Communicatie	nog n.v.t, wel vanuit project
Huisvesting	n.v.t.
Informatiemanagement	coproductie
Personeel en Organisatie	n.v.t.
Vaktechniek en Opsporing	n.v.t.
Vorming en Opleiding	n.v.t.

Bespreek- / beslispunten	:	Het MT wordt, op advies van de Stuurgroep implementatie Summ-IT, gevraagd in te stemmen met de volgende beslispunten: 1. het inrichten van het beheer van Summ-IT conform de processen die in dit memo zijn beschreven; 2. het initieel uitwerken van de verschillende (deel)processen onder verantwoordelijkheid van het project, waarbij m.n. de stafteams IM, bedrijfsvoering en I&A intensief worden betrokken; 3. het overdragen aan en structurele uitwerking / uitvoering van deze (deel)processen onder verantwoordelijkheid van de betreffende stafteams, waarbij nauw wordt samengewerkt met het project zodat een soepele overdracht wordt gerealiseerd; 4. het verder ontwikkelen van het proces 'behoeftemanagement' binnen de uitwerking van de 'houtskoolschets', onder regie van [redacted], waarbij de stafteams input leveren.
Vervolgtraject na accordering	:	
Opnemen in Handboek FIOD:		

MT12-058a

Memo

Te beleggen en te plannen activiteiten in het kader van Inrichten Beheer Summ-IT

Aan	Kerngroep Inrichten beheer Summ-IT, Businessoverleg Summ-IT
Van	
Datum	30 januari 2012
Kenmerk	Memo activiteiten inrichten beheer Summ-IT v02.doc
Kopieën aan	

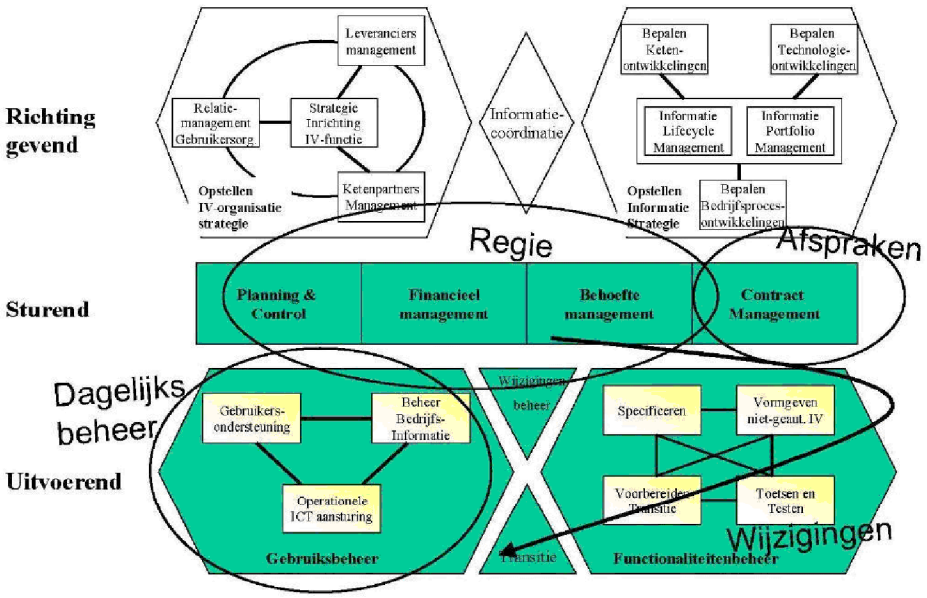
Aanleiding en doel

In de beheerarchitectuur van Summ-IT is beschreven wat er aangaande overkoepelend beheer moet worden ingericht om Summ-IT met succes te kunnen implementeren en beheren. De beheerarchitectuur versie 1.1 is goedgekeurd door de stuurgroep GO/BOD.
In deze memo wordt op basis van de beheerarchitectuur de in het kader van het in te richten beheer de uit te voeren activiteiten benoemd en wordt een voorstel gedaan aangaande de planning. Het is voor een deel overkoepelend over - en voor een deel binnen de klant- en leverancierorganisatie.
Het doel is op basis hiervan te komen tot het toewijzen van de inrichtingsactiviteiten aan verantwoordelijken, het komen tot een planning van de activiteiten en het beleggen van het bewaken van die planning. De memo wordt aangeboden aan het businessoverleg Summ-IT en aan de kerngroep Inrichten Beheer Summ-IT.

Opbouw memo

De beheerarchitectuur (BA) is opgehangen aan het functioneel beheer. In onderstaande figuur zijn de hoofdgroepen genoemd die binnen het functioneel beheer van Summ-IT worden onderkend. Deze hoofdgroepen vormen de structuur van deze memo:

- Regie
- Afspraken leverancier en klant
- Wijzigingen
- Dagelijks beheer



Regie (Sturende processen, BA hoofdsstuk 5.2– 5.6)
Bij de sturing op de informatievoorziening binnen een organisatie zijn vier onderwerpen waarop deze sturing plaatsvindt:

- De planning van de tijd en capaciteit (wie en wanneer)
- De kosten (hoeveel)
- De kwaliteit van de inhoud en de functionaliteit (wat)
- De afspraken over de dienstverlening (hoe en waarmee)

Deze onderwerpen hebben nauwe relaties met elkaar. Het is daarom belangrijk integraal te sturen over alle stuuraspecten heen. Daarnaast is ook integrale sturing nodig op alle activiteiten binnen de informatievoorzienig. Dat beperkt zich niet tot alleen de dienst Summ-IT Opsporing, maar strekt zich uit tot de gehele IV-voorziening.

Voor de klantorganisaties geldt dat vanuit de sturende processen kaders worden meegegeven voor de operationele processen. De sturende processen moeten dus eigenlijk het eerst worden ingericht. Als de organisatie van deze tactische processen nog niet helder zijn, dan kunnen noodzakelijke besluiten allicht door de stuurgroepen en/of het (lijn)management worden genomen.

	Omschrijving	**Status**	**Voorgestelde planning voor in de lijn beleggen**
	Sturende processen		
1.	Planning & Control	Dit wordt nu ingevuld vanuit programma GO/BOD en project Implementatie Summ-IT voor alleen Summ-IT. Het jaar 2012 is daardoor wel afgedicht.	4e kwartaal 2012
2.	Behoeftemanagement (kwaliteit)	Dit wordt nu ingevuld vanuit programma GO/BOD en project Implementatie Summ-IT voor alleen Summ-IT. In 2012 daardoor wel afgedicht.	4e kwartaal 2012
2a	Beschrijving standaard dienst vtsPN	Dit is ingevuld vanuit programma GO/BOD. Opgenomen in offerte en onderdeel contract.	-
3	Financieel management	Dit wordt nu ingevuld vanuit programma GO/BOD (offertetraject)	Urgentie hoog. Initieel: 1e kwartaal 2012 Structureel: 2e kwartaal 2012
3a	Financiën • Afsluiten offerte, incl. afrekenmechanisme • Controleren en goedkeuren facturen (incl. urenstaten) • Raming 2013 en verder	Dit wordt nu vanuit het offerteproces van het programma GOBOD bepaald. Sturing moet van programma naar de lijn.	Urgentie hoog. Initieel: 1e kwartaal 2012 Structureel: 2e kwartaal 2012

Afspraken leverancier en klant (Contractmanagement, BA hoofdstuk 5.6)
Er worden afspraken gemaakt over de samenwerking tussen de leverancier en de afnemers. Deze afspraken worden opgenomen in een "contract". Daar in het OGO is afgesproken dat er wordt samengewerkt op basis van vertrouwen en het een samenwerking is tussen overheidsinstanties, kan de omvang van het contract worden beperkt. Het contract heeft deze onderdelen:

- Beschrijving van de standaard dienst Summ-IT Opsporing van de vtsPN;
- Financiën (Dossier Financiële afspraken (DFA));
- Service Level Agrement (SLA);
- De wijze van besturing (Governance) op de operationele, tactische en strategische niveaus.

In de offertefase komt over de inhoud van het contract al veel duidelijkheid. De offerte vormt de stevige basis voor het contract. De besturing wordt ingericht op de operationele, tactische en strategische niveaus. Met de bijbehorende periodieke overleggen.
Hiernaast moet ook het beheer van de onderhavige beheerarchitectuur worden belegd.

	Omschrijving	Status	Voorgestelde planning voor in de lijn beleggen
	Sturende processen (vervolg)		
4	Contractmanagement	Dit wordt nu ingevuld vanuit programma GO/BOD (offertetraject). Moet van programma naar de lijn.	Urgentie: hoog
4a	Sturing (Governance) • Operationeel • Tactisch • Strategisch	Hoog. Nu nog grotendeels vanuit programma. Dit is een onderdeel van de contractafspraken. Moet van programma naar de lijn.	Initieel: 1e kwartaal 2012 Structureel: 2e kwartaal 2012
4b	SLA afsluiten met vtsPN	Betreft aangaande het hosting gedeelte de standaard SLA van vtsPN (het ter beschikking stellen van Summ-IT). Hier valt het Wijzigingenbeheer niet onder.	Initieel: 1e kwartaal 2012 Structureel: 2e kwartaal 2012
4c	SLA aanpassen met B/CIE	Afwijkingen tov de standaard SLA met huidige leverancier vastleggen	Initieel: 1e kwartaal 2012 Structureel: 2e kwartaal 2012
4d	DAP maken en afsluiten met vtsPN	Met name operationele afspraken vastleggen	Initieel: 1e kwartaal 2012 Structureel: 2e kwartaal 2012
4d	DAP aanpassen met de B/CIE	Met name (gewijzigde) operationele afspraken vastleggen	Initieel: 1e kwartaal 2012 Structureel: 2e kwartaal 2012
4e	Beleggen Beheer BA	Beleggen conform Governance. Advisering	Structureel: 2e kwartaal 2012

Wijzigingen, Functionaliteiten beheer en Transitie (BA, hoofdstuk 5.7 – 5.9)
De applicatie Summ-IT is een onderdeel van de dienst Summ-IT Opsporing. De applicatie wordt afgenomen op basis van licenties, en de functionaliteit is voor de klantorganisaties een gegeven. Het kan vergeleken worden met een pakket. Er kan wel enige invloed worden uitgeoefende via een gebruikersoverleg. En door het samenwerken op bedrijfsproces- en informatiemanagement niveau tussen de gebruikende organisaties van Summ-IT, zodat de bedrijfsprocessen én de informatiebehoefte afgestemd zijn en ook in de toekomt ondersteund kunnen worden door één ICT-systeem. Rond het Wijzigingen zijn de volgende zaken in te richten:

- Inrichten strategisch Informatiemanagement overleg rond bedrijfsproces Opsporing;
- Inrichten Opsporingsbreed Gebruikersoverleg Summ-IT;
- Positioneren afspraken rond werkgroep gegevensset GSO / standaard formulieren / landelijke en specifiek tabellen / kerngroep Beveiliging;
- Inrichten afstemming rond (impact van) specificaties wijzigingen Summ-IT;
- (Voorbereiding) Transitie. Daar we nu projectmatig de belangrijkste initiële implementatie gaan uitvoeren, kan de kennis direct worden "vertaald" naar het in te richten proces.

	Omschrijving	Status	Voorgestelde planning voor in de lijn beleggen
	Activiteit Wijzigingenbeheer		
5	Proces rond wijzigingen inrichten	Moet van programma naar de lijn.	Urgentie hoog. Initieel: 1e kwartaal 2012 Structureel: 2e kwartaal 2012
5a	Overkoepelende zaken • Inrichten expertisegroep (wordt gebruikersoverleg Summ-IT)	Hoog. Nu is er al een lijst met > 100 wijzigingsverzoeken, met name vanuit Politie. Dit is een bestaand overleg, met name gekoppeld aan POC Haaglanden. Moet van programma naar de lijn. Actie : vtsPN/ LFB	Urgentie hoog. Structureel: 2e kwartaal 2012

	Omschrijving	Status	Voorgestelde planning voor in de lijn beleggen
		Deelname vanuit de lijn: FIOD / NVWA	
5b	Overkoepelende zaken • Inrichten overkoepelend functioneel beheergroep	Hoog. Nu is er al een lijst met > 100 wijzigingsverzoeken, met name vanuit Politie. Dit is een bestaand overleg met de huidige functioneel beheerders. Hieraan gekoppeld zijn werkgroepen als die van der formulieren en de GSO. Actie : vtsPN/ LFB Deelname vanuit de lijn: FIOD / NVWA	Urgentie hoog. Initieel: 1e kwartaal 2012 Structureel: 2e kwartaal 2012
5c	Overkoepelende zaken • Inrichten Change Advisory Board (CAB)	Nu is er al een lijst met > 100 wijzigingsverzoeken, met name vanuit Politie. Dit is een bestaand overleg dat verder moet worden ontwikkeld. Actie : vtsPN/ LFB Deelname vanuit de lijn: FIOD en BCIE NVWA en DICTU	Urgentie hoog. Initieel: 1e kwartaal 2012 Structureel: 2e kwartaal 2012
5d	Overkoepelend: • Inrichten regiegroep: besluitvormend orgaan aangaande de adviezen uit het CAB	Deze regiegroep kan aansluiten bij de Governance structuur die is afgesproken in de contracten (zie actie 4a) De regiegroep gaat dan niet alleen over de inhoudelijke wijzigingen, maar ook over de dienst Summ-IT in bredere zin. Dus ook over de regiegebieden 1 t/m 4.	Urgentie hoog. Initieel: 1e kwartaal 2012 Structureel: 2e kwartaal 2012
5e	Klantorganisatie: Intern gebruikersoverleg (inventariseren wensen gebruikers)	Dit wordt vanuit het proces Gebruikersondersteuning worden georganiseerd	Urgentie midden. Structureel: 2e kwartaal 2012, als Summ-IT wordt geïmplementeerd en dus door gebruikers in gebruik wordt genomen.
5f	Klantorganisatie: Intern overleg aangaande proces Opsporing (eigenaar proces). Impulsen vanuit keten, wetgeving, techniek	Dit wordt in de IV keten doorgaans informatiemanagement genoemd. Dit is met name van belang als er over de opvolger van Summ-IT nagedacht gaat worden. De FIOD en NVWA moeten dan ook aanschuiven.	Urgentie Midden
	Activiteit Transitie		
6	Voor een implementatie van Summ-IT moeten op verschillende niveaus zaken worden gewijzigd: • Businessniveau (oa. gebruikers en proces) • Functioneel beheer (oa systeemtabellen, formulieren) • Applicatiebeheer (programma's, landelijke systeemtabellen en formulieren)	Bij de initiële implementatie wordt dit vanuit projecten geregeld (vtsPN, FIOD, NVWA, BCIE, DICTU). De volgende release wordt vanuit de lijn georganiseerd. Het is nodig de beproefde werkwijze over te kunnen dragen naar de lijn, waarbij de geleerde lessen zijn verwerkt.	Urgentie hoog

	Omschrijving	Status	Voorgestelde planning voor in de lijn beleggen
	• Technisch beheer (infrastructuur, uitvoering installatie)	Het is daarom de aanbeveling de initiële implementatie te laten (mee)uitvoeren door de medewerkers die dit later vanuit de lijn moeten uitvoeren.	

Dagelijks beheer (Gebruiksbeheer, BA hoofdstuk 5.10 – 5.13)
Zowel de klantorganisaties als de leveranciersorganisatie gaan het dagelijks beheer intern inrichten.
Bij de vtsPN wordt dit dienstinrichting genoemd.
Het gaat hier vooral over:

- Het ondersteunen van de gebruikers (o.a. afhandelen vragen en incidenten en verstrekken autorisaties);
- Het beheren van de gegevens (o.a. beheren tabellen en formulieren, controleren, aanpassen);
- Het aansturen van de ICT, dus van de vtsPN en ook van de "eigen" dienst B/CIE of DICTU.

De te maken afspraken over de operationele koppelvlakken rond het operationele beheer tussen klant- en leverancierorganisatie worden opgenomen in een Dossier Afspraken en Procedures (DAP).

	Omschrijving	Status	Voorgestelde planning voor in de lijn beleggen
	Activiteit Gebruiksbeheer		
7	Inrichten dienst Summ-IT Opsporing	Actie vtsPN. Door [redacted] vtsPN	2e kwartaal 2012 (4 mei)
8	Gebruikersondersteuning (BA, hoofdstuk 5.11)	Actie intern FIOD en NVWA	2e kwartaal 2012 (4 mei)
8a	Eerste lijn incident management		2e kwartaal 2012 (4 mei)
8b	Regie over incidenten die niet direct te plaatsen zijn bij één leverancier		2e kwartaal 2012 (4 mei)
8c	Kunnen beantwoorden functionele vragen		2e kwartaal 2012 (4 mei)
8e	Samenwerking (informeel) tussen "helpdesken" klantorganisaties		2e kwartaal 2012 (4 mei)
8f	Afspraken over escalatie (bijv. bij damage)	Opnemen in DAP, ook op basis van Governance	2e kwartaal 2012 (4 mei)
8g	Gebruikersoverleg	Zie Wijzigingen 5E	2e kwartaal 2012 (4 mei)
9	Beheren bedrijfsinformatie (BA, hoofdstuk 5.12)		Initieel: 1e kwartaal 2012 Structureel: 2e kwartaal 2012
9a	Bewaken en controleren	Actie intern FIOD en NVWA Afspraken tussen business en functioneel beheer over verantwoordelijkheden, taken en bevoegdheden.	Initieel: 1e kwartaal 2012 Structureel: 2e kwartaal 2012
9b	Informeren en rapporteren	Actie intern FIOD en NVWA Afspraken tussen business en functioneel beheer over verantwoordelijkheden, taken en bevoegdheden.	Initieel: 1e kwartaal 2012 Structureel: 2e kwartaal 2012
9c	Wijzigen gegevens	Actie intern FIOD en NVWA Afspraken tussen business en	Initieel: 1e kwartaal 2012 Structureel: 2e kwartaal 2012

	Omschrijving	Status	Voorgestelde planning voor in de lijn beleggen
		functioneel beheer over verantwoordelijkheden, taken en bevoegdheden. Denk ook aan beheer systeemtabellen en formulieren.	
9d	Admin-account	Actie vtsPN: Duidelijkheid verkrijgen over autorisaties van [redacted].	1e kwartaal 2012
10	Operationele ICT aansturing	Afspraken maken tussen vtsPN en FIOD / NVWA over opdrachtverstrekking Vastlegging in DAP.	Initieel: 1e kwartaal 2012 Structureel: 2e kwartaal 2012
10a	Bewaking dienstverlening	SLA rapportage. Aansluiten bij Governance.	Initieel: 1e kwartaal 2012 Structureel: 2e kwartaal 2012

MT12-058b

Memo Structurele inbedding beheer Summ-IT

Aan	Managementteam FIOD, d.t.k.v. Stuurgroep implementatie Summ-IT
Van	
Auteurs	
Datum	24 april 2012
Kenmerk	/12016
Kopieën aan	
Versie	1.0
Bijlage	Memo 'Te beleggen en te plannen activiteiten in het kader van Inrichten Beheer Summ-IT' (d.d. 30 januari 2012)

Historie

Versie	Datum	Veranderingen (concept/definitief)	Opdrachtnemer	Auteur(s)
0.1	15-03-2012	initiële opzet document		
0.2	27-03-2012	wijzigingen n.a.v. bespreking SG van 27/03/12: - eenduidige verantwoordelijkheid bij 'wie' - copafijth-bi oppakken SG is akkoord na aanpassing van bovenstaande. Gezien raakvlak met besturingsfilosofie, wenselijk om, met inachtneming reactie betrokken stafteams, in te brengen in MT. Dit is tekstueel in onderhavige versie toegevoegd.		
0.3	17-04-2012	besproken met (staf)teams IM, bedrijfsvoering en I&A, nadere toelichting en tweedeling in 'al bestaand' en 'nieuw' (m.n. behoeftemgt (raakt niet alleen Summ-IT))		
1.0	24-04-2012	accordering in stuurgroep		

Inleiding

In het opdrachtgeveroverleg van het Programma GO/BOD is het memo 'Te beleggen en te plannen activiteiten in het kader van Inrichten Beheer Summ-IT' geaccordeerd. Doel van dit memo is het 'toewijzen van inrichtingsactiviteiten aan verantwoordelijken, het komen tot een planning van de activiteiten en het beleggen van het bewaken van die planning'. Na accordering heeft de GO/BOD het memo toegezonden aan de 'verantwoordelijk ' binnen de FIOD van het project implementatie Summ-IT.
Tijdens de vergadering van de stuurgroep (SG) implementatie Summ-IT, d.d. 14 maart jl., is het memo besproken.
De SG heeft aan de projectleiders gevraagd om met een concreet voorstel te komen waar, naar hun mening, werkzaamheden moeten worden opgepakt en bewaakt om tot een goede en structurele borging van het 'beheer' na afronding van het Programma en project te komen. Onderhavig memo behelst het concrete voorstel hiervan ten behoeve van de FIOD. Evident is dat gedurende de looptijd van het project de activiteiten mede vanuit het project vorm worden gegeven. De SG heeft in de bijeenkomst van 27 maart jl. het eerste concept besproken en, met inachtneming van een aantal kleine tekstuele aanpassingen, geaccordeerd.
Uitgangspunt bij het oppakken van de activiteiten is dat de initiële activiteiten onder verantwoordelijkheid van het project worden uitgevoerd, zoveel mogelijk in samenwerking met de 'staande organisatie' (ic. het stafteam dat ook na afronding van het project 'hiervoor

staat opgesteld'). Voor de structurele activiteiten geldt dat de verantwoordelijkheid ligt bij de 'staande organisatie', waar nodig in samenwerking met het project[1].
Omdat de SG zich ook realiseert dat onderhavig onderwerp een relatie heeft met het besturingsmodel van de FIOD, acht zij het van belang dat het voorstel ook door het MT wordt geaccordeerd.

Voorstel

Het beheer dient op een aantal niveaus te worden ingericht, te weten: strategisch / tactisch en operationeel. Het lijkt voor de hand te liggen om de strategisch en tactische 'items' te beleggen bij / in een van de stafteams, waarbij primair wordt gedacht aan IM daar deze vraagstukken met name zien op de sturing, kwaliteit en borging. Daarnaast betreft het met name activiteiten die nu ook al door dit team worden uitgevoerd.
Het operationeel beheer wordt primair in het team I&A belegd, in verband met de meer dagelijkse gang van zaken betreft ten aanzien van het gebruik en ondersteuning van de gebruikers van Summ-IT.

In onderhavig memo wordt de in het aangehaald memo gehanteerde indeling, omschrijving, etc. aangehouden, om de 'beheer' activiteiten te beleggen, voor zover deze intern door de FIOD moeten worden opgepakt.
In de 'Beheerarchitectuur inrichten beheer Summ-IT' (versie 1.1., d.d. 11 november 2011) is een aantal vragen opgenomen. De beantwoording van deze vragen is behulpzaam bij de nadere duiding van het 'wat' in de onderstaande tabellen.

In onderstaande tabellen is het voorstel opgenomen welke stafafdeling als 'verantwoordelijke' moet worden gezien bij de 'copafijth-bi brede uitvoering'. Dit wil dus niet zeggen dat zij alle werkzaamheden zelf moeten uitvoeren, maar wel dat ze de verantwoordelijkheid hebben dat het wordt gerealiseerd[2]. De met een '(*)' gemerkte activiteiten behoren reeds tot de 'verantwoordelijkheid / taak' van het stafteam IM.

Het item behoeftemanagement verdient een nadere toelichting, enerzijds omdat een aantal activiteiten hiermee samenhangend reeds impliciet wordt uitgevoerd. Maar anderzijds ook om dit juist meer te expliciteren binnen de organisatie en te verankeren in de ontwikkeling met betrekking tot 'postbus 2.0' en de 'houtskoolschets'. Waarmee het een (relatief) nieuw maar zeker 'onontwikkeld' terrein binnen de organisatie is.
Behoeftemanagement heeft als uitgangspunt de behoefte van(uit) de organisatie te ondersteunen door middel van de informatievoorziening. Hierbij gaat het vooral om de kwaliteit van de bedrijfsprocessen en hoe deze verbeterd kunnen worden zodat ze beter aansluiten bij de behoefte van de organisatie. Daarnaast is behoeftemanagement verantwoordelijk voor het onderkennen van de behoeften binnen een bedrijfsproces en de besluitvorming over wat er met de behoefte moet worden gedaan.
Het doel is om de informatievoorziening zo goed mogelijk aan te sluiten op gebruikers, de procesgang binnen een organisatie en de omgeving waarin de organisatie zit. Hiermee vormt behoeftemanagement de 'verbindende schakel' tussen 'informatiemanagement, gebruiksbeheer en wijzigingenbeheer'.
Het verdient dan ook aanbeveling om behoeftemanagement nader te laten uitwerken vanuit het perspectief van de 'houtskoolschets' en de regie hierop bij [ ] te beleggen.
Input hierop dient door alle (staf)teams te worden gegeven.

---

1 In de tabellen is de initiële verantwoordelijkheid aangeduid met (i) en de structurele met (s).
2 Als voorbeeld: IM neemt het contractmanagement (de regie) voor haar rekening. Hierin spelen uiteraard de financiën een rol, waarvoor primair bedrijfsvoering staat opgesteld. IM heeft echter vanuit haar verantwoordelijkheid de 'taak' om dit (procesmatig en inhoudelijk) met bedrijfsvoering kort te sluiten.

Regie (sturende processen, BA hoofdsstuk 5.2– 5.6)

	omschrijving	planning belegging in lijn (kwartaal 2012)	Wat	Wie
	sturende processen			
1	planning & control (*)	4e		IM (s)
2	behoeftemanagement (kwaliteit)	4e		
3	financieel management (*)	urgentie: hoog initieel: 1e structureel: 2e	opnemen in begroting en verantwoording cyclus	project (i) bedrijfsvoering (s)
3a	financiën (*) - controleren en goedkeuren facturen - raming 2013 en verder	urgentie: hoog initieel: 1e structureel: 2e	"	project (i) bedrijfsvoering (s)

Afspraken leverancier en klant (contractmanagement, BA hoofdstuk 5.6)

	omschrijving	planning belegging in lijn (kwartaal 2012)	Wat	Wie
	sturende processen (vervolg)			
4	contractmanagement (*)	Urgentie: hoog	opnemen in proces	IM (s)
4a	sturing (governance) - operationeel - tactisch - strategisch	initieel: 1e structureel: 2e		IM (s)
4b	SLA afsluiten met vtsPN	initieel: 1e structureel: 2e	inregelen proces monitoring / aanpassing / verlenging SLA, in- en externe afstemming met betrokkenen	project (i) IM (s)
4c	SLA aanpassen met B/CIE	initieel: 1e structureel: 2e	"	project (i) IM (s)
4d	DAP maken en afsluiten met vtsPN	initieel: 1e structureel: 2e	inregelen proces monitoring / aanpassing DAP, in- en externe afstemming met betrokkenen	project (i) IM (s)
4e	DAP aanpassen met B/CIE	initieel: 1e structureel: 2e	"	project (i) IM (s)
4f	beleggen beheer 'business architectuur' (m.n. documenten)	structureel: 2e	integrale opname in administratieve organisatie	IM (s)

Wijzigingen, functionaliteit beheer en transitie (BA, hoofdstuk 5.7 – 5.9)

	omschrijving	**planning belegging in lijn (kwartaal 2012)**	**Wat**	**Wie**
	activiteit wijzigingenbeheer			
5	proces rond wijzigingen (*)	urgentie: hoog initieel: 1e structureel: 2e		project (i) IM (s)
5a	overkoepelende zaken - inrichten expertisegroep (wordt gebruikersoverleg Summ-IT)	urgentie: hoog structureel: 2e	actie ligt bij vtsPN, deelname FIOD vooralsnog [redacted]	IM (s)
5b	overkoepelende zaken - inrichten overkoepelende functioneel beheergroep	urgentie: hoog initieel: 1e structureel: 2e	actie ligt bij vtsPN	programma / project (i) I&A (s)
5c	overkoepelende zaken - inrichten Change Advisory Board (CAB)	urgentie: hoog initieel: 1e structureel: 2e	actie ligt bij vtsPN	programma / project (i) IM (s)
5d	overkoepelende zaken - inrichten regiegroep: besluitvormend orgaan aangaande de adviezen uit de CAB	urgentie: hoog initieel: 1e structureel: 2e	actie ligt bij Programma, deelname FIOD op MT niveau (i.c. [redacted])	programma / project (i) MT (s)
5e	klantorganisatie - intern gebruikersoverleg (inventariseren wensen gebruikers)	urgentie: midden structureel: 2e	inrichten functioneel loket bij team I&A, en organiseren gebruikersoverleg vertegenwoordigers verspreid over CT's	I&A (s)
5f	klantorganisatie - intern overleg aangaande proces opsporing (eigenaar proces). Impulsen vanuit keten, wetgeving, techniek etc.	urgentie: midden	inrichten overlegstructuur gebruikers, en aanbrengen expertisegroep (5a), intern raakvlak met 'van impuls tot ... '	IM (relatie behoefte-management) (s)
	activiteit transitie			
6	voor een implementatie van Summ-IT moeten op verschillende niveaus zaken worden gewijzigd: - businessniveau (oa. gebruikers en proces) - functioneel beheer (oa systeemtabellen, formulieren) - applicatiebeheer (programma's, landelijke systeemtabellen en formulieren) - technisch beheer (infrastructuur, uitvoering installatie)	urgentie: hoog		I&A (t.a.v. ICT) (s) IM (m.b.t. business) (s)

Dagelijks beheer (gebruiksbeheer, BA hoofdstuk 5.10 – 5.13)

	omschrijving activiteit gebruiksbeheer	**planning belegging in lijn (kwartaal 2012)**	**Wat**	**Wie**
8	gebruikersondersteuning (BA, hoofdstuk 5.11)	structureel: 2e (opleveringsdatum)		I&A (s)
8a	1e lijn incident management	structureel: 2e (opleveringsdatum)		I&A (s)
8b	regie over incidenten die niet direct te plaatsen zijn bij één leverancier	structureel: 2e (opleveringsdatum)		I&A (s)
8c	kunnen beantwoorden functionele vragen	structureel: 2e (opleveringsdatum)		I&A (s)
8d	samenwerking (informeel) tussen 'helpdesken' klantorganisaties	structureel: 2e (opleveringsdatum)		I&A (s)
8e	afspraken over escalatie (bijv. bij damage)	structureel: 2e (opleveringsdatum)	opnemen in DAP, inregelen proces monitoring / aanpassing DAP, in- en externe afstemming met betrokkenen	I&A (s)
8f	gebruikersoverleg	structureel: 2e (opleveringsdatum)	inrichten functioneel loket bij team I&A, en organiseren gebruikersoverleg vertegenwoordigers verspreid over CT's	I&A (s)
9	beheren bedrijfsinformatie (BA, hoofdstuk 5.12)	initieel: 1e structureel: 2e		
9a	bewaken en controleren	initieel: 1e structureel: 2e	maken van afspraken tussen business en functioneel beheer over verantwoordelijkheden, taken en bevoegdheden	vanuit behoeftemgt vormgeven I&A (s)
9b	informeren en rapporteren	initieel: 1e structureel: 2e	maken van afspraken tussen business en functioneel beheer over verantwoordelijkheden, taken en bevoegdheden	vanuit behoeftemgt vormgegeven I&A (s)
9c	wijzigen gegevens	initieel: 1e structureel: 2e	maken van afspraken tussen business en functioneel beheer over verantwoordelijkheden, taken en bevoegdheden	vanuit behoeftemgt vormgeven I&A (s)
10	operationele ICT aansturing	initieel: 1e structureel: 2e	opnemen in DAP, inregelen proces monitoring / aanpassing DAP, in- en externe afstemming met betrokkenen	project (i) I&A (s)
10a	bewaking dienstverlening	initieel: 1e structureel: 2e	opnemen in SLA, inregelen proces monitoring / aanpassing / verlenging SLA, in- en externe afstemming met betrokkenen	project (i) I&A (s)

Besluit en vervolg

Het MT wordt, op advies van de Stuurgroep implementatie Summ-IT, gevraagd in te stemmen met de volgende beslispunten:

1. het inrichten van het beheer van Summ-IT conform de processen die in dit memo zijn beschreven;
2. het initieel uitwerken van de verschillende (deel)processen onder verantwoordelijkheid van het project, waarbij m.n. de stafteams IM, bedrijfsvoering en I&A intensief worden betrokken;
3. het overdragen aan en structurele uitwerking / uitvoering van deze (deel)processen onder verantwoordelijkheid van de betreffende stafteams, waarbij nauw wordt samengewerkt met het project zodat een soepele overdracht wordt gerealiseerd;
4. het verder ontwikkelen van het proces 'behoeftemanagement' binnen de uitwerking van de 'houtskoolschets', onder regie van [redacted], waarbij de stafteams input leveren.

MANAGEMENT TEAM

AANBIEDINGSFORMULIER

		MT-nummer :MT12-059
Titel	:	***Leidraad gevoelige zaken***
Vergaderdatum	:	8 mei 2012
Afkomstig van	:	
Verantwoordelijk MT lid	:	
Aanleiding	:	Besluit MT 11-16, 06-06-2011 Opmaak van een draaiboek/checklist voor gevoelige onderzoeken, uitwerken van de rollen van M1, TL en PL.
Vorige behandeling	:	06-06-2011
Relevante stukken	:	-
Aard bespreking	:	besluitvormend
Gepland tijdsbeslag	:	Min:
Bevoegdheid Ondernemingsraad:		-
Korte inhoud	:	Voor gevoelige onderzoeken bestaat behoefte aan een leidraad voor het opzetten van dergelijke onderzoeken. De leidraad moet het mogelijk maken de risico's die zich kunnen voordoen bij het uitvoeren van gevoelige onderzoeken in kaart te brengen en te beperken. Aan de orde komen: ▪ de kenmerken van een gevoelige zaak en een embargozaak ▪ de inrichting van het onderzoek, met daarbij aandacht voor onder meer de verschillende rollen en actoren en de digitale omgeving ▪ aandachtspunten bij het inrichten van de fysieke locatie en ▪ de inzet van tolken / vertalers. Als bijlage is onder meer een checklist met contactpersonen opgenomen. De inhoud van de leidraad is afgestemd met alle contactpersonen/afdelingen en BZT.
Advies IM	:	Verwerkt (GEFIS 2.0, i.o.m.)
Personele consequenties	:	-
Financiële consequenties	:	Geen directe, alleen bij externe locaties (i.o.m.)
IT-consequenties	:	Verwerkt (Summ-IT, i.o.m. ,)
Beleid		Verwerkt (WPG, i.o.m.)
Bespreek- / beslispunten	:	Accordering inhoud leidraad
Vervolgtraject na accordering	:	Verspreiding onder Staf, TL, PL en contactpersonen
Opnemen in Handboek FIOD:		Ja

MT12-059

Recherchehandboek	X-XX-XXX

Gevoelige zaken

Relevante beschrijvingen:

- Meldingsplicht voor (publiciteits-)gevoelige opsporingsonderzoeken
  (Fenster/Voor iedereen/Communicatie en publiciteit)
- Tegenspraak bij de FIOD
  (Recherchehandboek 4-11-400)
- Tolk- en vertaaldiensten
  (Recherchehandboek 4-8-400)
- MT-besluit 11-029 / gebruik GRPDATA

Validatie/huidige versie: april 2012 Deze procedure is geldig tot: dec. 2012	Mail voor informatie of tips naar de eigenaar van dit onderwerp: / Staf / V&O

INHOUD

1 Inleiding 4

2 Gevoelige zaken 5
2.1 Wat is een gevoelige zaak? 5
2.2 Wat is een embargo-zaak? 5
2.3 Verschil: afscherming 5
2.4 Gradaties en gremia bij gevoelige onderzoeken 7

3 Inrichting van het onderzoek 8
3.1 Rollen en actoren 8
3.1.1 stuurgroep FP - FIOD 8
3.1.2 Formele opdrachtgever: directeur FIOD / MT 8
3.1.3 Gedelegeerd opdrachtgever: teamleider opsporing 9
3.1.4 De projectleider 9
3.1.5 De rol van de pv-coördinator binnen het onderzoeksteam: plv. projectleider 9
3.1.6 Tegenspraak 9
3.2 Teamopbouw en kick-off 10
3.2.1 Teamopbouw naar rollen 10
3.2.2 Kick-off 10

4 In opsporing nemen van een dossier, bestaande vastleggingen 11
4.1 De herkomst van het dossier 11
4.2 GEFIS 11
4.3 MRO en RBS 11

5 De huidige digitale omgeving 13
5.1 PVS, GEFIS en SHERLOCK: geen afscherming 13
5.2 Autorisatieniveaus PVS, GEFIS en SHERLOCK 13
5.3 GRPDATA 14
5.4 RBS 14
5.4.1 RBS en VROS 14
5.4.2 Autorisatieniveaus 15
5.4.2.1 Standaardautorisatie 15
5.4.2.2 Autorisatieniveaus gevoelige onderzoeken 15
5.4.3 Blueview en RBS 16

6 De digitale omgeving medio 2012 17
6.1 Summ-IT 17
6.1.1 MRO-functionaliteit 17
6.1.2 Autorisatieniveaus 17
6.1.2.1 Standaardautorisatie 17
6.1.2.2 Autorisatieniveaus gevoelige onderzoeken 17
6.1.3 Summ-IT en Blueview 18
6.1.4 Summ-IT en 'Zoeken en Speuren' 19
6.2 GEFIS 2.0 19

7 De fysieke locatie 20
7.1 Externe locatie 20
7.2 Interne locatie 20
7.2.1 Afgescheiden onderzoekslocatie 20
7.2.2 'Sweepen' van de onderzoeksruimten 20
7.2.3 Overige aandachtspunten 21
7.3 Locatie OVC en Tap 21

8 Inzet van tolken en vertalers 22
8.1 TVCN en Concorde 22
8.2 Het Nationaal Tolken Coördinatiepunt 22

1869931 00899

Bijalgen

Bijlage 1 : Checklist gevoelige onderzoeken
Bijlage 2 : Autorisatiematrix
Bijlage 3 : Relevante wetgeving

1 Inleiding

Naast de reguliere onderzoeken worden binnen de FIOD onderzoeken ingesteld die publicitair gevoelig zijn of op andere wijze een verhoogd afbreukrisico hebben.
Voor deze onderzoeken is de behoefte ontstaan aan een soort leidraad voor het opzetten dergelijke onderzoeken.

De leidraad moet het mogelijk maken de mogelijke risico's die zich kunnen voordoen bij het uitvoeren van gevoelige onderzoeken in kaart te brengen en te beperken.
De gebruiker moet voor ogen houden dat het gaat om risico*beheersing* en niet om volledige risico*afdekking* bij het uitvoeren van gevoelige onderzoeken.

Een ander aspect is dat van bewustwording.
Meer nog dan bij reguliere onderzoeken is het nodig dat alle betrokkenen in en rond het onderzoek zich bewust zijn van hun (beperkte) rol bij het onderzoek en dat niet alle informatie voor iedereen (rolbinding) beschikbaar zal zijn.

Achtereenvolgens komen aan de orde:
- de kenmerken van een gevoelige zaak en een embargozaak
- de inrichting van het onderzoek, met daarbij aandacht voor onder meer de verschillende rollen en actoren en de digitale omgeving
- aandachtspunten bij het inrichten van de fysieke locatie en
- de inzet van tolken / vertalers

Als bijlagen zijn opgenomen:
- de checklist gevoelige onderzoeken
- een autorisatiematrix en
- een overzicht van de relevante wettelijke bepalingen

Tot slot:

Verwacht wordt dat Summ-IT in de tweede helft van 2012 gefaseerd uitgerold zal worden.
Dit heeft tot gevolg dat RBS zal verdwijnen en PVS zal worden uitgefaseerd.
Er komt mogelijk medio 2012 een opvolger van het huidige GEFIS.
In het nieuwe GEFIS (versie 2.0) zal waarschijnlijk alleen de voorfase en de afloop van de zaak worden geregistreerd.

Gelet op deze ontwikkelingen is er voor gekozen om de huidige en toekomstige situatie te beschrijven. Eind 2012 volgt aanpassing aan de actuele stand van zaken.

De beschrijving 'Gevoelige onderzoeken' is niet volledig.
Praktische tips, aanvullingen, en op- en aanmerkingen zijn van harte welkom en zullen bij de eerste aanpassing zoveel mogelijk worden verwerkt.

2 Gevoelige zaken

2.1 Wat is een gevoelige zaak?

In de Handleiding Gevoelige zaken van het College van procureurs-generaal[1] wordt een aantal kenmerken gegeven van het begrip gevoelige zaak. Deze kenmerken zijn:

- de ernst of de aard van het delict brengt landelijk of lokaal grote commotie teweeg of kan dat te weeg brengen, bijvoorbeeld beursfraude of (aan) terrorisme (gelieerde zaken);
- de verdachte, het slachtoffer / de aangever of een andere betrokkene geniet landelijk of lokaal grote bekendheid vanwege zijn of haar positie, functie of beroepsuitoefening, bijvoorbeeld strafbare feiten gepleegd door een minister of burgemeester waarbij de integriteit in opspraak is of strafzaken waarbij dwangmiddelen worden toegepast tegen advocaten;
- de zaak ligt (inter)nationaal politiek, juridisch of publicitaire gevoelig of dreigt dat te worden, daaronder begrepen zaken die gegeven het principiële karakter landelijke afstemming behoeven; bijvoorbeeld door gehanteerde opsporingsmethoden of internationale problematiek (alcoholcontrole piloten).

Daarnaast kan een onderzoek als een gevoelige zaak worden beschouwd indien mag worden verwacht dat:

- vanuit het criminele milieu activiteiten (kunnen) worden ondernomen om de onderzoeksresultaten te beïnvloeden, bijvoorbeeld door het afluisteren van (leden van het) onderzoeksteam, het uitvoeren van contra-observaties en het bedreigen van rechercheurs of de officier van justitie.

2.2 Wat is een embargo-zaak?

Een embargo-zaak is een gevoelige zaak die door het College van procureurs-generaal als embargo-zaak is aangemerkt.
Het belangrijkste criterium om een gevoelige zaak op te schalen tot een embargo-onderzoek is het afbreukrisico bij publiciteit.

2.3 Verschil: afscherming

Het belangrijkste operationele verschil tussen een gevoelige zaak en een embargo-zaak zit in het al dan niet verplicht delen van onderzoeksinformatie. Voor embargo-onderzoeken kan het delen van onderzoeksinformatie worden beperkt of hoeft dat helemaal niet. Op grond van artikel 15, tweede lid WPG en artikel 2:13 eerste lid onder f van het Besluit politiegegevens kan de verantwoordelijke het ter beschikking stellen van politiegegevens bij embargo-onderzoeken weigeren of aan beperkende voorwaarden onderwerpen. In dat geval wordt de free-flow of information beperkt of zelfs geheel gestopt.

Let op:
Alleen het College van procureurs-generaal kan een onderzoek aanmerken als een embargo-onderzoek. Daarmee wordt voorkomen dat onderzoeken te lichtvaardig als embargo-onderzoek worden bestempeld en het uitgangspunt van de WPG – ter beschikkingstelling van politiegegevens – wordt ondergraven.
Gevoelige onderzoeken vallen onder de normale free-flow of information van de WPG. Dat houdt in dat (delen van) de onderzoeksinformatie *direct en verplicht* moet worden gedeeld met andere opsporingsinstanties. De verplichting tot het delen van informatie kan op gespannen voet staan met de mate van gevoeligheid van het onderzoek.

Naar de huidige inzichten wordt aan de minimaal verplichte free-flow of information voldaan indien via de Verwijsindex Recherche Onderzoeken en Subjecten (VROS) de entiteitgegevens

[1] Handleiding gevoelige zaken nummer 2007H003, ***niet gepubliceerd***

politioneel worden gedeeld.

2.4 Gradaties en gremia bij gevoelige onderzoeken

Niet elke zaak kent eenzelfde mate van gevoeligheid. Naarmate een zaak als meer gevoelig wordt aangemerkt, wordt de beslissingen op een hoger niveau getild. Dit geldt niet alleen voor de operationele besluitvorming, maar ook voor beslissingen rond bijvoorbeeld publiciteit.

De (zaaks) officier van justitie moet een gevoelige zaak direct melden aan de hoofdofficier van justitie. Deze beoordeelt of de zaak moet worden gemeld aan het College van procureurs-generaal (hierna: het College). Wordt de zaak gemeld bij het College dan beoordeelt het College of en in hoeverre de betrokken minister moet worden geïnformeerd.

Dit houdt in dat er minimaal door de hoofdofficier van justitie permanent wordt 'meegekeken' in het onderzoek. Hij zal de opzet en voortgang van het onderzoek bewaken en moet worden geïnformeerd over alle relevante stappen die in het onderzoek zullen worden gezet. Hierbij gaat het niet alleen om de opsporing, maar ook om allerlei bestuursrechtelijke beslissingen die het onderzoek (kunnen) raken, bijvoorbeeld inzet van het tucht- en bestuursrecht.
Naarmate het onderzoek als meer vertrouwelijk wordt gekwalificeerd, zal vanuit het OM opschaling in toezicht op het onderzoek plaatsvinden.

Binnen de FIOD zal het MT periodiek of voortdurend moeten worden geïnformeerd over de stand van zaken in het onderzoek en van te voren moeten worden gekend in cruciale besluitvorming binnen het onderzoek en significante afwijkingen van het plan van aanpak van het onderzoek.

De FIOD en het OM zullen het toezicht op de uitvoering van gevoelige onderzoeken onderbrengen in de stuurgroep FP- FIOD. Deze stuurgroep is ook het gremium dat bepaalt of een zaak als gevoelig moet worden aangemerkt.

Bij de opzet en uitvoering van een gevoelig onderzoek moeten er binnen de FIOD sluitende afspraken gemaakt worden over de wijze waarop de interne en externe informatie-uitwisseling plaatsvindt.
Er moeten verder afspraken worden gemaakt over de mate van informatie-uitwisseling en wie de informatie uitwisselt.

3 Inrichting van het onderzoek

Als een dossier aan één of meer van de hiervoor omschreven kenmerken voldoet en daarmee door de stuurgroep FIOD – FP als gevoelige zaak wordt gekwalificeerd, moet daarmee bij de totale inrichting van het onderzoek rekening worden gehouden.
In de volgende onderdelen worden diverse aandachtspunten beschreven die bij de start en inrichting van het onderzoek van belang kunnen zijn.

3.1 Rollen en actoren

In termen van projectmanagement zijn rond het onderzoek de volgende rollen en actoren met bijbehorende verantwoordelijkheden van direct belang:

- De stuurgroep FP - FIOD
- De opdrachtgever (directeur FIOD / MT)
- De gedelegeerd opdrachtgever (teamleider opsporing)
- De projectleider
- De pv-coördinator
- tegenspraak

3.1.1 stuurgroep FP - FIOD

Zoals gezegd ligt de feitelijke regie van omvangrijke, complexe onderzoeken of onderzoeken met een hoge mate van vertrouwelijkheid bij de stuurgroep FP – FIOD.

De stuurgroep formuleert de doelstelling van het onderzoek en vertaalt deze in één of meer concrete onderzoeksopdrachten. De stuurgroep beslist dus over de strategische bandbreedte van het onderzoek.
Het is voor het welslagen van het onderzoek noodzakelijk dat alle betrokkenen (stuurgroep, teamleider opsporing en projectleider) een eenduidig beeld hebben van de strekking en reikwijdte van de onderzoeksopdracht(en). Dit kan alleen worden bereikt wanneer zij allen bij de formulering van de doelstelling van het onderzoek en de verdere uitwerking daarvan worden betrokken.

De stuurgroep beoordeelt verder periodiek de onderzoeksresultaten op basis van de doelstellingen van het onderzoek. Ook weegt de stuurgroep de mogelijke onderzoeksrisico's en fiatteert zij door haar geaccepteerde risico's bij de verdere uitvoering van het onderzoek.
Tenslotte levert de stuurgroep een belangrijke bijdrage aan de belangenafweging tussen FIOD en FP, bijvoorbeeld bij de inzet van capaciteit, afgezet tegen de beoogde doelstellingen van het onderzoek.

De projectleider heeft bij de beoordeling en besluitvorming van de stuurgroep een voorbereidende en uitvoerende taak. Zo maakt hij voortgangsrapportages, op basis waarvan de stuurgroep haar beeld vormt.

3.1.2 Formele opdrachtgever: directeur FIOD / MT

De directeur FIOD / MT is binnen de FIOD de *formele* opdrachtgever van het onderzoek. Dit opdrachtgeverschap is gemandateerd aan de stuurgroep FP – FIOD.

De directeur FIOD / MT heeft bij gevoelige onderzoeken ook een *inhoudelijke* rol.
Hij is op strategisch niveau vanuit de FIOD verantwoordelijk voor het (organisatieoverstijgend) faciliteren van het onderzoek en het wegnemen of kanaliseren van de externe (politieke) druk die het onderzoek kan beïnvloeden.

3.1.3 Gedelegeerd opdrachtgever: teamleider opsporing

De teamleider opsporing is *gedelegeerd* opdrachtgever. Hij bepaalt namens de FIOD vanuit deze rol in samenspraak met de projectleider binnen de onderzoeksopdracht en doelstelling(en) van het onderzoek de inrichting van het onderzoek. Hij accordeert beleidsbeslissingen binnen het onderzoek en faciliteert het onderzoek daar waar het de menskracht en middelen betreft.
Verder is de teamleider opsporing verantwoordelijk voor de externe, onderzoeksoverstijgende communicatie en rapportages, bijvoorbeeld het overleg met de stuurgroep FP – FIOD.

3.1.4 De projectleider

De projectleider is verantwoordelijk voor het realiseren van de doelstellingen van het onderzoek. Hij definieert de activiteiten die voor de realisatie noodzakelijk zijn en stuurt op uitvoering daarvan.
Eenvoudig gezegd: de teamleider bepaalt uiteindelijk **wat** er in het onderzoek gedaan wordt, de projectleider bepaalt **hoe** deze activiteiten worden ingevuld.
Hij rapporteert over de voortgang van het onderzoek, afwijkingen in planning en onderzoeksopdrachten, de risico's en dergelijke aan de teamleider opsporing.

3.1.5 De rol van de pv-coördinator binnen het onderzoeksteam: plv. projectleider

Naast de rol van projectleider is binnen het onderzoek voor de pv-coördinator een centrale rol weggelegd. Hij is, samengevat, verantwoordelijk voor de opbouw en kwaliteit van het werk- en het procesdossier en staat vanuit deze optiek operationeel vaak naast de projectleider.
Het ligt voor de hand binnen deze rol de vervanging / waarneming van de projectleider te beleggen.

3.1.6 Tegenspraak

Tegenspraak is in opsporingsonderzoeken een additioneel instrument dat bijdraagt aan het voorkomen van groepsdenken en tunnelvisie, waarbij advisering van de projectleider het primaire doel is.

Wanneer wordt tegenspraak ingezet?
Tegenspraak is binnen de FIOD facultatief (op basis van het Programma Versterking Opsporing en Vervolging) en kan worden wordt ingezet bij zaken met een hoge moeilijkheidsgraad, zaken die grote maatschappelijke commotie veroorzaken en/of zaken met een groot politiek / juridisch afbreukrisico, waardoor uitzonderlijke inzet en aandacht van opsporingsdiensten noodzakelijk geacht wordt.
Tegenspraak kan verder worden ingezet in onderzoeken waarin de materie en/of de bewijsvoering meer dan gemiddeld gecompliceerd is.

De criteria voor inzet van tegenspraak komen in belangrijke mate overeen met de criteria die bepalen of er sprake is van een gevoelig onderzoek.
Het is dan ook noodzakelijk dat bij gevoelige onderzoeken wordt beoordeeld of en in hoeverre het instrument tegenspraak wordt ingezet.
Het initiatief voor het inzetten van tegenspraak kan worden genomen door de verschillende betrokkenen bij het opsporingsonderzoek: van het College tot projectleider.

In onderdeel 4-11-400 van het Recherchehandboek zijn een stappenplan en een checklist opgenomen voor de inzet van tegenspraak. Inhoudelijke afstemming vindt plaats met de Landelijk coördinerend vaco; de formele besluitvorming over de inzet van tegenspraak door het MT-FIOD.

3.2 Teamopbouw en kick-off

3.2.1 Teamopbouw naar rollen

Binnen het opsporingsonderzoek zijn – mede gelet op het Copernicus gedachtegoed – behalve de rol van projectleider en pv-coördinator, de volgende rollen benoemd:

- dossierbeheerder
- rechercheur
- hoorder
- pv-schrijver
- pv-lezer
- medewerker geheimhouding.

Voor het bemensen van *omvangrijke onderzoeken* kunnen andere rollen verder essentieel zijn. Gedacht kan worden aan deelprojectleiders, een BOB-coördinator en een EDP-auditor.

Het is bij de teamopbouw en- inrichting van belang de verschillende rollen die noodzakelijk zijn voor het adequaat uitvoeren van het opsporingsonderzoek te benoemen.
Bij gevoelige onderzoeken kunnen namelijk aan de diverse rollen binnen het opsporingsonderzoek verschillende autorisatieniveaus worden gekoppeld (zie hierna ook onderdeel 3.4.5.2 / RBS en 4.1.2 / Summ-IT). Daarmee wordt voorkomen dat iedereen binnen het onderzoek over alle informatie beschikt.
Zo kan het noodzakelijk zijn dat de medewerkers opsporing die bijvoorbeeld observaties uitvoeren slechts toegang hebben tot die delen van het onderzoek die direct invloed hebben op hun observatiewerkzaamheden. De gevoeligheidgraad van een onderzoek kan bepalen dat zij niet geautoriseerd worden voor hogere, tactische niveaus.

3.2.2 Kick-off

De operationele fase van het onderzoek begint met de kick-off. Dit is de eerste bijeenkomst van het onderzoeksteam. De leden van het team worden onder meer geïnformeerd over de doelstellingen van het onderzoek, de onderzoeksopzet, de (digitale) inrichting van het onderzoek en ieders taak binnen het team.
Zeker bij gevoelige onderzoeken is het noodzakelijk de rechercheurs goed te informeren over de wijze waarop de informatie wordt gedeeld, en welke informatie wel en niet wordt gedeeld (only need to know). Dit legt, meer nog dan bij reguliere opsporingsonderzoeken, een extra verantwoordelijkheid bij de rechercheurs. Ook hier geldt dat een meer professionele bewustwording vooropstaat.
Het is binnen de FIOD (nog) niet echt gebruikelijk, maar overwogen kan worden om in een 'charter' of manifest de specifieke afspraken, taken en verantwoordelijkheden vast te leggen die gelden binnen het team.
Gedacht kan worden aan:

- geheimhouding
- afspraken over het gebruik van email
- de inrichting en gebruik van de digitale omgeving (PVS / GRPDATA / RBS / Summ-IT met bijbehorende autorisatieniveaus)
- het al dan niet gebruiken van bio-usbsticks, iPad's en dergelijke
- (beperkt) gebruik van mobiel kantoor internet
- beschikbaarheid van onderzoeksgegevens: alleen op de onderzoekslocatie
- gebruik van printers en beveiligd printen
- clean desk en clean wand
- beveiligingsaspecten van de fysieke locatie
- het gebruik van afgesloten kasten voor gegevensopslag
- bijzondere aandachtspunten, zoals bijvoorbeeld de insiderregeling bij beursgenoteerde ondernemingen
- personele afspraken (reistijdcompensatie, aanwezigheidsregistratie, overwerk en dergelijke)

4 In opsporing nemen van een dossier, bestaande vastleggingen

4.1 De herkomst van het dossier

Een gevoelige zaak kan ruwweg op twee manieren in onderzoek worden genomen:
- door een directe opdracht van de stuurgroep FP – FIOD (veelal geïnitieerd vanuit het OM) en
- via het reguliere (SO/TPO) aanmeldingstraject.

De herkomst van het dossier bepaalt in belangrijke mate de vastleggingen die in het voortraject zijn gedaan.

Bij een directe opdracht van de stuurgroep zal er binnen de FIOD inhoudelijk nog nauwelijks iets bekend zijn over het onderzoek. Er zal in de diverse systemen niet of nauwelijks iets zijn vastgelegd.

Dit ligt anders bij gevoelige onderzoeken die (deels) een 'normaal' aanmeldingstraject hebben gevolgd.
Melding van deze onderzoeken vindt plaats vóór of tijdens de TPO-fase door de teamleider opsporing aan de MT-coach. De MT-coach informeert vervolgens de stuurgroep FP – FIOD.
In opdracht van de stuurgroep kan het onderzoek vervolgens worden opgestart, veelal via het reguliere TPO.
Gedurende het aanmeldingstraject hebben diverse betrokkenen over het onderzoek veel vastleggingen gedaan. Een deel van deze vastleggingen is niet (direct) beheersbaar en onomkeerbaar (mailverkeer!).
De projectleider moet de afbreukrisico's die hiermee gepaard gaan in kaart brengen en de stuurgroep moet uiteindelijk een besluit nemen over de risico's die in het onderzoek worden geaccepteerd.

4.2 GEFIS

Een dossier dat (een deel van) het reguliere aanmeldingstraject heeft doorlopen wordt uiterlijk voorafgaand aan het TPO A in het Geïntegreerd fraude-informatiesysteem (GEFIS) geregistreerd. Daarmee is de onderzoeksinformatie binnen zowel de afdeling Account-OI van de FIOD bekend, als bij de aanleverende ketenpartner (Belastingdienst (aanmelder / BFC-er / CA), Toeslagen, NMa, DNB enzovoort).
De projectleider moet overwegen om de binnen GEFIS vastgelegde informatie aan te passen of zelfs te verwijderen. Dit kan door of via Account-OI worden gerealiseerd.
Verder leggen de medewerkers van Account-OI voorafgaand aan de TPO-fase *buiten* GEFIS onderzoeksinformatie vast, bijvoorbeeld in een projectvoorstel en binnen de GRPDATA-directories.
De projectleider moet inventariseren welke informatie is vastgelegd en hoe deze eventueel is verspreid. Hij bepaalt in overleg met Account-OI welke informatie moet worden vernietigd.

Ook binnen het OM kan inmiddels op diverse plaatsen gevoelige informatie zijn verspreid. De projectleider beoordeelt samen met de zaaksofficier van justitie of en in hoeverre dit is gebeurd en welke maatregelen noodzakelijk zijn om (verdere) verspreiding te voorkomen.

4.3 MRO en RBS

Voor het TPO maakt Account-OI een Melding Recherche Onderzoek (MRO). De FIOD maakt door middel van deze MRO via de Verwijsindex Recherche Onderzoeken en Subjecten (VROS) aan de aangesloten opsporingsdiensten kenbaar dat er binnen de FIOD een strafrechtelijk onderzoek loopt of zal worden opgestart. Daarbij wordt ook informatie verspreid over de subjecten (o.a. verdachten) en de vermoedelijk gepleegde delicten.

Deze informatieverstrekking is onomkeerbaar.
Wel kan verdere tactische verspreiding van de informatie worden voorkomen door aan de MRO de afhandelingscode '00' toe te kennen. Door toekenning van deze afhandelingscode wordt, simpel gezegd, de MRO landelijk alleen op CIE-niveau zichtbaar, maar blijft terugmelding van andere

opsporingsonderzoeken gehandhaafd.
Toekenning van de '00'-afhandelingscode vindt plaats door -en na afstemming met de CIE.

Let op:
De '00'-afhandelingscode mag op basis van de WPG eigenlijk alleen worden gebruikt voor door het College gekwalificeerde embargo-onderzoeken.

De MRO wordt opgemaakt in het Recherche Basis Systeem (RBS). Verder wordt in RBS door Account-OI minimaal een startmutatie opgemaakt. In deze startmutatie zijn naast de MRO-gegevens vaak andere operationele gegevens opgenomen, bijvoorbeeld een omschrijving van de fraude,

5 De huidige digitale omgeving

De FIOD gebruikt en voedt bij het verrichten van een opsporingsonderzoek verschillende systemen, zoals het Proces Verbaal Systeem (PVS), vastleggingen in de directory GRPDATA en RBS.
Verder beschikt de opsporing over de Sherlock-applicatie.

5.1 PVS, GEFIS en SHERLOCK: geen afscherming

Alleen geautoriseerde medewerkers hebben toegang tot deze systemen. Daarmee lijkt een zekere mate van afscherming gerealiseerd, maar in de praktijk is dit niet zo.

Omdat de autorisaties veelal gekoppeld zijn aan algemene functieprofielen, zoals bijvoorbeeld het profiel medewerker opsporing, is binnen de opsporing geen of slechts beperkte afscherming mogelijk. Bovendien zijn ook buiten de opsporing bepaalde functionarissen geautoriseerd.
Bij de toegekende autorisaties is een onderscheid gemaakt tussen de *mutatiefunctie* (relatief beperkte autorisaties) en de *raadpleegfunctie* (relatief uitgebreide autorisaties).
Met name het breed toekennen van deze raadpleegfunctie leidt ertoe dat zowel binnen als buiten onze organisatie een groot aantal functionarissen toegang hebben tot (operationele) opsporingsinformatie. Dit geldt vooral voor de zaken die via het huidige AAFD-traject zijn aangemeld (voorheen het ATV-traject).

PVS maakt gebruik van GEFIS-zaakgegevens. Omgekeerd wordt GEFIS aangevuld met gegevens die in PVS worden vastgelegd. Dit houdt in dat bijvoorbeeld gegevens over verdachten die in PVS worden ingevoerd, ook in GEFIS zichtbaar zijn.
Binnen PVS kunnen geen gegevens zodanig worden afgeschermd, dat zij binnen de raadpleegfunctie in het geheel niet zichtbaar zijn. Hetzelfde geldt voor de gegevens binnen GEFIS.

Sherlock is een applicatie die de gegevens uit GEFIS en PVS doorzoekt.
Sherlock is toegankelijk voor medewerkers van de FIOD die geautoriseerd zijn voor het gebruik van PVS. Ook hiervoor geldt dat geen gegevens kunnen worden afgeschermd.

Binnen GEFIS kan een onderzoek als vertrouwelijk worden aangevinkt, wat tot gevolg heeft dat deze onderzoeken niet in Sherlock wordt opgenomen. Hiermee wordt voor Sherlock een beperkte mate van afscherming gerealiseerd

5.2 Autorisatieniveaus PVS, GEFIS en SHERLOCK

Het raadplegen van de lopende en afgesloten zaken is veelal gefaseerd en gekoppeld aan de fase waarin de zaak zich bevindt (SO / TPO / Lopend enz.).
Als bijlage 2 bij deze beschrijving is een autorisatiematrix gevoegd waarin per applicatie de functietypen / autorisatiegebieden zijn benoemd met de daarbij behorende bevoegdheden (beheren / muteren / raadplegen).
Voor PVS, GEFIS en SHERLOCK gelden *binnen de FIOD* voor het raadplegen globaal de hierna vermelde autorisatieniveaus.

Functieprofiel	***Autorisatie***
Opsporingsmedewerker (OMD)	lopende zaken van eigen kantoor van de zaak waar de medewerker aan gekoppeld is als zaaksrechercheur en alle afgesloten zaken
Medewerker opsporingsinformatie (MOP) Medewerker CIE	lopende zaken van alle kantoren en alle afgesloten zaken
teamleider opsporing (TOP) Medewerker account (MAC) teamleider account (TAC)	lopende zaken van eigen kantoor en alle afgesloten zaken

Verder zijn *binnen de FIOD* voor GEFIS nog de volgende autorisatieniveaus voor het raadplegen van onderzoeken toegekend:

Functieprofiel	***Autorisatie***
Administratie medewerker (ADM) Informatiemedewerker (INF) FIOD vestigingshoofd (FVH)	alle onderzoeken van het kantoor (gefaseerd)
Helpdesk medewerker (HDM) Algemeen project manager (APM):	alle onderzoeken (landelijk)

Extern zijn de volgende autorisatieniveaus toegekend:

Functieprofiel	***Autorisatie***
Boete Fraude Coördinator (BFC) Contactambtenaar (CA) Medewerkers van de Belastingdienst en Douane	raadpleegrechten in alle onderzoeken. (gefaseerd, landelijk)

Uit het voorgaande blijkt dat afscherming van gevoelige onderzoeken binnen PVS, GEFIS en SHERLOCK slechts zeer beperkt mogelijk is.
Bij een hoge gevoeligheidsgraad van het onderzoek wordt gebruik van deze systemen in de operationele fase van het onderzoek dan ook ontraden. Eventueel kan worden besloten na afronding van (delen van) het onderzoek relevante data op te nemen in de systemen.

5.3 GRPDATA

Binnen de kantoorautomatisering kan voor een gevoelig onderzoek een eigen map of mapstructuur worden aangemaakt. De teamleden binnen het opsporingsonderzoek worden individueel voor één of meer mappen geautoriseerd, met bijbehorende schrijf- of leesrechten.
De aldus aangemaakt map(structuur) is niet toegankelijk voor andere gebruikers van de kantooromgeving. Wel blijft de map(structuur toegankelijk voor de (systeem)beheerder.

Hoewel in verband met WPG-aspecten het gebruik van GRPDATA-directories moet worden beperkt, kan binnen een gevoelig onderzoek toch worden gekozen voor integrale vastlegging van de onderzoeksdata in een dergelijke structuur.
De teamleider opsporing moet voor het gebruik van GRPDATA-directories toestemming geven (besluit MT 11-029)

5.4 RBS

5.4.1 RBS en VROS

RBS heeft geen directe koppeling met VROS. Momenteel wordt binnen de CIE de gegevens van de MRO handmatig verwerkt in de Basis Voorziening Opsporing (BVO) van waaruit export plaatsvindt naar VROS. BVO is een van de bedrijfsprocessystemen van de politie.
Levert de VROS-matching een hit op dan worden beide instanties geïnformeerd. Er wordt verder geen operationele onderzoeksinformatie uitgewisseld, dit vindt uitsluitend plaats na (telefonisch) overleg tussen de partijen die bij de VROS-hit zijn betrokken.

Hieruit vloeit voort dat indien de MRO-melding niet (verder) wordt aangevuld en geactualiseerd, er geen verdere informatie over een lopend onderzoek met andere politiediensten wordt gedeeld.

De CIE kan worden gevraagd om de MRO-melding niet in VROS op te nemen, als afgehandeld te coderen of geheel uit VROS te verwijderen.
Een als afgehandeld gecodeerde MRO-melding blijft nog zes maanden in VROS zichtbaar en is daarna verdwenen. Een verwijderde VROS-melding verdwijnt direct uit de VROS-database.

Uit oogpunt van afscherming kan het wenselijk zijn om de MRO-gegevens niet in VROS op te nemen of daaruit te verwijderen, maar dit heeft een keerzijde. Het onderzoeksteam blijft dan verstoken van mogelijk relevante subjectinformatie, bijvoorbeeld actueel vuurwapengebruik van (nieuwe) verdachten.

5.4.2 Autorisatieniveaus

RBS kent de mogelijkheid om horizontale en verticale autorisaties toe te kennen en daarmee (een deel van) de informatie af te schermen.
Binnen RBS wordt aan gegevens(groepen) een autorisatieniveau toegekend in het bereik van 0 t/m 9. De *horizontale* autorisatieniveaus 0 t/m 3 worden gebruikt om gegevens zichtbaar te maken binnen en buiten de eigen registratie (onderzoek). De *verticale* autorisatieniveaus 4 t/m 9 worden gebruikt om binnen de eigen registratie onderscheid aan te kunnen brengen wie bij welke gegevens kan.

Medewerkers worden binnen RBS geautoriseerd voor specifieke onderzoeken. Daarnaast kunnen medewerkers op basis van rollen en taken autorisatie krijgen waarbij er ook doorzicht (op de verticale autorisatie) kunnen worden gerealiseerd.
In beginsel wordt alle beschikbare informatie tot en met niveau 3 binnen RBS onbeperkt gedeeld.

5.4.2.1 Standaardautorisatie
Aan de FIOD-onderzoeken worden standaard autorisatieniveau 4 toegekend. Dat houdt in dat binnen de opsporingsomgeving alleen aan een bepaald onderzoek toegewezen rechercheurs (gebruikers)toegang hebben tot de onderzoeksinformatie.
Verder zijn de onderzoeksgegevens op autorisatieniveau 4 zichtbaar voor de medewerkers van de infodesk (politie: informatieorganisatie), OI/Account en de CIE.
Autorisatieniveau 5 tot en met 9 kennen telkens een hogere mate van gegevensafscherming.

5.4.2.2 Autorisatieniveaus gevoelige onderzoeken
Op basis van het voorgaande kan voor gevoelige onderzoeken worden gekozen voor de volgende verticale autorisatieniveaus:

functie	***niveau***	***bijzonderheden***	***Productvoorbeeld:***
Teamleider, Projectleider PV- coördinator	7	Gegevens zijn alleen beschikbaar voor teamleider en projectleider	Afsprakenjournaal (Voortgangs)rapportages Gespreksverslagen MT, OM
Deelprojectleider, Dossiervormer	6	Gegevens zijn beschikbaar voor teamleider, (deel)projectleider en de overige leven van de teamleiding. *Buiten het onderzoek:* teamleider / coördinator CIE.	Verstrekkingenjournaal Plan van aanpak BOB-specifieke PV's
Medewerker opsporing	5	Gegevens zijn zichtbaar voor alle leden van het opsporingsteam Gegevens zijn *buiten het onderzoek* zichtbaar voor de teamleider CIE en teamleider Infodesk.	PV-AH Documenten PVVV Rechtshulpverzoek

Indien een hogere mate van of meer differentiatie in afscherming noodzakelijk is, kan in uitzonderingsgevallen gekozen worden voor uitbreiding van de autorisatieniveaus:

functie	***niveau***	***bijzonderheden***	***Productvoorbeeld:***
Teamleider, Projectleider PV- coördinator	8	Gegevens zijn alleen beschikbaar voor teamleider en projectleider	Afsprakenjournaal (Voortgangs)rapportages Gespreksverslagen MT, OM
Deelprojectleider, Dossiervormer BOB-coördinator	7	Gegevens zijn beschikbaar voor teamleider, (deel)projectleider en de overige leden van de teamleiding.	Verstrekkingenjournaal Plan van aanpak BOB-specifieke PV's
Medewerker opsporing	6	Gegevens zijn zichtbaar voor alle leden van het opsporingsteam *Buiten het onderzoek:* teamleider / coördinator CIE.	Rechtshulpverzoek PV-AH PVVV Documenten CIE-info
Medewerker opsporing, observatie	5	Gegevens zijn zichtbaar voor alle leden van het opsporingsteam Gegevens zijn *buiten het onderzoek* zichtbaar voor de teamleider CIE en teamleider Infodesk	PV-observatie Documenten PVVV

Let op:
Door verhoging van de autorisatieniveaus wordt de free-flow of information naar andere politiediensten die op basis van de WPG verplicht is, ernstig beperkt.
Dit is formeel alleen toegestaan als er een WPG-weigeringsgrond bestaat, conform art 2:13 van het Besluit Politiegegevens.
Wordt besloten tot een verhoging van de autorisatieniveaus is voorafgaande afstemming met de stuurgroep FP – FIOD noodzakelijk.

5.4.3 Blueview en RBS

Blueview is een zoekmachine die binnen de politie wordt gebruikt om vanuit de totale beschikbare informatie de relevante gegevens op te zoeken.
De zoekmachine maakt gebruik van een achterliggende centrale database die onder meer wordt gevoed met de lokaal (FIOD, politie) ingevoerde gegevens.

Blueview heeft geen directe koppeling met RBS, maar wel een exportfunctie vanuit BVO.
Zowel de CIE als de Infodesk hebben binnen de FIOD toegang tot BVO en muteren op basis van RBS-informatie in dit systeem (zie onderdeel 5.4.1: RBS en VROS).
Via BVO worden dus onderzoeksgegevens verwerkt in Blueview.
Deze informatie is zichtbaar voor de aangewezen opsporingsambtenaren binnen de aangesloten opsporingsdiensten.
De toegankelijkheid van de informatie gaat daarmee in Blueview verder dan die binnen VROS. In VROS is sprake van het hit - no hit principe, terwijl binnen Blueview de feitelijke informatie zichtbaar is.

Geadviseerd wordt om bij gevoelige onderzoeken de exportfunctie van gegevens vanuit BVO naar Blueview uit te zetten.

6 De digitale omgeving medio 2012

6.1 Summ-IT

6.1.1 MRO-functionaliteit

In Summ-IT wordt geen aparte MRO mutatie meer gemaakt, de functionaliteit hiervan is binnen Summ-IT verbonden aan de entiteit Strafbaar Feit. Alle entiteiten die aan het Strafbaar Feit zijn gerelateerd (behalve slachtoffers, getuigen en melders) worden automatisch in de MRO opgenomen.

De VROS-koppeling binnen Summ-IT staat standaard aan. Indien het voor een onderzoek ongewenst is om de gegevens mee te sturen richting VROS dan kan de koppeling worden uitgeschakeld.
Gelet op de wettelijk verplichte (WPG) free-flow of information moet deze basale informatie-uitwisseling gehandhaafd blijven.

6.1.2 Autorisatieniveaus

Summ-IT kent de mogelijkheid om horizontale en verticale autorisaties toe te kennen en daarmee (een deel van) de informatie af te schermen.
Binnen Summ-IT wordt aan gegevens(groepen) een autorisatieniveau toegekend in het bereik van 0 t/m 9. De *horizontale* autorisatieniveaus 0 t/m 3 worden gebruikt om gegevens zichtbaar te maken binnen en buiten de eigen registratie. De verticale autorisatieniveaus 4 t/m 9 worden gebruikt om binnen de eigen registratie onderscheid aan te kunnen brengen wie bij welke gegevens kan.
Medewerkers worden binnen Summ-IT geautoriseerd voor specifieke registraties (onderzoeken). Daarnaast kunnen medewerkers op basis van rollen en taken autorisatie krijgen waarbij er ook doorzicht (op de verticale autorisatie) kunnen worden gerealiseerd.
In beginsel wordt alle beschikbare informatie tot en met niveau 3 binnen Summ-IT onbeperkt gedeeld.

6.1.2.1 Standaardautorisatie

Verticale autorisatie vindt plaats vanaf autorisatieniveau 3 en regelt wie binnen de FIOD over welke informatie kan beschikken. Aan de FIOD-onderzoeken worden standaard autorisatieniveau 4 toegekend. Dat houdt in dat binnen de opsporingsomgeving alleen aan een bepaald onderzoek toegewezen rechercheurs (gebruikers) toegang hebben tot de onderzoeksinformatie.
Verder zijn de onderzoeksgegevens op autorisatieniveau 4 zichtbaar voor de medewerkers van de infodesk, OI/Account (politie: informatieorganisatie) en de CIE.
Autorisatieniveau 5 tot en met 9 kennen telkens een hogere mate van gegevensafscherming.

6.1.2.2 Autorisatieniveaus gevoelige onderzoeken

Op basis van het voorgaande kan voor gevoelige onderzoeken worden gekozen voor de volgende verticale autorisatieniveaus:

functie	***niveau***	***bijzonderheden***	***Productvoorbeeld:***
Teamleider, Projectleider, PV- coördinator	7	Gegevens zijn alleen beschikbaar voor teamleider en projectleider	Afsprakenjournaal (Voortgangs)rapportages Gespreksverslagen MT, OM
Deelprojectleider, Dossiervormer	6	Gegevens zijn beschikbaar voor teamleider, (deel)projectleider en de overige leven van de teamleiding. *Buiten het onderzoek:* teamleider / coördinator CIE.	Verstrekkingenjournaal Plan van aanpak BOB-specifieke PV's
Medewerker opsporing	5	Gegevens zijn zichtbaar voor alle leden van het opsporingsteam Gegevens zijn *buiten het onderzoek*	PV-AH Documenten PVVV

		zichtbaar voor de teamleider CIE en teamleider Infodesk	Rechtshulpverzoek

Indien een hogere mate van afscherming noodzakelijk is, of bijvoorbeeld in het onderzoek wordt getapt, waarbij het van belang is dat de medewerkers van de tap en tolken / vertalers niet kunnen beschikken over strategische en tactische informatie, kan gekozen worden voor uitbreiding van de autorisatieniveaus:

functie	***niveau***	***bijzonderheden***	***Productvoorbeeld:***
Teamleider, Projectleider	8	Gegevens zijn alleen beschikbaar voor teamleider en projectleider	Afsprakenjournaal (Voortgangs)rapportages Gespreksverslagen MT, OM
PV- coördinator, Deelprojectleider, Dossiervormer BOB-coördinator	7	Gegevens zijn beschikbaar voor teamleider, (deel)projectleider en de overige leden van de teamleiding.	Verstrekkingenjournaal Plan van aanpak BOB-specifieke PV's
Medewerker opsporing	6	Gegevens zijn zichtbaar voor alle leden van het opsporingsteam *Buiten het onderzoek:* teamleider / coördinator CIE.	Rechtshulpverzoek PV-AH PVVV Documenten CIE-info
Medewerker opsporing, observatie	5	Gegevens zijn zichtbaar voor alle leden van het opsporingsteam Gegevens zijn *buiten het onderzoek* zichtbaar voor de teamleider CIE en teamleider Infodesk	PV-observatie Documenten PVVV

Let op:
Door verhoging van de autorisatieniveaus wordt de free-flow of information naar andere politiediensten die op basis van de WPG verplicht is, ernstig beperkt.
Dit is formeel alleen toegestaan als er een WPG-weigeringsgrond bestaat, conform art 2:13 van het Besluit Politiegegevens.
Wordt besloten tot een verhoging van de autorisatieniveaus is afstemming met de stuurgroep FP – FIOD noodzakelijk.

6.1.3 Summ-IT en Blueview

Blueview is een zoekmachine die binnen de politie wordt gebruikt om vanuit de totale beschikbare informatie de relevante gegevens op te zoeken.
De zoekmachine maakt gebruik van een achterliggende centrale database die onder meer wordt gevoed met de lokaal (FIOD, politie) ingevoerde gegevens.

Voor Summ-IT wordt de subject -en delictsinformatie tot en met autorisatieniveau 5 opgenomen in de centrale database en is daarmee in beginsel zichtbaar voor aangewezen functionarissen binnen de aangesloten opsporingsdiensten.
Naast subject- en delictsinformatie wordt ook andere informatie opgenomen die in Summ-IT is verwerkt. Bijvoorbeeld informatie over vervoersmiddelen, communicatiemiddelen en locaties.
De informatie tot en met autorisatieniveau 5 is via Blueview landelijk zichtbaar voor de teamleider infodesk (politie: informatiecoördinator) en de teamleider/ coördinatoren CIE.

Daarmee wordt door middel van Blueview een deel van de operationele onderzoeksinformatie gedeeld met de aangesloten opsporingsdiensten.

Geadviseerd wordt om bij gevoelige onderzoeken de exportfunctie van gegevens vanuit Summ-IT naar Blueview uit te zetten.

6.1.4 Summ-IT en 'Zoeken en Speuren'

Binnen Summ-IT is een zoekfunctionaliteit opgenomen: Zoeken en Speuren.
Door middel van 'zoeken' en 'speuren' heeft de geautoriseerde medewerker toegang tot alle onderzoeken op het aan hem toegekende algemene autorisatieniveau. Aan de medewerker opsporing is standaard autorisatieniveau 4 toegekend. Concreet hout dit in dat de medewerker opsporing kan zoeken in alle onderzoeken, tot en met autorisatieniveau 4.

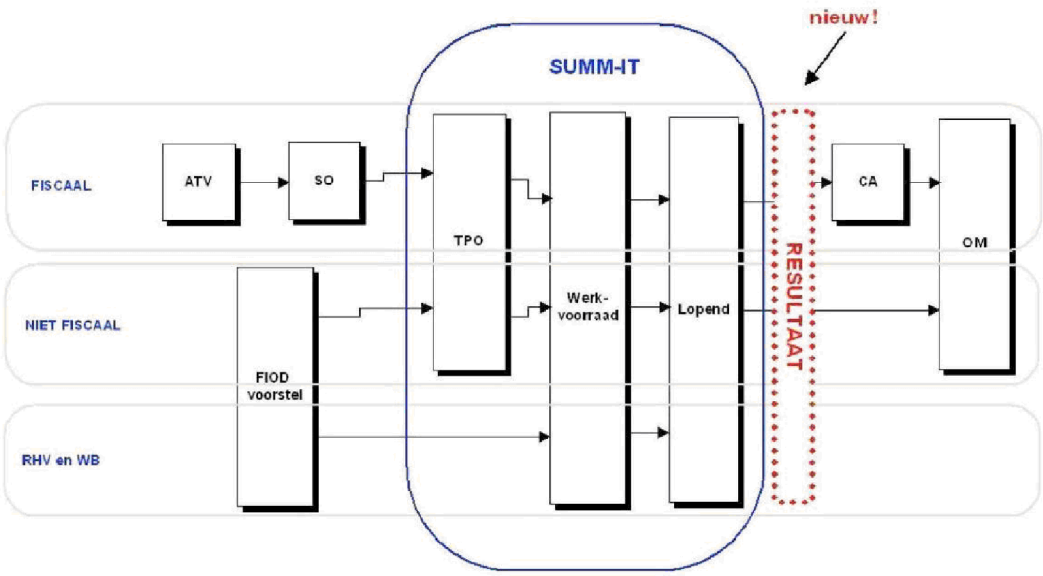
Daarnaast heeft hij via 'speuren' toegang tot zijn 'eigen' onderzoeken tot en met het autorisatieniveau wat hem voor die specifieke onderzoeken is toegekend. Dat zal veelal een hoger autorisatieniveau zijn dan het algemene niveau 4.

Het voorgaande houdt in dat gegevens die binnen Summ-IT tot en met autorisatieniveau 4 zijn geclassificeerd, voor iedere medewerker opsporing zichtbaar zijn. Gegevens met een hoger autorisatieniveau zijn alleen zichtbaar voor rechercheurs met autorisatie voor dat hogere niveau.

6.2 GEFIS 2.0

De applicatie GEFIS is om systeemtechnische redenen in de huidige vorm tot uiterlijk eind 2013 bruikbaar.

Er is onderzocht of Summ-IT alle functies van GEFIS voor de FIOD kan vervullen. Dit bleek niet het geval. Daarom is in december 2011 aangegeven dat een deel van de huidige functies van GEFIS van de FIOD gehandhaafd moeten blijven. Deze functies zitten voornamelijk in de aanmeldingsfase van het onderzoek en de fase van afwerking van het onderzoek.
Schematisch:



Voor het ontwerp van GEFIS 2.0 wordt een businesscase gemaakt, waarbij rekening zal worden gehouden met de wens vanuit de opsporing om gevoelige onderzoeken te kunnen afschermen.

7 De fysieke locatie

Gevoelige onderzoeken vragen om een fysieke locatie die volledig of gedeeltelijk is afgescheiden van de reguliere opsporingsomgeving. Ook hier bepaalt de mate van vertrouwelijkheid de mate van afscherming.

7.1 Externe locatie

Bij extreem gevoelige zaken kan gekozen worden voor een externe locatie die beter is beveiligd dan de eigen FIOD-locaties. Zo zijn in het verleden onderzoeken ondergebracht in een districtsbureau van politie, een locatie van de Koninklijke Marechaussee en een militair vliegveld, alle met 24/7 bewaking.

De keuze voor een dergelijke locatie brengt enerzijds het voordeel van een optimale beveiliging, maar vergt anderzijds organisatorisch nogal het nodige.
Zo zal een eigen digitaal netwerk moeten worden ingericht met beheersborging vanuit de FIOD.
Voor het gebruik van Summ-IT zal vanaf de externe locatie dan toegang tot het Belastingdienstnetwerk moeten worden verkregen.
Er zal ook binnen de externe locatie bijvoorbeeld fysieke toegangsbeperking moeten worden georganiseerd.
Is een dergelijke externe locatie noodzakelijk, zal dit door de directeur FIOD / MT moeten worden gefaciliteerd.

7.2 Interne locatie

7.2.1 Afgescheiden onderzoekslocatie

Nagenoeg alle gevoelige onderzoeken zullen binnen de eigen FIOD-omgeving worden uitgevoerd. Zoals al eerder aangegeven vraagt dit om een (gedeeltelijke) fysieke afscheiding van de reguliere opsporingsomgeving. Dit kan worden gerealiseerd door het onderzoek onder te brengen op een afzonderlijke vleugel of gang van een FIOD-kantoor. Via pasautorisatie wordt geregeld dat slechts de leden van het onderzoeksteam toegang hebben tot de onderzoekslocatie.
Bij omvangrijke inbeslagnames kan gekozen worden voor een externe ruimte waar het beslag wordt opgeslagen. Het spreekt voor zich dat voor een dergelijke ruimte overeenkomstige toegangsbeperking moet worden gecreëerd. Uit beheersoogpunt kan de toegang tot een dergelijke ruimte binnen het opsporingsteam verder worden beperkt tot bijvoorbeeld de pv-coördinator en de dossiervormer(s).

Speciale aandacht vraagt afscherming op de kantoren waar de opsporing organisatiegericht is gehuisvest. Het gebruikt van flex-werkplekken staat haaks op de gewenste afscherming en moet worden vermeden.

Ook hier geldt dat een en ander met de (in dit geval) gedelegeerd opdrachtgever (teamleider opsporing) van het onderzoek moet worden afgestemd. Hij is immers vanuit zijn rol verantwoordelijk voor de facilitering.

7.2.2 'Sweepen' van de onderzoeksruimten

Laat voorafgaand aan het onderzoek de onderzoeksruimten controleren op ongewenste (afluister)apparatuur. Dit onderzoek, het zogenaamde 'sweepen' van de onderzoeksruimten, wordt via de CIE uitgevoerd door specialisten van het KLPD. Het sweepen moet periodiek worden herhaald. Naast het onderzoeken van de onderzoekslocatie kan ook worden overwogen de auto's die bij het onderzoeksteam in gebruik zijn op dezelfde wijze te laten onderzoeken.

7.2.3 Overige aandachtspunten

Denk bij de verdere inrichting om de volgende aandachtspunten:

- zorg ervoor dat de individuele kamers, actiekamers en opslagruimten kunnen worden afgesloten
- zorg ervoor dat de onderzoeksleiding kan beschikken over één of meer kluiskasten bij voorkeur met een cijferslot
- zorg ervoor dat alleen onder toezicht (schoonmaak)werkzaamheden binnen de onderzoeksruimten plaatsvinden
- zorg met name bij dergelijke werkzaamheden voor clean desk en clean wand
- indien gebruik wordt gemaakt van printers die buiten de afgeschermde omgeving staan, zorg er dan voor dat er uitsluitend beveiligd wordt afgedrukt en dat de leden van het onderzoeksteam hierover afdoende zijn geïnformeerd

7.3 Locatie OVC en Tap

Het kan voorkomen dat in een onderzoek wordt besloten tot het opnemen van vertrouwelijke communicatie (OVC) of het opnemen van telecommunicatie. Gaat het daarbij om het opnemen van communicatie in de Nederlandse taal, kan de coördinatie en het uitwerken van de communicatie in beginsel plaatsvinden op de eigenlijke onderzoekslocatie.

Wordt gebruik gemaakt van tolk- en/of vertaaldiensten dan moet worden overwogen om de OVC/taplocatie fysiek af te scheiden van de overige onderzoeksruimten.

Ervaringen met eerdere gevoelige onderzoeken hebben geleerd dat de inzet van tolken en vertalers die toegang hebben tot strategische onderzoeksruimtes het risico op het lekken van vertrouwelijke informatie aanmerkelijk verhoogt.

8 Inzet van tolken en vertalers

8.1 TVCN en Concorde

Momenteel is de FIOD, als onderdeel van de Belastingdienst, contractueel verplicht de tolkdiensten af te nemen via het Tolk- en vertaalcentrum Nederland BV: TVCN. Eenzelfde verplichting geldt voor het inhuren van vertalers die worden betrokken via de Concorde Group BV.
Van de afnameverplichting kan worden afgeweken indien TVCN of Concorde geen tolk of vertaler kan leveren met de door de FIOD gewenste specificaties, met name daar waar de FIOD vraagt om gescreende tolken/vertalers.

Bestaat binnen een gevoelig onderzoek de behoefte aan een gescreende tolk of vertaler, dan kan om die reden een tolk of vertaler worden gecontracteerd buiten TVCM of Concorde-contracten om.

Dat kan via het Nationaal Tolken Coördinatiepunt (NTC), een onderdel van het KLPD.

8.2 Het Nationaal Tolken Coördinatiepunt

Het NTC beheert een database waarin ca 1000 beëdigde tolken/vertalers zijn ondergebracht. Het NTC screent via het bureau veiligheid en integriteit van het KLPD de tolken voordat zij worden opgenomen in de database. Periodiek vindt hertoetsing plaats. Een eventuele AIVD-screening is bij het NTC bekend.
Verder legt het NTC waar nodig de ervaringen met tolken in de opsporing vast.

Met ingang van 1 januari 2012 is het Nationaal Tolken Coördinatiepunt (opgericht door de Politie Haaglanden) ondergebracht bij het KLPD. Bij het NTC zijn inmiddels nagenoeg alle politieregio's aangesloten. De FIOD streeft naar een aansluiting medio 2012.

Let op 1:
De tolken / vertalers maken voor hun vertaaldiensten vaak gebruik van CAT Tools (digitale vertaalhulpmiddelen) zoals Trados of Wordfast.
De tolken/vertalers slaan in dit programma tekstfragmenten en dergelijke op voor (toekomstig) vertaalwerk.
Dit kan ertoe leiden dat geclassificeerde onderzoeksinformatie buiten het onderzoek wordt gebracht. Geadviseerd wordt om bij een hoge mate van gevoeligheid het vertaalwerk uitsluitend te laten uitvoeren met behulp van FIOD-apparatuur en software.

Let op 2:
Het spreekt voor zich dat gevoelige informatie niet extern wordt vertaald. De gecontracteerde tolk of vertaler mag zijn tolk- of vertaaldiensten uitsluitend uitvoeren binnen de FIOD-omgeving.

Bijlage 1 Checklist gevoelige onderzoeken

Rollen en actoren

- ☐ Controleer of de rol van de stuurgroep voldoende duidelijk is en of deze rol afdoende is beschreven/vastgelegd[1]
- ☐ Stel vast of is bepaald wanneer / door wie / op welke wijze de stuurgroep wordt geïnformeerd[1]
- ☐ Stem de rolinvulling van teamleider en projectleider op elkaar af en benoem zo concreet mogelijk per rol de taken en verantwoordelijkheden
- ☐ Beoordeel of de onderzoeksopdracht / doelstelling van het onderzoek voldoende duidelijk en eenduidig is
- ☐ Borg de waarneming / vervanging van de sleutelrollen binnen het opsporingsteam, met name die van de projectleider en de pv- coördinator
- ☐ Beoordeel of en in hoeverre er tegenspraak moet worden ingezet
  Zie onderdeel 4-11-400 van het Recherchehandboek (stappenplan + checklist).
  Stem zo nodig inhoudelijk af met de Landelijk coördinerend vaco,
  Contactpersoon: [ ], [ ], *06-*[ ]

Teamopbouw en kick-off

- ☐ Bepaal welke functies en rollen er binnen het opsporingsteam noodzakelijk zijn en welke informatie er tussen deze teamleden moet worden gedeeld
- ☐ Organiseer een startbijeenkomst waarbij de diverse functies en rollen worden benoemd met de daaraan verbonden rechten en plichten
- ☐ Benoem de specifieke afspraken die binnen het onderzoeksteam geldend zullen zijn en zorg ervoor dat ieder teamlid deze kent en onderschrijft ('charter')

Informatie-uitwisseling intern (FIOD)

- ☐ Stem af met wie en op welke momenten er informatie wordt gedeeld
  (stuurgroep / teamleider)
  Let op: dit is een wederkerig proces; ook moet geborgd zijn dat strategische en beleidsmatige besluiten direct worden gedeeld met de projectleider
- ☐ Stem af of de informatie mondeling en/of schriftelijk wordt uitgewisseld
- ☐ Bepaal welke informatie wordt gedeeld
  (strategisch / beleidsmatig / inhoudelijk)
- ☐ Indien er (ook) schriftelijk wordt gerapporteerd: bepaal op welke wijze deze rapportage plaatsvindt
  (voortgangsrapportage / inzage onderzoeksjournaal)
- ☐ Borg bij voortgangsrapportages met significante afwijkingen afstemmingsoverleg met de stuurgroep
- ☐ Leg de routing vast van de schriftelijke informatieverstrekking
  (rechtstreeks MT of stuurgroep / via de 'lijn')

Informatie-uitwisseling extern (OM / andere ketenpartners)

- ☐ Bepaal met wie onderzoeksinformatie wordt uitgewisseld
  (hoofdofficier / zaaksovj / parketsecretaris / ontnemingsovj)
- ☐ Bepaal op welke wijze de onderzoeksinformatie wordt uitgewisseld
  (fysiek/mondeling/fax/mail)
- ☐ Bepaal welke informatie er wordt uitgewisseld en wanneer dit plaatsvindt
- ☐ Maak afspraken hoe de uitwisseling van informatie wordt vastgelegd
- ☐ Bepaal wie onderzoeksinformatie aan (anderen dan het OM) mag verstrekken en mag verspreiden
- ☐ Maak een versterkingsjournaal en een verspreidingsjournaal waarin alle verstrekkingen en verspreidingen worden vastgelegd
- ☐ Inventariseer de belangen van de aanmelder / toezichthouder en anticipeer daarop

(afspraken inzet bestuur/tuchtrecht, daarvoor noodzakelijke informatiedeling)

- ☐ Maak afspraken over persvoorlichting met het FP en beperk de te verstrekken informatie tot de gebeurtenissen. Verstrek geen inhoudelijke informatie.
- ☐ Maak zo nodig een communicatiematrix waarin de totale informatie-uitwisseling verder wordt uitgewerkt

In opsporing nemen van het dossier

- ☐ Inventariseer welke partijen reeds over onderzoeksinformatie beschikken (Belastingdienst, andere toezichthouder / TPO / OM)
- ☐ Tref maatregelen om verdere ongewilde verspreiding van deze informatie te voorkomen (overleg BFC / CA/ andere aanmeldende toezichthouder / OM)
- ☐ Inventariseer met Account-OI welke startinformatie er over het onderzoek inmiddels in de systemen (Email / GEFIS / RBS / PVS / Groepsdata / Summ-IT) is verwerkt en wie tot deze informatie is geautoriseerd
- ☐ Zorg er voor dat waar nodig deze informatie wordt aangepast/geanonimiseerd/verwijderd en de autorisaties worden beperkt.
  [ ] [ ], [ ] *Account-OI Midden, 06 –* [ ]
- ☐ Ga na of er een MRO is aangemaakt. Is er een MRO aangemaakt dan deze in overleg met de CIE als '00'classificeren .
  Is er nog geen MRO aangemaakt, moet met de melding terughoudend worden omgegaan; ook in dit geval kan de afhandelingscode '00' worden toegekend.
  Contact CIE: *Helpdesk CIE, 030 –* [ ]

De digitale omgeving

- ☐ Beoordeel of en in hoeverre een eigen digitaal netwerk noodzakelijk is
  [ ] [ ], [ ] *FITT, 06 –* [ ]
- ☐ Bepaal welke bestaande systemen er worden gebruikt binnen het onderzoek en op welk moment er welke informatie wordt vastgelegd of vrijgegeven
  (PVS / GEFIS / SHERLOCK / GRPDATA / RBS / Summ-IT)
- ☐ Bepaal bij gebruik van RBS/Summ-IT voor de diverse onderzoeksrollen –en functies het verticale autorisatieniveau
- ☐ Beoordeel of de informatie die via de MRO-melding in VROS is opgenomen moet worden aangepast.
  Houd rekening met de WPG-verplichting tot het delen van informatie!
- ☐ Zorg er voor dat de blueview-exportfunctie is uitgeschakeld
  [ ] [ ], *Applicatiebeheer RBS 06 –* [ ]
  [ ] [ ], *Functioneel beheer, 06 –* [ ]
- ☐ Bepaal bij gebruik van de GRPDATA-director(y)(ies) wie toegang heeft en welke rechten er worden toegekend
  (lees en/of schrijfrechten)
  Contactpersoon: [ ], [ ] *toepassingsbeheer, 06 –* [ ]

De fysieke locatie

- ☐ Beoordeel of het onderzoek op een externe locatie moet worden ondergebracht. Afstemming met de opdrachtgever (directeur FIOD / MT) is noodzakelijk in verband met hun facilitering!
- ☐ Laat voorafgaand aan het onderzoek en periodiek via de CIE de onderzoeksruimten 'sweepen'
  [ ] [ ], [ ] *CIE, 06 –* [ ]
- ☐ Bepaal of en in hoeverre het onderzoek moet worden uitgevoerd in een afgeschermd deel van een FIOD-kantoor en bepaal waar nodig de toegangsautorisaties voor (delen van) de onderzoeksruimte(n). Wordt gebruik gemaakt van een externe beslagruimte, zorg ook daar voor afdoende toegangsbeperking
  Afstemming met gedelegeerd opdrachtgever (teamleider opsporing) is noodzakelijk in verband met diens facilitering!

		, 06 –	
		, 06 –	

- ☐ Realiseer waar nodig afsluitbare individuele kamers, actiekamers en opslagruimten
- ☐ Zorg ervoor dat de onderzoeksleiding kan beschikken over één of meer kluiskasten bij voorkeur met een cijferslot
- ☐ Zorg ervoor dat alleen onder toezicht (schoonmaak)werkzaamheden binnen de onderzoeksruimten plaatsvinden
- ☐ Zorg met name bij dergelijke werkzaamheden voor clean desk en clean wand
- ☐ Zorg bij gebruik van externe printers dat er uitsluitend beveiligd wordt afgedrukt. Zie de Gebruikersinstructie multifunctional als printer (Fenster/Voor iedereen/automatisering, telefonie/automatisering, Diversen/ Multifunctionals (printen)

Locatie OVC, Tap en inzet tolken

- ☐ Beoordeel of er een afzonderlijke locatie voor OVC/Tap noodzakelijk is
- ☐ Zorg dat vertaalwerk uitsluitend op een daartoe aangewezen FIOD-locatie plaatsvindt en binnen de digitale omgeving van de FIOD
- ☐ Huur indien noodzakelijk uitsluitend gescreende tolken en vertalers in (Nationaal Tolken Coördinatiepunt KLPD)
  Contactpersoon: *(Staf/V&O) 06 –*

Bijlage 2 Autorisatiematrix PVS, GEFIS en SHERLOCK

Applicatie / Functietypen / Autorisatiegebied	*Bevoegdheden*										
PVS FIOD											
MAC – Medewerker account	26	27	Z	Y	2a	S					
MOP – Medewerker opsporingsinformatie	28		X	Y	2a	S					
OMD – Opsporingsmedewerker	22	23	X	Y	2a	S					
TAC – teamleider account	26	27	Z	Y	2a	S					
TOP – teamleider opsporing	24	25	X	Y	2a	S					
GEFIS FIOD											
ADM – Admin. Medewerker (muteren eigen CT)	4 B	1 C	1 E	1 F	1I	3H	P				
FVH – FIOD teamleider, muteren eigen CT	4 B	1 C	1 E	1 F	1I	3H	P	29			
INF – Informatiemedew./ account , muteren eigen CT)	4 B	1 C	1 E	1 F	1I	3H	P				
GEFIS BELASTINGDIENST / DOUANE											
BFC – Boetefraudecoordinator	1 A	1 B	1 D	7 F	7 H	7 I	R				
BFC/OG – Boetefraudecoordinator / ondersteuning	1 A	1 B	1 D	7 F	7 H	7 I	R				
BFC/CA – Boetefraudecoordinator / contactamb.	2 B	2 C	3 C	2 F	3 F	5 F	1 H	2 I	5 I	Q	8
BFC/CA-OG – Boete fraude coördinator / contactambtenaar ondersteuning	2 B	2 C	3 C	2 F	3 F	5 F	1 H	2 I	5 I	Q	9
GEFIS ANDERS											
APM – Algemeen projectmanager (landelijk alles met beperkte mutatierechten-Liaison)	1 H	S									
HDM – Helpdesk medewerker (HIT NO HIT raadplegen landelijk in detail)	2 H	S									
SHERLOCK											
MAC – Medewerker account	12	14									
MOP – Medewerker opsporingsinformatie	12	13									
OMD – Opsporingsmedewerker	12	15									
TAC – teamleider account	12	14									
TOP – teamleider opsporing	12	14									

Code	*Bevoegdheid*
1	Muteren alle zaken, uit deze fase, die in beheer zijn bij kantoren uit het autorisatiegebied.
2	Raadplegen in detail van alle zaken, uit deze fase, die in beheer zijn bij kantoren uit het autorisatiegebied.
2a	Raadplegen zaken, uit deze fase, die in beheer zijn bij kantoren uit het autorisatiegebied.
3	Raadplegen alle zaken, uit deze fase, die in een voorgaande fase (m.u.v. fase voorstel) in beheer waren (bij overgang naar een volgende fase) bij een kantoor uit het autorisatiegebied.
4	Raadplegen alle zaken, uit deze fase, als de betreffende zaak lopend is in fase "SO", die bestemd zijn voor de kantoren uit het autorisatiegebied.
5	Raadplegen alleen de betreffende zaken die het ATV-traject volgen.
7	Muteren alle zaken, uit de fase fiod-ecd werkvoorraad en lopend, die in fase "SO" in beheer waren bij de kantoren uit het autorisatiegebied.
8	Raadplegen alle zaken (landelijk) in detail die via de BFC-module zijn opgevoerd.
9	Raadplegen zaken in detail die via de BFC-module zijn opgevoerd.
12	Raadplegen afgesloten zaken, m.u.v. embargo-onderzoeken
13	Raadplegen lopende zaken van alle clusters, m.u.v. embargo-onderzoeken
14	Raadplegen lopende zaken van eigen cluster, m.u.v. vertrouwelijke zaken
15	Raadplegen lopende zaken waaraan hij/zij gekoppeld is als zaakrechercheur , m.u.v. vertrouwelijke zaken
22	Beheren tabbladen PV en opsporing van zaken, waaraan hij/zij gekoppeld is als zaakrechercheur
23	Beheren nieuwe modellen, nieuwe bijlagen en nieuwe journaalmutaties van afgesloten zaken, waaraan gekoppeld is als rechercheur
24	Beheren tabbladen PV en opsporing van zakenvan clustervestiging, waaraan hij/zij gekoppeld is
25	Beheren nieuwe modellen, nieuwe bijlagen en nieuwe journaalmutaties van afgesloten zakenvan clustervestiging, waaraan hij/zij gekoppeld is
26	Beheren tabblad account van zaken in alle fasen van clustervestiging, waaraan hij/zij gekoppeld is
27	Beheren nieuwe journaalmutaties in tabblad account van afgesloten zaken van clustervestiging, waaraan hij/zij gekoppeld is
28	Raadplegen van zaken van clustervestiging, waaraan hij/zij gekoppeld is
29	Beheren van SO en TPO vergaderdata

Code	Bevoegdheid
P	Autorisatie alle FIOD-kantoren waaraan deze functionaris is gekoppeld. Deze functionaris wordt, binnen de beheermodule, gekoppeld aan een FIOD-cluster en daarmee aan alle FIOD-kantoren die gekoppeld zijn aan dit FIOD-cluster.
Q	Autorisatie alle belastingdienst/douane-kantoren waaraan deze functionaris is gekoppeld. Deze functionaris wordt, binnen de beheermodule, gekoppeld aan deze kantoren. Deze zijn weer gekoppeld aan een of meer arrondissementen. Elk arrondissement is weer aan een of meer arrondissementsclusters gekoppeld. Deze functionaris is gekoppeld aan alle belastingdienst/douane-kantoren die vallen onder betreffende arrondissementsclusters.
R	Autorisatie alle belastingdienst/douane-kantoren waaraan deze functionaris is gekoppeld. Deze functionaris wordt, binnen de beheermodule, rechtstreeks gekoppeld aan deze kantoren.
S	Autorisatie Landelijk
T	Dit functietype heeft alleen rechten op de platte database
X	Raadplegen in Gefis landelijk. (eigen CT alle tabbladen raadpleegbaar)
Y	Raadplegen Gefis landelijk (beperkte info)
Z	Raadplegen in Gefis landelijk. (slechts eigen CT alle tabbladen in detail raadpleegbaar)

Code	Fase onderzoek
A	ATV-voorstel
B	SO
C	TPO
D	BD-kantoor
E	FIOD-voorstel
F	FIOD-werkvoorraad en lopend
G	OPS-voorstel
H	CA
I	OM
J	Terugverwezen
K	Transactie douane

Bijlage 3 Relevante wetgeving

Art. 3 Wet BOD-en
Hoofdstuk II. Taken en bevoegdheden
Artikel 3
Een bijzondere opsporingsdienst is onder gezag van de officier van justitie belast met:
a. de strafrechtelijke handhaving van de rechtsorde op de beleidsterreinen waarvoor Onze betrokken minister verantwoordelijkheid draagt;
b. de strafrechtelijke handhaving van de rechtsorde op een beleidsterrein waarvoor een andere minister dan de onder a. bedoelde, verantwoordelijkheid draagt en die door die minister in overeenstemming met Onze betrokken minister en Onze minister van Justitie aan die bijzondere opsporingsdienst is opgedragen;
c. opsporingshandelingen in verband met strafbare feiten die zijn geconstateerd in het kader van de taakuitoefening bedoeld onder a. en b., en die met die taakuitoefening verband houden;
d. de opsporing van andere strafbare feiten, indien de bijzondere opsporingsdienst daarmee is belast door de officier van justitie.

Artikel 15 WPG
Artikel 15 lid 2 (ter beschikking stellen van politiegegevens)
2. In bijzondere gevallen kan, indien dit noodzakelijk is voor een goede uitvoering van de politietaak, de terbeschikkingstelling van politiegegevens door de verantwoordelijke worden geweigerd dan wel kan de verantwoordelijke beperkende voorwaarden stellen aan de verdere verwerking. Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld over de gronden waarop de terbeschikkingstelling kan worden geweigerd en over de beperkende voorwaarden die kunnen worden gesteld.

Artikel 2:13 Besluit Politiegegevens
Artikel 2:13. Weigeringsgronden (artikel 15, tweede lid WPG)
1. Het ter beschikking stellen van politiegegevens kan alleen worden geweigerd of aan beperkende voorwaarden worden onderworpen in het geval:
   a. het gegevens betreft omtrent informanten of andere personen als bedoeld in artikel 12, vijfde lid van de wet;
   b. gevaar voor leven of gezondheid van betrokkene of derden is te duchten;
   c. van een verwerking voor een intern integriteitonderzoek onder verantwoordelijkheid van de korpsbeheerder;
   d. van een verwerking door de rijksrecherche onder verantwoordelijkheid van het College van procureurs-generaal;
   e. het gegevens betreft die worden verwerkt op grond van artikel 10, eerste lid, onderdeel b van de wet;
   f. van een verwerking voor een door het College van procureurs-generaal als embargo-onderzoek aangemerkt onderzoek met een zeer groot belang van afscherming vanwege afbreukrisico's, levensbedreigende risico's, politieke gevoeligheid of publiciteitsgevoeligheid van het onderzoek.

Besluit politiegegevens bijzondere opsporingsdiensten.
Artikel 2. Van overeenkomstige toepassing verklaring
1. Onverminderd artikel 46, eerste lid, van de wet (*JvU: de WPG*) is het bij die wet bepaalde met betrekking tot de verwerking van politiegegevens van overeenkomstige toepassing op de verwerking van persoonsgegevens door de bijzondere opsporingsdiensten, met uitzondering van artikel 10, eerste lid, de onderdelen b en c, derde lid en vierde lid, artikel 16, eerste lid, onderdeel d, en de artikelen 37 tot en met 45.
2. Onverminderd artikel 46, eerste lid, van de wet is het in het Besluit politiegegevens bepaalde met betrekking tot de verwerking van politiegegevens van overeenkomstige toepassing op de verwerking van persoonsgegevens door de bijzondere opsporingsdiensten, met uitzondering van de artikelen 2:4, 2:5, tweede lid, 2:7, 2:13, tweede lid, 3:2, 4:1, eerste lid, onderdeel b, en tweede lid, 4:2, eerste lid, de onderdelen a, c, d, e, f, i, j, k, o en q, en 6:6 van het Besluit politiegegevens.

Memo

Overleg [redacted] ivm voorstel pilot trendwatching

MT12-060

Aan [redacted]

Van [redacted] en [redacted]

Datum 03 mei 2012

Kenmerk

Kopieën aan

Intro.
Maandag 2 april hebben wij een overleg gehad met [redacted], [redacted] van trendonderzoeksbureau Science of the time. Dit naar aanleiding van het voorstel Trendwatching (coolhunting) als onderdeel van de informatiehuishouding bij de FIOD. Dit overleg stond in het teken om een scherper beeld te schetsen van het voorstel Trendwatching. De volgende onderwerpen kwamen aan bod: de pilot, veiligheid, kosten project, en kennis en technologie binnen de FIOD.

Aanleiding.
De wereld om ons heen is aan snelle verandering onderhevig. En dat geldt zeker voor de financiële branche. Voortdurende verandering vraagt om voortdurend vernieuwen. Alleen op die manier moet je continu inspelen op de wensen van onze relevante partners. In onze zoektocht naar het vroegtijdig onderkennen van fraude bedreigingen hebben we ons verdiept in de methodieken van het trendwatchen. Deze methodieken worden al jaren met succes toegepast binnen het bedrijfsleven en daar hebben wij aansluiting gezocht. Een cursus trendwatching, strategie, conceptontwikkeling en scenario verkenning hebben ons zeer enthousiast gemaakt. Wij zijn ervan overtuigd dat trendwatching een belangrijke bijdrage kan leveren aan het informatieproces binnen de FIOD. We staan met trendwatching aan de vooravond om op een innovatieve manier “vooruit te rechercheren” .

Trendwatching.
Trendwatchen en toekomstverkenning kennen veel gezichten, van abstracte tot concrete processen. Professioneel trendwatchen heeft een plaats verworven binnen het bedrijfsleven, kent inmiddels een volwaardige HBO studierichting en is wel degelijk te verifiëren. Onbewust ontwikkelen organisaties zich in een richting terwijl de omgeving een totaal andere richting op gaat. Trends maken je bewust van die andere bewegingen en prikkelen je om te komen tot strategie en beleid. Het signaleren van trends houden je organisatie scherp, brengt het innovatieproces op gang, zet mensen aan het denken en brengt veranderingen tot stand. Trendwatching zorgt ervoor dat je als organisatie een basishouding aanleert om bedreigingen om te vormen tot kansen.
Trends “verplichten” je tot handelen op basis van de uitkomsten, zijn over het algemeen inspirerend voor het genereren van ideeën. Trendwatching en innovatie in het bijzonder moeten verankerd worden binnen de FIOD en een vast agendapunt worden binnen het MT.

Professioneel trendwatching binnen de informatiehuishouding is nieuw en het hele proces bestaat naast trendwatchen uit trend interpretatie en trendanalyse, er uit deze trends te vertalen naar scenario's en concepten, waarop beleid en strategie kan worden ontwikkeld. De uitdaging is de “bedreigingen” om te zetten naar kansen voor je organisatie. Om dit te verankeren binnen de organisatie wordt dit bij andere organisaties ondergebracht bij een innovatiemanager die doorlopend bezig is met nieuwe ontwikkelingen en trends en dit te vertalen naar kansen binnen een organisatie. SOI kan binnen de FIOD hieraan een belangrijke bijdrage leveren.

FIOD belang
Trendwatching stelt de FIOD in staat in een vroegtijdig stadium signalen te detecteren die een bijdrage leveren aan het versterken van de informatiepositie aan de voorzijde van de opsporing. Hierdoor kunnen nieuwe vormen (trends) van bijv. witwassen en het vaststellen van vermogensbestanddelen (afpakken) sneller worden onderkend. Je kun deze trends gebruiken om de toekomst van je organisatie vorm te geven, een visie en strategie te bepalen die overeenkomt met de missie en ambitie van je organisatie. Trendwatching kan een belangrijke bijdrage leveren aan de intelligence agenda van de FIOD. Trendwatchen d.m.v. coolhunters lijkt voor alsnog de meest geschikte vorm van trendwatching voor de FIOD.

Innovatief.
Trendwatching als onderdeel van de informatiehuishouding binnen de FIOD is innovatief en vernieuwend binnen zowel de opsporing als de trendwatch business zelf. Er gaat een enorme PR vanuit en er is zelfs voor de start van de pilot al veel belangstelling vanuit de Douane, Kmar, het FP, de politie en de (financiële) opsporingswereld. Door het TIOC van het FP is gevraagd om een presentatie te verzorgen over trendwatching.

Pilot trendwatching.
Bij de pilot is het van belang gebruik te maken van de kennis en kunde van een professional die zijn sporen heeft verdiend in het bedrijfsleven zoals bijv. [redacted].
De FIOD zal bij de pilot in the lead zijn en de betrokkenheid van [redacted] is éénmalig en zal zich beperken tot de pilot. In een later stadium kan hij als adviseur worden geraadpleegd. Zijn deskundige inbreng is cruciaal voor het slagen van de pilot omdat trendwatching professioneel moet worden ingericht op een methodologisch en academisch verantwoorde wijze. Hier staat [redacted] voor garant. Na de pilot moet de FIOD in staat zijn een volgend traject zelfstandig te kunnen inzetten. Het is daarom van belang zowel mensen van SOI als de CIE in te zetten bij de pilot en de continuïteit te borgen. Ook bij de voorbereiding is de samenwerking tussen SOI en de CIE goed en draagt bij tot het succes van de pilot.

Veiligheid.
Het trendwatchen is in beginsel gericht op het binnen halen van toekomstige fraude bedreigingen en is gebaseerd op (gevalideerde) signalen waarna de CIE en SOI dit nader gaan valideren/toetsen op subjectniveau. Hierdoor is er van privacygevoelig informatie nauwelijks sprake in de trendwatch fase.

[redacted] zelf werkt met multinationals waarvan de vertrouwelijke bedrijfsinformatie afgeschermd moet worden en dit heeft in de praktijk nog nooit tot problemen geleid. De afgeschermde coolhunt-omgeving is veilig omdat alles draait op één up to date server met goede firewall en virusscanner, de omgeving is niet via de index traceerbaar via google (afgeschermd)en de omgeving heeft ingebouwde spamprotectielaag. Gebruikers worden d.m.v. een lijst ingevoerd en gecontroleerd en krijgen een pascode (zoals internet bankieren) zodat oneigenlijke gebruikers geen toegang kunnen krijgen. Na de coolhunt pilot worden alle gegevens ter beschikking gesteld.

Voor het inrichting van een veilige upload omgeving is, na overleg met [redacted], contact gelegd met het Forensisch IT team (FITT) in Haarlem. Dit om de (technische) mogelijkheden te bekijken voor- en tijdens de pilot zodat na de pilot de continuïteit van de lopende cool hunt en de op te starten nieuwe cool hunt zijn gewaarborgd. Een actieve bijdrage van de FITT tijdens de pilot is zeer gewenst.

Kennis en technologie.
De fraude cool hunt wijkt in enkele opzichten af van een algemene cool hunt. Hierdoor zijn o.a. diepte interviews noodzakelijk. Dit om experts en anderen relevante partijen op hun kennis te kunnen inzetten, om draagvlak te creëren en de bereidheid te vergroten tot het leveren van parttime coolhunters. [redacted] voert hierbij een nadrukkelijke rol tijdens de pilot. Hierdoor wordt de methodologische en academische diepgang binnen de pilot gewaarborgd. De acquisiteurs van de CIE en medewerkers SOI worden nauw betrokken en integreren binnen de pilot waardoor de kennis wordt overgedragen t.b.v. vervolg trajecten. De acquisiteurs en medewerkers van SOI zullen tijdens de hele pilot een belangrijke bijdrage leveren binnen de pilot waardoor de kennis binnen de FIOD is geborgd. Hierdoor kan na de pilot indien er een eigen coolhuntomgeving is gebouwd binnen de FIOD in toenemende mate zelf worden doorgestart met trendwatching wellicht met enig advies van [redacted] of diens medewerkers. Er is een misvatting ontstaan dat wij coolhunters gaan betalen. Dit is niet het geval. We moeten wel iets teruggeven. Te denken valt

aan informatie deling, het creëren van een win- win situatie, landelijke coolhuntersdag, en uitroepen beste coolhunter.

Kosten aspect pilot.
Vanwege het prestigieuze en uitdagende karakter van dit project heeft [redacted] al een scherpe offerte ingediend. In overleg is een aangepaste offerte gemaakt hetgeen een totale besparing van ruim 12.000 euro heeft opgeleverd. Hierdoor komen de kosten op ongeveer 42.000 euro.

In een korte presentatie die aan het MT zal worden gegeven zullen de methodiek, opbrengst en relevantie verder worden toegelicht.

Start pilot.
De voorbereidingen kunnen nog voor de zomervakantie aanvangen en de daadwerkelijk uitvoering van de pilot zal in het najaar 2012 kunnen plaats vinden.

03 mei 2012.

[redacted] en [redacted]
CIE FIOD

Info:

[redacted].
[redacted] is een toonaangevende persoonlijkheid binnen de trendwatch wereld met een enorme goede reputatie en een mondiale uitstraling op dit gebied. Het uitdragen van de cool fraude hunt door hem in binnen- en buitenland levert de Fiod een enorme goede PR op. Bovendien kunnen we gebruik maken van het (inter)nationale (trend)netwerk van [redacted]. [redacted] is zeer enthousiast vooral over het nieuwe domein en staat te popelen om uit de startblokken te gaan. [redacted] is werkzaam voor een groot aantal multinationals in binnen- en buitenland en geeft gastcolleges op universiteiten o.a. in China dit jaar.
(http://www.fontys.nl/lectoraten/trendwatching/cv.[redacted]htm)



7 mei - 11 mei 2012

	maandag 7	dinsdag 8	woensdag 9	donderdag 10	vrijdag 11
7 30					
8 30				iManagement -- Den Haag, Min Fin, Rembrandtzaal	
9 30	Maandagavondsessie Internati -- kamer	Tafel Account / OI A.01.08	-- FIOD Utrecht, Bernadottelaan 13-15, 3527 GA te Utrecht. --		
10 30			managementontwikkeling binnen de dienst -- Utrecht, Bernadottelaan 13-15, kamer --	Kamer voor	Agenda overleg OR B01.10
11 30	Voorbespreken CVI bu				
12 30				Bijeenkomst BZT Amersfoort	'De 3' FIOD Utrecht, B01.10
13 30		MT vergadering MT kamer			
14 30	MT Belastingdienst MinFin Den Haag vergaderzaal S 2.19.		Stuurgroep Antifraudebox -- Locatie : Utrecht, Vergadercentrum De Wereld Herman Gorterstraat 55 3511 EW Utrecht Ruimte, De Wereld Utrecht, Malediven, 3e verdiepin		Koninklijke marechaussee kamer
15 30					
16 30					
17 30					
18 30					

/FIOD/BLD 03-05-2012 12:15:13 1



7 mei - 11 mei 2012

	maandag 7	dinsdag 8	woensdag 9	donderdag 10	vrijdag 11
	niet aanwezig				(M)
7 30					
8 30	Geen afspraken	Bespreken viermaandsrapportage	Thuiswerken, geen afspraken		Keek op de week!
9 30	Themadag Forensische Accountants (incl lunch) -- A.01.08	Tafel Veiligheid -- A.01.19 --		Voortgangsgesprekken bijpraten -- Kamer --	Regiegroep SummIT Zaandam, Guishof 1
10 30				Voorbespreken regiegroep Sum	
11 30					
12 30	Ecrins toelichting -- Fp den haag			Bijeenkomst BZT teamleiders Amersfoort, Mariënhof	
13 30		MT -- MT kamer			Bespreken autorisatieprofielen ihkb informatiecoördinatie
14 30					
15 30	Stuurgroep Summ-IT (klein comité) Kamer				
16 30					
17 30		17:00 - 22:00 Geen afspraken			
18 30					

/FIOD/BLD 03-05-2012 10:55:27 1



7 mei - 11 mei 2012

	maandag 7	dinsdag 8	woensdag 9	donderdag 10	vrijdag 11
			[redacted]	[redacted]	Verlof
8 30	Week 19 [redacted] vrij	[redacted] vrij			[redacted] vrij
9 30		Klankbordgroepoverleg FIOD - LCA FIOD Utrecht, Bernadottelaan [redacted]	Vaco overleg	CT Zuidwest	
10 30					
11 30	Ter info, om 11.00u, CT overleg NW				
12 30	Ecrins FP den haag	Spraaktechnologie en sprekersherkenning			
13 30		MT vergadering MT kamer		1:1 [redacted] -- Zaal 01. 063 -- [redacted]	
14 30				1:1 [redacted] -- Zaal 01. 063 -- [redacted]	
15 30					
16 30					
17 30					
		19:00 - 20:00 Kranten -- Rktvc			

[redacted] /FIOD/BLD 03-05-2012 12:15:19 1



7 mei - 11 mei 2012

	maandag 7	dinsdag 8	woensdag 9	donderdag 10	vrijdag 11
			Deeltijd		
8 30	*Start Blog* vrij	vrij		iManagement - Het belang van ICT voor FIOD 8.30-15.00 -- MinFin, Rembrandtzaal, Den Haag	vrij
9 30	-- voortg	-- FIOD Utrecht, kamer Rei			Gesprek -- kam er --
10 30		FIOD Utrecht, kamer			Agenda overleg OR -- B01. 10 --
11 30					- voortgang
12 30					
13 30	Evalueren FIOD Utrecht, A01.21	MT MT kamer			Pasmiddag
14 30					
15 30					
16 30					
17 30					*Einde Blog*

/FIOD/BLD 03-05-2012 12:19:02 1



7 mei - 11 mei 2012

	maandag 7	dinsdag 8	woensdag 9	donderdag 10	vrijdag 11
	niet aanwezig			'52	
7 30					
8 30				Lokatiebezoek	
9 30	Bespreken gefis / -- Kamer --		Selectiegesprekken Acc/OI Eindhoven Eindhoven		
10 30	Teamleiders / Voorbereiding en selectie gesprekke	Overleg IM Kamer		Beoordelingsgesprek met	Bijpraten Almelo / Zwolle
11 30	Voortgangsgesprek -- Kamer --			Beoordelingsgesprek met	
12 30		Bijpraten Communicatie -- Kamer			
13 30	Voortgangsgesprek -- Kamer --	MT MT kamer			
14 30					
15 30			Geen afspraken	Afscheid	
16 30					
17 30					
18 30					

/FIOD/BLD 03-05-2012 10:53:17 1