

Input

Signalen
behandeling

Aangifte(uitworp)
Risicomix

Systeemsignalen

Renseignemententer

Queries
Risicomix

Berichten bel.pl.

Capaciteit

Throughput

Voor-
sorteren

'Wegen'

Archiveren

BHV nevenakt.

BHV risico

Direct behandelen

Analyse

RSP-Boekhouding

Risicoselectie

Belastingdienst

Output

+ Behandelduur

+ Behandeladvies

Behandelopdracht

Capaciteitsafstemming

Luitgifte

Behandeling

Resultaat

RBPro/RMF

**Risico-
beheersings-
organisatie**

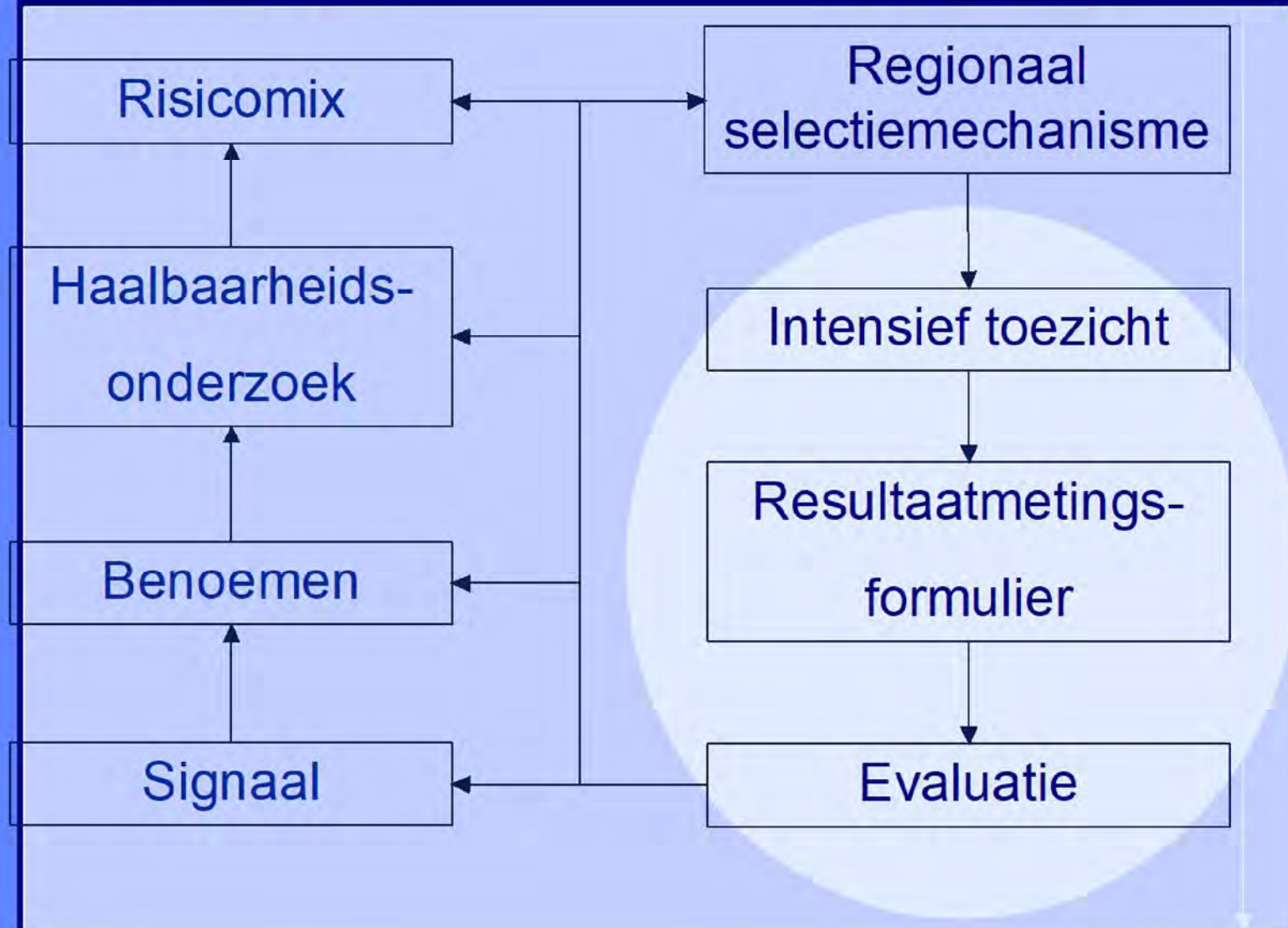


Belastingdienst

ITO-tools

Uitvoering	Ontwerp/selectie
* Risico database * RBPro-RMF * Auditfile-Clair * Controleset * ATK	* Risico database * RBPro-RMF * Risicokennisgroepen * Risicomix * RAM (Risicoanalysemodel) * Inforay * Risicoselectie

Belastingdienst



Tegenstellingen?

**Risicoselectie versus
Zelfsturing**

of

**Risicoselectie samen met
Zelfsturing**

Belastingdienst

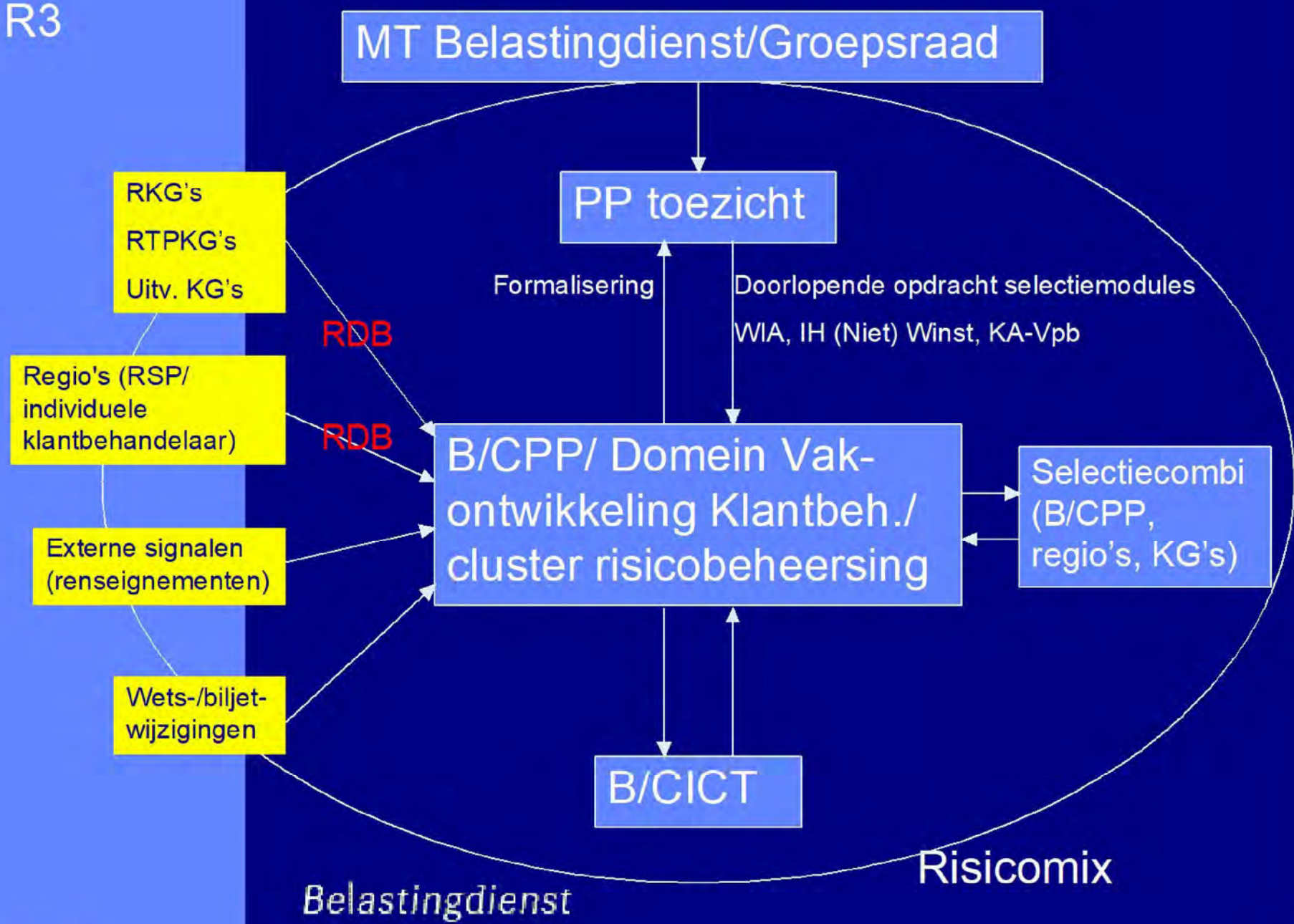
Tegenstellingen?

Procesgericht werken

Risicogericht werken

Branchegericht werken

Belastingdienst



Ontheffingsprocedure AWS+

Inleiding

Op 4 juli 2017 heeft opdracht gegeven om een fijnmazigere set van maatregelen te treffen rondom de beveiliging van de AWS+ omgevingen. De eerste maatregel in dat kader was om de AWS+ omgevingen te deactiveren. Op het moment van schrijven zijn er 23 AWS+'en uitgezet. Alle bijbehorende databases op Teradata zijn ontoegankelijk gemaakt en de SAS Visual Analytics omgeving is technisch onbereikbaar gemaakt. Tevens zijn alle bestaande autorisaties op de AWS+ omgevingen ingetrokken.

Op dit moment zijn IV-accent en B/CIE gestart met een onderzoek naar de implementatie van generieke maatregelen die ervoor zullen zorgen dat externe email, internet en file transfer mogelijkheden voor gebruikers met AWS+ autorisaties worden beperkt. Deze maatregelen zullen op een andere moment worden toegelicht.

heeft bovendien aangegeven dat daar waar problemen ontstaan ten aanzien van de continuïteit, er via de directeur van het betreffende dienstonderdeel om ontheffing kan worden gevraagd aan de Naar aanleiding daarvan is de navolgende ontheffingsprocedure opgesteld.

Randvoorwaarden

- De directeur van het dienstonderdeel zorgt dat aan onderstaande ontheffingseisen wordt voldaan;
- Er worden via deze procedure geen nieuwe AWS+'en uitgegeven;
- De scope van de ontheffingsprocedure betreft hier de AWS+ omgevingen (ICT service XBA);
- Voorafgaand aan activering van een AWS+ wordt er een pre-audit uitgevoerd door een interne onafhankelijke partij op de reeds aanwezige logbestanden;
- De autorisaties voor AWS+ gebruikers worden jaarlijks getoetst.

Ontheffingseisen

Gegevens

Data die beschikbaar gesteld wordt voldoet aan de volgende eisen:

#	Eisen	Ja / Nee / Anders	Motivatie
01.	Iedere bron die beschikbaar gesteld wordt in het Teradata platform is voorzien van een WMK-toets (doelmatigheid en doelbinding) en/of PIA.		
02.	Er is een leverovereenkomst tussen eigenaar AWS+ en eigenaar van brondata.		
03.	Er wordt geen andere data beschikbaar gesteld dan ruwe bron-data.		

Naam dienstonderdeel
IV-accent & CAP

Contactpersoon
 (IV-accent)
CAP)

Datum
6-7-2017

Versienummer
1.0

Auteurs

04.	Structurele gegevensleveringen door het AWS+ team CAP worden alleen beschikbaar gesteld op het Teradata platform.		
05.	De totale lijst met bronnen wordt beheerd bij de klantgroep en geadministreerd bij het AWS+ team CAP.		
06.	Het specifieke doel en bijbehorende opdracht waarvoor de inzet van de AWS+ gerechtvaardigd is, is beschreven.		
07.	Brondata op Teradata wordt in gepseudonimiseerde vorm ter beschikking gesteld, zodra deze functionaliteit beschikbaar is. Afwijkingen hierop dienen via een PIA te worden vastgelegd.		

Gebruikers

Gebruikers van de AWS mogen werken op de omgeving zodra voldaan is aan de volgende eisen:

#	Eisen	Ja / Nee / Anders	Motivatie
08.	Er is een getekende geheimhoudingsverklaring (eed/belofte) voor iedere gebruiker van de AWS+.		
09.	Alle gebruikers van de AWS+ hebben de cursus DigiBewust/DigiVeilig uitgevoerd.		
10.	Per klantgroep is er een lijst van AWS+ gebruikers. Deze lijst wordt geschoond wanneer de AWS+ gebruikers niet meer in dienst zijn, van dienstonderdeel wisselen of wanneer zij geen activiteiten meer uit voeren op AWS+ omgeving.		
11.	De AWS+ gebruikers hebben een basistraining gevolgd voor SAS en Teradata.		
12.	De directeur van het dienstonderdeel is verantwoordelijk voor monitoring, houding en gedrag van de AWS+ gebruikers.		

Autorisaties

De volgende eisen gelden rondom het toekennen van autorisaties:

#	Eisen	Ja / Nee / Anders	Motivatie
13.	De directeur van het betreffende dienstonderdeel geeft aan welke medewerkers (en in welke rol) er gaan werken op de AWS+ omgeving.		
14.	De autorisaties worden goedgekeurd door de leidinggevende en gevalideerd door functioneel beheer CAP. Dit geldt ook voor aanpassingen en verwijder acties.		
15.	Alle aanvragen verlopen rechtstreeks via IMS en niet direct via AAA (autorisatie beheertool).		

Technologie

De volgende eisen t.a.v. de techniek worden gesteld:

#	Eisen	Ja / Nee / Anders	Motivatie
---	-------	-------------------	-----------

16.	Benodigde lokale diskruimte op de AWS+ (niet Teradata) omgeving is niet meer dan 1 Terabyte. Dit wordt gedaan om te voorkomen dat brondata buiten Teradata wordt gepersisteerd. Geef aan indien "nee" waarom er meer diskruimte nodig is.		
17.	De lokale diskruimte mag alleen gebruikt worden voor SAS projecten, tijdelijke werkbestanden en eindresultaten.		
18.	Het gebruik van XCMD wordt sterk afgeraden i.v.m. toekomstige migratie naar SAS Grid. Geef aan indien "nee" waarom XCMD toch nodig is.		
19.	De AWS+ is bedoeld voor exploratieve data analyse en adhoc reporting en is niet ontwikkeld voor gebruik in het primair proces. Geef aan indien "nee" waarom dit toch nodig is.		
20.	De AWS+ biedt functies voor Analytics, het gebruik beperkt zich hiertoe. Er wordt geen functionaliteit buiten de AWS+ functies om gebruikt die de migratie in de toekomst zullen bemoeilijken. Geef aan indien "nee" waarom dit toch nodig is.		
21.	Het versturen van e-mails naar persoonlijke mailboxen vanaf de AWS+ is niet toegestaan. Het versturen van productie-data via e-mail is NIET toegestaan.		
22.	Zodra de technische opvolger van de AWS+ beschikbaar is, zal de klantgroep actief medewerking dienen te verlenen aan een migratie.		

Proces

De volgende eisen gelden t.a.v. het proces:

#	Eisen	Ja / Nee / Anders	Motivatie
23.	De initiële aanvraag om een AWS+ weer operationeel te maken, wordt ingediend door de directeur van het betreffende dienstonderdeel bij de Persoonsgegevens		
24.	De aanvraag wordt functioneel en technisch getoetst op de voorwaarden die in dit memo verwoord staan. Het resultaat van de toetsing, inclusief een advies, wordt teruggekoppeld richting directeur van het dienstonderdeel en Persoonsgegevens		
25.	De klantgroep levert een beveiligingsvertegenwoordiger aan die actief werkt aan de eventuele signalen die voortkomen uit de logging en monitoring.		

Opdrachtformulier D&A

Opdrachtnummer MIP016

Opdrachtnaam: Profiling Tool ANBI

1. Datum opdracht door BV	16 maart 2017
2. Kenmerk opdracht	Profiling tool ANBI
3. Prioriteit indicatie Loket BV	Hoog

Klantgegevens

4. Opdrachtgever (management Segment)	Persoonsgegevens
5. Contactpersoon Bedrijfsvoering	
5. Bereikbaar; telefoonnummer	
5. Bedrijfs onderdeel (segment/werkgebied/team)	PDB/ANBI
6. Klant (gebruiker data)	Persoonsgegevens

Opdrachtgegevens

7. Dashboard, standaard overzicht of ad hoc BI	Permanente tool (LOA)
8. Doel van de aanvraag	Het bouwen van een permanent systeem voor risicoselectie en weging bij ANBI's
9. Belang/prioriteit proces	Zeer groot belang en prioriteit. Zonder deze tool is selectie en weging van risico's niet mogelijk en ontbreekt het aan effectief toezicht op ANBI's
10. Gewenste opleverdatum product	z.s.m.
11. Aard opdracht	☐ Nieuwbouw ☒ Aanpassing ☐ Herhaalopdracht
12. Bij aanpassing of herhaling	Productnaam en kenmerk: zie bijgevoegde info bij onderdeel bijzonderheden

Specificatie klantvraag

13. Systeem(en)/bronnen	Zie info bij onderdeel bijzonderheden
14. Detailbeschrijving opdracht: de inhoud, de vorm, de selectiecriteria en de velden	De profiling tool is in zijn huidige vorm (eenmalig) gebruikt om de meest risicovolle ANBI's te selecteren en te controleren. Dit in het kader van toezicht dat er toe doet. Op dit moment worden er onderzoeken gedaan om de risico indicatoren die in de tool opgenomen zijn te valideren, aan te passen of te wijzigen. Het uiteindelijke doel is dat ook FIU-gegevens (MOT-meldingen) en risico-indicatoren die bij MKB gebruikt worden gekoppeld worden aan dit systeem. Zo willen we onze risico selectie en weging steeds verder verfijnen. Ons toezichtplan 2017 e.v. is volledig geënt op een optimaal gebruik van deze tool. Het is namelijk onmogelijk om handmatig al onze signalen te wegen en beoordelen. Het is dus de bedoeling dat de huidige vorm van de tool omgebouwd wordt naar een toekomstbestendig systeem dat doorlopend gebruikt kan worden voor selectie, weging en uitgifte signalen voor boekenonderzoeken. We zullen ANBI's continue door deze tool halen om zo actueel toezicht te houden waarvan een preventieve werking uit gaat naar het volledige ANBI-bestand.
15. Eventuele afhankelijkheden	
16. Aanlevering invoer	☐ Nee ☐ Ja:
17. Aantal records invoer	
18. Format invoer	
19. Uitvoervoorstelling	
20. Formaat uitvoer	
21. Sortering	

Eisen t.b.v. Testen22. Test vereist ☐ Nee ☒ Ja:

23. Deelnemers Test ANBI team

Uitlevering24. Frequentie uitlevering ☐ ☐ eenmalig ☒ Herhaling gewenst

25. Wijze van aanlevering data

26. Contactpersoon D&A

Bijzonderheden

27. Bijzonderheden

Gegevens aangeleverd door **(EHI)****ANBI-profiling tool!**

Stand van zaken per 14-3-2017

wie heeft de tool gebouwd?

EHI,

Belastingdienst**Expertisecentrum Handhaving & Intelligence**Herman Gorterstraat 55 | 3511 EW Utrecht
Postbus 18200 | 3511 CE Utrecht**M** @belastingdienst.nl
www.belastingdienst.nl**wie beheert de tool tot nu toe?**

Beheer vindt op dit moment niet echt plaats. De tool is in principe een eenmalig project geweest waarbij er gebruik is gemaakt van de gegevens van een 15-tal bestanden. Deze bestanden zijn in meerderheid van het RAM platform gehaald. Incidenteel is er gebruik gemaakt van bestanden uit de TeraData omgeving (3-tal). Wel is alles wat er na het verzamelen van de bestanden gebeurt tot het opleveren van een lijst met posten op volgorde van belang, geautomatiseerd. Wel is destijds, met het bouwen van deze tool, rekening gehouden met het feit dat het op een later moment met meer recentere gegevens herhaalbaar moet zijn. Dus ophalen van de bronbestanden (geautomatiseerd in RAM), de koppeling met TeraData en het aan elkaar weven van deze gegevens en er op de juiste manier naar kijken (script) is allemaal zo opgezet dat het met relatief weinig inspanning opnieuw kan plaatsvinden.

waarom stopt dat?

Niet duidelijk is of EHI nog opgesteld wordt voor dit soort werkzaamheden. Er is een informatieplatform waar het onder zou kunnen vallen en die ervoor zorgt dat de tool up to date blijft maar formeel is daar nog niets voor geregeld.

is er een beschrijving van de tool?

Door het script te volgen en doordat het is voorzien van commentaarregels kun je vrij eenvoudig volgen wat er in de diverse stadia gebeurt. De bouwer is beschikbaar om het script van een

uitgebreide beschrijving te voorzien.

aan welke bestanden is deze tool gekoppeld (waar komt de input weg)

Zoals hierboven beschreven merendeel bestaat uit RAM-bestanden en een deel TeraData. Waarbij moet worden aangetekend dat de RAM-groep op dit moment bezig is een aantal van de externe bronnen te vervangen door gegevens uit de TeraData-omgeving (hierna TD). Destijds is er voor een 3-tal bestanden al rechtstreeks geput uit de TD maar dat worden er in de toekomst alleen maar meer.

wat is de output?

Tot nu toe een bestand, in excel vorm, met daarin de raking per ANBI per risico-indicator. Hierin zit een wegingsfactor per individuele risico-indicator die in het script aangepast kan worden. Eventueel kan de output nog worden uitgebreid met de relevante gelieerde bestuurders en de familiegroep.

wat moet er wijzigen (o.a. koppeling via Teradata)?

- Een aantal RAM-opvragen zou kunnen worden vervangen door rechtstreekse opvraging in de TD-omgeving.
- Een beperkt aantal risicoprofielen zouden nog uitgewerkt kunnen worden.
- De oude profielen zouden na de evaluatie ook nog scherper gemaakt kunnen worden. E.e.a. is en blijft een continue proces.

Het grote voordeel van het vervangen van RAM-opvragen door een rechtstreekse koppeling zal zijn dat je dan kunt beschikken over een permanente tool. Dat wil zeggen bij beschikbaarheid van TeraData zou je de tool in een uurtje helemaal opnieuw kunnen laten draaien. Wel zullen er dan nog oplossingen gezocht moeten worden door een paar bronnen die wel in RAM te vinden zijn maar niet in de TD-omgeving.

ONDERSTAAND DE TOELICHTING VAN BERNARD HANSTED, HIJ IS VANAF HET BEGIN VANUIT ANBI BETROKKEN GEWEEST BIJ DE ONTWIKKELING EN HET GEBRUIK VAN DE PROFILING TOOL.

Zo'n anderhalf jaar al werkt de Belastingdienst met een aparte eenheid voor data-analyse, welke als broedkamer is bestempeld. Het is een club van wis- en natuurkundigen die in principe alle voorhanden zijnde informatie van de Belastingdienst analyseren. De info richt zich op Social Network Analysis (SAS) om "foute" instellingen / ANBI's te helpen opsporen. Door netwerkdetectie en visualisatie algoritme te combineren met grote hoeveelheden data komen verbanden in beeld. Wij gebruiken dan (toekomst) een web-based interface voor verdachte activiteiten en verdachte ANBI aanmeldingen.

De ANBI wil in de pilot met de Fiod in de eerste stap het navolgende realiseren; ontwikkelen van methodiek/werkwijze om risico's van misbruik ANBI's (op effectieve en efficiënte wijze) te beperken. Middels risico classificering van de ANBI's te komen tot de posten met het hoogste risico die vervolgens verder in behandeling zullen worden genomen.

Risico- analyse

Afpellen middels risicoanalyse bestaande uit de volgende fasen:

1. Benoemen en uitwerken van alle te bedenken concrete risico's. Een risico is (bijna) altijd gelinkt aan een handhavingstekort dat zich vertaalt in een te (lage belastingafdracht (IB, OB, VPB, Successierecht, etc) dan wel een commuun delict (witwassen, verduistering, oplichting).
2. Benoemen en uitwerken van indicatoren ten aanzien van voornoemde risico's.

3. Risico's en indicatoren in kruistabel verwerken. Vervolgens risico's waarderen en bepalen meest relevante en realistische indicatoren.
4. Benoemen van bronnen waaruit informatie t.b.v. indicatoren wordt verkregen (internet, Kvk, kadaster, loonbelasting gegevens, etc.).
Bepalen waar, hoe en met behulp van welke systemen deze informatie kan worden binnengehaald (ICOV, RAM, Internet Service Center, Dienst Justis, FEC, AMLC, FIU). Hoe leggen we informatie vast! maken we deze toegankelijk.
5. Analyseren van data; indicatoren en data loslaten op ANBI's die na classificatie zijn overgebleven.
6. Geselecteerde posten uit fase 5 individueel verder opwerken aan hand van beschikbare informatie (bronnen) die nog niet zijn ingezet. Denk aan controlerapporten/IKB, internetrecherche, etc). Veelal handmatig werk maar waarbij ook gebruik gemaakt kan worden van tools.

Uiteindelijk effect

Ontwikkeling methodiek/werkwijze voor meer effectievere en efficiëntere aanpak van misbruik ANBI's. Meer inzicht in omvang en aard misbruik.

- Rechtsherstel ten aanzien van bevindingen uit 15 behandelde posten middels fiscale aanslagen dan wel het sanctioneren van misbruik middels strafrechtelijke veroordeling.
- Eventueel middels media aandacht effect vergroten.
- Signaleren tekortkomingen in de wetgeving.
- Signaleren tekortkomingen in handhavingproces/ -keten; voorstellen tot verbetering.
- Nieuwe vormen van misbruik (risico's) detecteren.

Uitgangspunt

In iedere fase wordt op basis van ervaringen en bevindingen indien nodig "teruggegrepen" naar voorafgaande fase (leercirkel).

De databasebouwers zijn Persoonsgegevens in samenwerking met FIOD en ANBI namens FIOD, ANBI-team, EHI, FIOD

Opdrachtgever

Persoonsgegevens - FIOD Account OI Zuid-Oost.
Uitvoering in overleg met FIOD SOI, Belastingdienst ANBI en LTO.
Persoonsgegevens is opdrachtgever EHI

Is er een beschrijving van de tool?

In 2015 gestart. De profilingtool ANBI, die is ontwikkeld binnen het samenwerkingsverband FIOD-ANBI team-EHI. Vanuit een fiscaal/financieel en ANBI perspectief een 'risicoranking' gemaakt van alle ANBI's en ex-ANBI's die tussen 1-1-2008 en 26-3-2015 tijdelijk of permanent de ANBI status bezaten (48.243 organisaties). De top 300 binnen deze ranking is in een samenwerkingsverband tussen FIOD, ANBI team en MKB beoordeeld en op basis van praktijk-, fenomeen- en risicokennis teruggebracht tot een top 80. Deze top 80 bevat de potentieel meest risicovol geachte posten, gezien vanuit fiscaal/financieel en ANBI perspectief. Deze 80 posten zijn integraal beoordeeld aan de hand van alle binnen de Belastingdienst voorhanden zijnde informatie(systemen) en de selectie is uiteindelijk teruggebracht tot 22 posten, waarbij de kans op onjuistheden en/of fraude en misbruik reëel aanwezig geacht wordt.

Opdrachtgever is Persoonsgegevens. Met ondersteuning van deelnemers van MT-fraude (directeuren Belastingdienst / FIOD) en daarna van de diverse M1-ers van de Belastingdienst en de FIOD en de teamleiders van het ANBI-team, EHI, MKB en de afdeling Account/OI.. Via vastleggingssjablonen zijn overzichten gemaakt uit onze risico analyse tool met daarin opgenomen de indicatoren die uiteindelijk de basis zijn geweest om risicoposten te selecteren. Verder staan daarin de bevindingen, de adviezen en de weging van de risico's en het fiscale belang in deze sjablone. Aan deze weging hebben een groot aantal personen meegedaan. Ieder vanuit zijn eigen discipline. In samenspraak met ons (FIOD Eindhoven) is per individuele post een inschatting gemaakt van de veiligheidsrisico's die eventueel een rol kunnen spelen.

Medio 2017 pilotevaluatie, hervalidatie van tooling en operationele inzet van de tooling.

Aan welke bestanden is deze tool gekoppeld (waar komt de input weg)

ICOV, RAM, Internet Service Center, Dienst Justis, FEC, AMLC, FIU en

Inspectie, controle, toezicht

Wat is de output?

Op basis van risico's , het benoemen en uitwerken van indicatoren ten aanzien van voornoemde risico's en via een verwerking en weging van deze risico's en indicatoren in kruistabel te komen tot de meest risicovolle (ANBI) posten.

Excel overzicht

Inspectie, controle, toezicht

Inspectie, controle, toezicht

Voorbeelden

Indicatoren

Inspectie, controle, toezicht

Inspectie, controle, toezicht

Risico's profiling ANBI's

Middel:	Risico's:
IB	(familie) vermogen box III in ANBI plaatsen
IB/lb	luxue goederen van ANBI dienende voor privégebruik (geen algemeen nut) (boot, woning, kunst, antiek, auto, paarden, etc.)
IB/VPB	ten onrechte giftenaftrek derden met samenspanning ANBI (fake/ niet of niet volledig betaald)
IB/VPB/OB	ten onrechte giftenaftrek geclaimd (in werkelijkheid is gift een betaling voor tegenprestatie)
IB/VPB	onroerendgoedtransactie met bestuurder of relaties tegen niet zakelijke prijzen (verkoop boven of beneden marktprijs)
IB/VPB	bestuurder of relatie is tevens dienstverlener en factureert te hoog aan ANBI
IB/VPB	bestuurder of relatie is tevens leverancier en factureert te hoog aan ANBI
IB/VPB/ SR	vermogen ANBI overhevelen naar bestuurder zelf of relatie in buitenland
IB/VPB/Strafr	bezittingen (o.g.) worden gebruikt voor criminele activiteiten
IB/VPB/Strafr	ANBI wordt gebruikt voor financiering eigen hobby
IB	voor ondersteuning politiek partij wordt hogere (valse) kwitantie voor giften uitgeschreven
IB/LB	geld lenen van ANBI tegen niet zakelijke voorwaarden door bestuurder of relatie
IB/LB	geld lenen aan ANBI tegen niet zakelijke voorwaarden door bestuurder of relatie
IB/LB	verstrekke lening wordt kwijtgescholden door ANBI (verkapte schenking)
IB/LB	privé uitgaven bestuurder via ANBI
IB/LB	privé uitgaven wn/familie bestuurder via ANBI
OB	ANBI ten onrechte onbelast/vrijgesteld voor OB
VPB	ANBI ten onrechte onbelast/vrijgesteld voor VPB
ERF BELASTING	legaten overhevelen naar gelieerde ANBI, uiteindelijk bestemd voor private belangen (ontduiking erfbelasting) "estate planning"
SCHENK BELASTING	Schenken overhevelen naar gelieerde ANBI, uiteindelijk bestemd voor private belangen (ontduiking schenkbelasting) "estate planning"
VERDUIST.	Leeg factureren van ANBI vanuit bedrijf bestuurder of aan hem gelieerde onderneming
OPLICHTING	Oplichting bij fondsen werven
WITWASSEN	Crimineel geld witwassen middels ANBI
TERRO- RISME FIN.	Via ANBI gelden werven/doorsluizen voor financiering criminele activiteiten.

Invoegen

20160127 Kruistabel risico-indicator



Aan MT MKB

Midden- en Kleinbedrijf

Contactpersoon

<voorletters> <achternaam>

Datum

6 december 2023

Kenmerk

Impuls 202308-19

Versienummer

0.9

Opdrachtgever

Persoonsgegevens

Auteur

Persoonsgegevens

Behandeld door

Persoonsgegevens

Kopie aan

Persoonsgegevens

Bijlage(n)

<invullen>

nota

Uitfaseren dataset "IVT spoor 3"

Datum 6 december 2023
Betreft Mededeling

1 Aanleiding

Met het invoeren van het analyseproces op de ADP straat is het niet meer noodzakelijk om de dataset "IVT spoor 3" nog langer in de lucht te houden. "IVT spoor 3" is een dataset met kerngegevens per entiteit en per BSN, bedoeld voor tactische en strategische analyses ter ondersteuning van het Toezicht proces binnen MKB.

In het MT van 8-2-2022 is besloten het gebruik van IVT-spoor 3 voor een beperkt aantal mensen (5) met inachtneming van mitigerende maatregelen te continueren. Er is inmiddels een alternatief werkend waarbij de AVG beter is geborgd. Bovendien kost het in de lucht houden van deze voorziening capaciteit van DF&A.

2 Mededeling

ID&S geeft opdracht aan de keten GKT alle toegang voor deze dataset IVT spoor 3 per 31-12-2023 te verwijderen.

De functionele en technische beschrijving van de dataset "IVT spoor 3" zal worden bewaard t.b.v. eventuele onderzoeksvragen.

3 Kern

Het volgende is onderzocht:

1. het huidige gebruik van de dataset "IVT Spoor 3"
2. de mogelijkheid van alternatieve bron(nen) voor het kunnen beantwoorden van de informatieverzoeken die nu m.b.v. deze dataset worden beantwoord
3. het AVG compliant zijn van deze alternatieve bron(nen)
4. eventuele aanvullende aandachtspunten.

Het gebruik van dataset "IVT Spoor 3" is beperkt tot 5 personen. Inventarisatie van het gebruik leerde dat 2 van deze 5 personen af en toe nog gebruik maken van deze dataset voor het beantwoorden van ad hoc vragen.

Er bestaat inmiddels een beter AVG geborgd alternatief, waarmee deze informatieverzoeken ook beantwoord kunnen worden. De medewerkers van de

DataDesk MKB Klantbehandeling hebben toegang tot de daarvoor benodigde data op de zogenaamde "ADP straat".

Elk informatieverzoek dat wordt ingediend bij de DataDesk MKB Klantbehandeling wordt getoetst op AVG vereisten via een Willen Mogen Kunnen (WMK) toets door ID&S.

Midden- en Kleinbedrijf

Datum

6 december 2023

Ons kenmerk

Impuls 202308-19

Aandachtspunt bij deze alternatieve werkwijze betreft de doorlooptijd. Daar waar bevragingen nu binnen enkele uren beantwoord kunnen worden zal dit via de DataDesk MKB Klantbehandeling langer duren. De huidige doorlooptijd bedraagt enkele weken tot enkele maanden. Verwacht wordt dat dit korter wordt wanneer er meer ervaring met deze werkwijze is opgedaan. Daarnaast worden er passende maatregelen genomen om het proces te optimaliseren.

4 Toelichting

Proces behandelen informatieverzoek via DataDesk MKB Klantbehandeling

Elk informatieverzoek wordt getoetst op AVG vereisten via een Willen Mogen Kunnen (WMK) toets door ID&S.

Een akkoord bevonden informatieverzoek leidt tot een verzoek tot beschikbaar stellen van de benodigde data aan het CAP Gegevensloket. Ook daar wordt het verzoek getoetst op AVG vereisten.

Na akkoord door CAP wordt de benodigde data tijdelijk (maximaal 6 maanden) beschikbaar gesteld op de ADP omgeving voor de medewerkers van de DataDesk MKB Klantbehandeling. M.b.v. deze data kan vervolgens het informatieverzoek beantwoord worden. Dit kan het volgende inhouden:

1. DataDesk medewerker verzorgt de bevraging op die data en geeft het resultaat aan de indiener van het verzoek
 2. De indiener van het verzoek krijgt tijdelijk toegang tot de ADP straat om zelf bevragingen uit te kunnen voeren
- wordt, na aanvullend akkoord door ID&S, een export gemaakt van de ADP omgeving.

Door MKB Klantbehandeling is een traject opgestart om passende maatregelen te nemen om de doorlooptijd voor het beantwoorden van een informatieverzoek te verkorten tot aanvaardbare normen (maximaal 2 weken).

5 Communicatie

De medewerkers die nu toegang tot de dataset "IVT Spoor 3" hebben worden allemaal geïnformeerd over het uit faseren en de nieuwe werkwijze via de DataDesk MKB Klantbehandeling.

6 Politiek/bestuurlijke context

Over IVT-3 is geen informatie gedeeld met P-gv. of genoemd in stukken voor de Tweede Kamer. Ook voor dit besluit is het informeren van de P-gv. niet noodzakelijk.

Informatie die niet openbaar gemaakt kan worden

n.v.t.

Memo samenwerking TRACK-Belastingdienst

20 juli 2014

Persoonsgegevens

Persoonsgegevens @belastingdienst.nl

Bijlage: Convenant Belastingdienst-TRACK origineel.pdf

Vooraf

Op 2 november 2012 is een samenwerkingsovereenkomst gesloten tussen de Belastingdienst

Persoonsgegevens

Persoonsgegevens

en de afdeling TRACK van de dienst Justis, uitvoeringsorgaan van het Ministerie van Veiligheid en Justitie. De reden voor het sluiten van deze overeenkomst was de wens om tot een zo soepel mogelijke samenwerking te komen ter uitvoering van de Wet COR (controle op rechtspersonen).

De samenwerking bestaat uit:

- informatielevering op verzoek aan TRACK
- afname risicomeldingen door de Belastingdienst en interne verspreiding hiervan

De LTO, specifiek het cluster signaalanalyse, voert momenteel de taken uit die uit de samenwerkingsovereenkomst voortvloeien.

Op 21 juli 2014 vindt een kennismakingsgesprek plaats tussen het MT van de LTO en het MT van Justis, betreffende de Justis-producten BIBOB en TRACK. Om het MT van de LTO te voorzien van achtergrondinformatie over de invulling van de samenwerking TRACK-Belastingdienst, is deze memo opgesteld. Het doel is het geven van inzicht in hoe de praktische invulling van de samenwerkingsovereenkomst er voor LTO uit ziet, enkele stappen die inmiddels in 2014 gezet zijn om tot verbeteringen te komen, en het doen van aanbevelingen voor de toekomst.

Praktische invulling

Sinds het sluiten van de samenwerkingsovereenkomst, is een groot aantal informatieverzoeken en risicomeldingen ontvangen door de LTO. In onderstaande tabel staan de aantallen vermeld zoals opgeslagen op de schijfruimte van het cluster signaalanalyse.

type	jaar			
	2012	2013	2014	Eindtotaal
IV	3	30	31	64
IV-RM		12	5	17
RM	16	81	75	172
VRM	4	31	33	68

legenda	
IV	informatieverzoek
IV-RM	Informatieverzoek + risicomelding
RM	risicomelding
VRM	verkorte risicomelding (Veelplegers)

Eindtotaal	23	155	144	322
------------	----	-----	-----	-----

De tabel laat zien dat er d.d. juli 2014 al bijna even veel risicomeldingen en informatieverzoeken zijn binnengekomen als in heel 2013. Hiermee zijn wij de belangrijkste partner van TRACK.

Als het signaleringssysteem RADAR van TRACK daartoe aanleiding geeft, vraagt de voor de desbetreffende casus verantwoordelijke analist relevante verrijkinginformatie op bij de LTO. Momenteel geschiedt de informatielevering via een sjabloon o.b.v. RAM, en waar nodig bijlages uit IKB (aangiftes, verslagen boekenonderzoeken, etc.) Die informatie, maar ook informatie van andere bestuursorganen, kan leiden tot het afgeven van een risicomelding. De LTO ontvangt de voor de Belastingdienst relevante meldingen, en stuurt ze door naar de juiste persoon binnen de Belastingdienst ter behandeling. Ook is het mogelijk om bij TRACK een risicomelding op verzoek aan te vragen, of een netwerktekening. De LTO is ook daarvoor het aanspreekpunt voor Belastingdienstmedewerkers die deze producten willen ontvangen.

Het cluster signaalanalyse heeft (nog) niet de beschikking over een informatiesysteem waarin wordt bijgehouden wat het eindeffect is van elke (verkorte) risicomelding. Daarbij speelt allereerst de vraag of die verantwoordelijkheid wel bij ons cluster ligt, als doorgeefluik, of bij de uiteindelijke ontvanger van de melding. Deze vraag valt binnen het bredere vraagstuk over nut en noodzaak van een Belastingdienst-brede signalenadministratie. Op een later tijdstip zal de LTO hierover in gesprek moeten met bijv. IM/B.

Verbeterstappen 2014

In een gezamenlijk werkoverleg op 9 januari 2014 zijn een aantal problemen in de samenwerking aangestipt. De afgelopen maanden hebben in het teken gestaan van het op gang brengen van verbeteringen op de genoemde punten.

Algemeen

Er bleek op verschillende momenten dat de analisten van beide partners niet voldoende beeld hadden van elkaars werk. Aan de kant van LTO was er onbekendheid met het doel van en het proces binnen TRACK. Aan de kant van TRACK leeft de wens om meer fiscale achtergrondinformatie.

Hierin is voorzien door op 9 april 2014 nogmaals een voorlichting te geven aan analisten van LTO over TRACK. Daarnaast is er besloten om een van onze analisten als liaison naar TRACK af te vaardigen. Deze collega is momenteel één ochtend in de week aanwezig in Den Haag om direct hulpvragen te kunnen beantwoorden, o.a. op fiscaalinhoudelijk vlak. Zijn aanwezigheid, raad en direct inzetbare kennis worden als nuttig ervaren.

Logistiek/techniek

Een van de afspraken is dat informatieverzoeken, risicomeldingen, en geleverde informatie, onderling beveiligd worden verzonden. Omdat er via e-mail gecommuniceerd wordt, maar er geen gebruik kan worden gemaakt van een beveiligingscertificaat in Lotus Notes, is besloten om gebruik te maken van versleuteling met het hulpprogramma Eclips. Ons probleem is dat onze administratief ondersteuner veel kleine handelingen moet verrichten om meegestuurde bijlages te ont- en versleutelen.

Een goede oplossing zou zijn om aangesloten te worden op de Haagse Ring, een beveiligde ict-omgeving. Indien dat mogelijk is, kunnen we onderling efficiënter bestanden uitwisselen. Die oplossing laat helaas nog op zich wachten. D.d zomer 2014 zoekt Persoonsgegevens van TRACK uit wat hierin mogelijk is. Als tussenoplossing is er besloten om een liaison af te vaardigen (*zie ook boven*). De gedachte hierachter was dat ter plekke informatieverzoeken behandeld konden worden zonder dat er e-mailverkeer aan te pas komt met te versleutelen bijlages. In praktijk fungeert de liaison als eerste afvang van vragen zodat de omvang en inhoud van schriftelijke informatieverzoeken beter kan worden afgestemd op de situatie. De liaison handelt dus geen volledige informatieverzoeken af en blijft daarmee binnen de afspraken van de samenwerkingsovereenkomst.

Vorm en inhoud

TRACK ervoer de presentatievorm van de geleverde informatie als inefficiënt. Wat er geleverd werd, was een Excel-tabel van ruim 300 kolommen met gegevens die geëxporteerd werden uit RAM. Als de vragen uit het informatieverzoek daar aanleiding toe geven, worden er ook bijlages meegestuurd uit bijv. IKB. Aan deze Excel-tabel zit het voordeel dat de gegevens naar wens kunnen worden gepresenteerd en geanalyseerd. Het nadeel is dat er niet op voorhand intuïtief in doorgeklikt kan worden.

Ons probleem was dat de omvang van informatieverzoeken, en in het bijzonder het aantal gevraagde bijlages explosief toenamen tijdens het voorjaar van 2014. Het meesturen van 30 bijlages per verzoek was geen uitzondering. Hier zitten heel veel handelingen aan verbonden voor onze analisten.

Deze problemen zijn als volgt het hoofd geboden:

- De analisten hebben zelf gekeken welke routinematige versimpelingen mogelijk zijn om zo snel mogelijk een informatieverzoek af te handelen. Dit heeft er toe geleid dat voor de meeste verzoeken **dagverwerking** mogelijk blijkt. Dit is echter wel afhankelijk van de andere taken van de analist en de complexiteit van het verzoek. Voorheen werd de leveringstermijn van 2 weken af en toe overschreden. Al met al is hier dus een grote kwaliteitsslag in bereikt.
- Samen met TRACK is gekeken of het **aantal van 300 kolommen** kon worden verkleind. Uit een analyse bleek dat de analisten van TRACK niet meer dan 116 variabelen uit RAM gebruiken. Het verkleinen van het export is door LTO uitgevoerd. Het is zelfs gelukt met collega's van Business Analytics om de genoemde 116 variabelen met één druk op de knop te exporteren i.p.v. voorheen vele malen vinkjes zetten in RAM.
- Collega's van de afdeling BIBOB binnen de dienst Justis maken voor hun informatieverzoeken aan de Belastingdienst gebruik van het **informatiesjabloon** van onze collega Persoonsgegevens. Persoonsgegevens TRACK heeft dit sjabloon gezien, vindt dit een werkbare presentatievorm en wil hier ook gebruik van gaan maken. Op het moment van schrijven is Persoonsgegevens in overleg met zijn leveranciers (B/CA) of het informatiesjabloon op inhoud aan te passen is voor TRACK. De twee varianten zijn: standaardsjabloon + enkele toevoegingen voor TRACK, vs. het gehele sjabloon slechts inrichten met afgestemde informatiebehoefte.

Tijdens gezamenlijk overleg is ook een toekomstbeeld geschetst door TRACK. Men heeft aangegeven het wenselijk te vinden om al eerder in hun proces bronnen van de Belastingdienst te kunnen

bevragen. Het doel hiervan is om informatieverzoeken en risicomeldingen, ook aan andere partijen, van betere kwaliteit te maken. Er is geopperd dat onze bronnen mee zouden kunnen worden genomen in het geautomatiseerde signaleringssysteem RADAR.

Wat onderzocht zou kunnen worden, zijn de juridische en technische mogelijkheden van een getrapte analyse in RADAR, waarbij in een eerste stap de gebruikelijke bronnen automatisch worden bevraagd (Handelsregister, Insolventieregister, strafrechtelijke documentatie, GBA). A.d.h.v. het door stap 1 zeer ingeperkt aantal rechtspersonen, kunnen in stap 2 Belastingdienst-bronnen worden geraadpleegd zonder tussenkomst van de LTO. Dit alles kan leiden tot kwalitatief betere 'triggers' die uit RADAR komen.

Ons mogelijk voordeel hierbij is dat de schriftelijke informatieverzoeken zoals ze nu worden afgehandeld, kleiner van omvang en kleiner in aantal kunnen worden. Verdere automatisering van informatieverzoeken, hetzij als onderdeel van RADAR fungeren, hetzij alleen de huidige praktische invulling aanpassen, is een punt van aandacht waar we de komende periode over in gesprek zouden moeten.

Juridisch

Op juridisch vlak spelen een aantal kwesties.

- Begin 2014 werd af en toe geuit dat het huidige convenant niet in overeenstemming zou zijn met **artikel 67 van de AWR**. Na bestudering door TRACK bleek dat artikel 2 van de wet COR voorrang heeft op de AWR. Door naleving van de huidige afspraken in het convenant, en het in acht nemen van andere juridische bepalingen, kunnen we de samenwerking voortzetten.
- Recentelijk ontstond onduidelijkheid over de vraag of onze analisten slechts op basis van een informatieverzoek, en hun waarnemingen in onze systemen om het verzoek uit te voeren, al **intern signalen mogen uitzetten** (zie artikel 5 samenwerkingsovereenkomst). Dit **nog vóórdat TRACK zelf een risicomelding maakt**. Een typische situatie is als er informatie verzocht wordt over bepaalde subjecten, en onze analisten zien dat al eerder in bijv. IKB een notitie is gezet dat het subject betrokken was bij risicovol gedrag.

Onze deskundigen formeel recht melden dat het op zich toegestaan is om zo te handelen. Het lijkt echter niet wenselijk om het te doen. Het op deze manier afgeven van een signaal, en hoe het door de ontvanger geïnterpreteerd wordt, is erg onderhevig aan subjectieve normen. Goed bedoelde notities en e-mails kunnen zo een eigen leven gaan leiden. Het advies is om liever te wachten op een meer geobjectiveerde risicomelding van TRACK en die op de gebruikelijke manier uit te zetten.

- Bij het inzetten van de **liaison** is niet beoordeeld of dit juridisch gezien is toegestaan. In het convenant is namelijk benoemd dat het informatieverzoek een standaard vorm heeft die aangepast wordt aan de onderhavige situatie. De huidige werkwijze is in overeenstemming gebracht met doel en strekking van de samenwerkingsovereenkomst. Dit is gebeurd op advies van onze deskundigen formeel recht.

- Tot slot zijn er vragen opgeworpen of het juridisch gezien mogelijk is om van een andere presentatievorm gebruik te maken dan de huidige (export uit RAM plus bijlages). Het probleem rond het informatiesjabloon van Persoonsgegevens is dat het **standaardsjabloon meer variabelen** bevat dan waar TRACK doorgaans om vraagt. Na advies van de deskundigen formeel recht blijkt dat hier bezwaren aan zitten. De extra informatie is weliswaar allemaal handig om te weten, maar informatielevering dient te geschieden vanuit het principe dat er niet om meer wordt gevraagd/meer wordt geleverd dan wat nodig is. Dit probleem kan op 4 manieren worden aangepakt
1. **Standaardsjabloon + aanpassing met wensen TRACK:** kost enige ontwikkeltijd van persoon buiten LTO, plus TRACK zal moeten objectiveren waarom er meer informatie nodig is dan tot nu toe geleverd
 2. **Sjabloon geheel aanpassen aan slechts informatiebehoefte TRACK:** geen juridisch bezwaar, kost erg veel ontwikkeltijd van persoon buiten LTO
 3. **Huidige gegevens (inhoud export RAM) presenteren in eigen viewer:** geen juridisch bezwaar, kost enige tot veel ontwikkeltijd van collega binnen LTO
 4. **Alles laten zoals het is:** TRACK kan zelf viewer maken waarin het RAM-export ingeladen wordt: geen investering door Belastingdienst nodig (behalve bijv. naderhand toelichting door liaison)

Optie 1-2 is het vriendelijkste voor TRACK, optie 3 lijkt een middenweg, optie 4 is het vriendelijkste voor ons. Wat tevens pleit voor optie 4, is het feit dat de samenwerking *‘uit moet gaan van gelijkwaardigheid, en of het reëel is om ons in allerlei bochten te wringen om de informatieverzoeker tevreden te stellen’* (opmerking formeel recht). Deze vraag is d.d. augustus 2014 ook voorgelegd aan de Persoonsgegevens van TRACK.

Aanbevelingen toekomst

Samengevat komen uit deze memo de volgende aanbevelingen naar voren:

- Wend binnen de Belastingdienst invloed aan om een centrale signalenadministratie in te richten. Het alternatief is immers het leggen van de verantwoordelijkheid voor de monitoring van risicosignalen bij de eindafnemers.
- Laat TRACK op korte termijn duidelijk maken of en hoe wij aangesloten kunnen worden op de Haagse Ring. Hiermee zijn we af van een groot aantal repeterende handelingen met de huidige vorm van beveiligde communicatie.
- Onderzoek samen met TRACK de juridische en technische mogelijkheden voor verdere automatisering van de informatieverzoeken en directe inzage in Belastingdienst-systemen.
- Kom tot overeenstemming (met TRACK en intern) welk van de vier geschetste scenario's onder 'Juridisch' voor een nieuwe informatiepresentatie haalbaar is, voor beide partijen.

Internet Service Centre



*The spirit of
Partnership*

(Dutch) Internet Service Centre

Presentatie van mijzelf



Presentatie van mijzelf

Persoonsgegevens



Mijn werkzaamheden



Mijn werkzaamheden

- Tactisch advisering;
- Internet research & development;
- Contactpersoon/gesprekspartner namens belastingdienst bij andere overheden nationaal en internationaal;

-

Persoonsgegevens



Werkzaamheden ISC



Werkzaamheden ISC

- Ten dienste aan: Blauw, Douane, Toeslagen, FIOD-ECD en CKC;
- Research & development t.a.v.: monitoren internet en het duiden ervan;
- In opdracht monitoren, verzamelen, veredelen, duiden en indentificeren van internetdata; inclusief matchen met belastingdienstdata (RAM bestanden);
- Fenomeenherkenning en risicodetectie;
- Samenwerking in kennis en kunde met alle overheidsinstanties in Nederland, belastingdiensten internationaal (in het bijzonder met UK), Europese comissie (JRC);
- Kennisoverdracht aan regio's (opleidingen, syllabus e.d.)

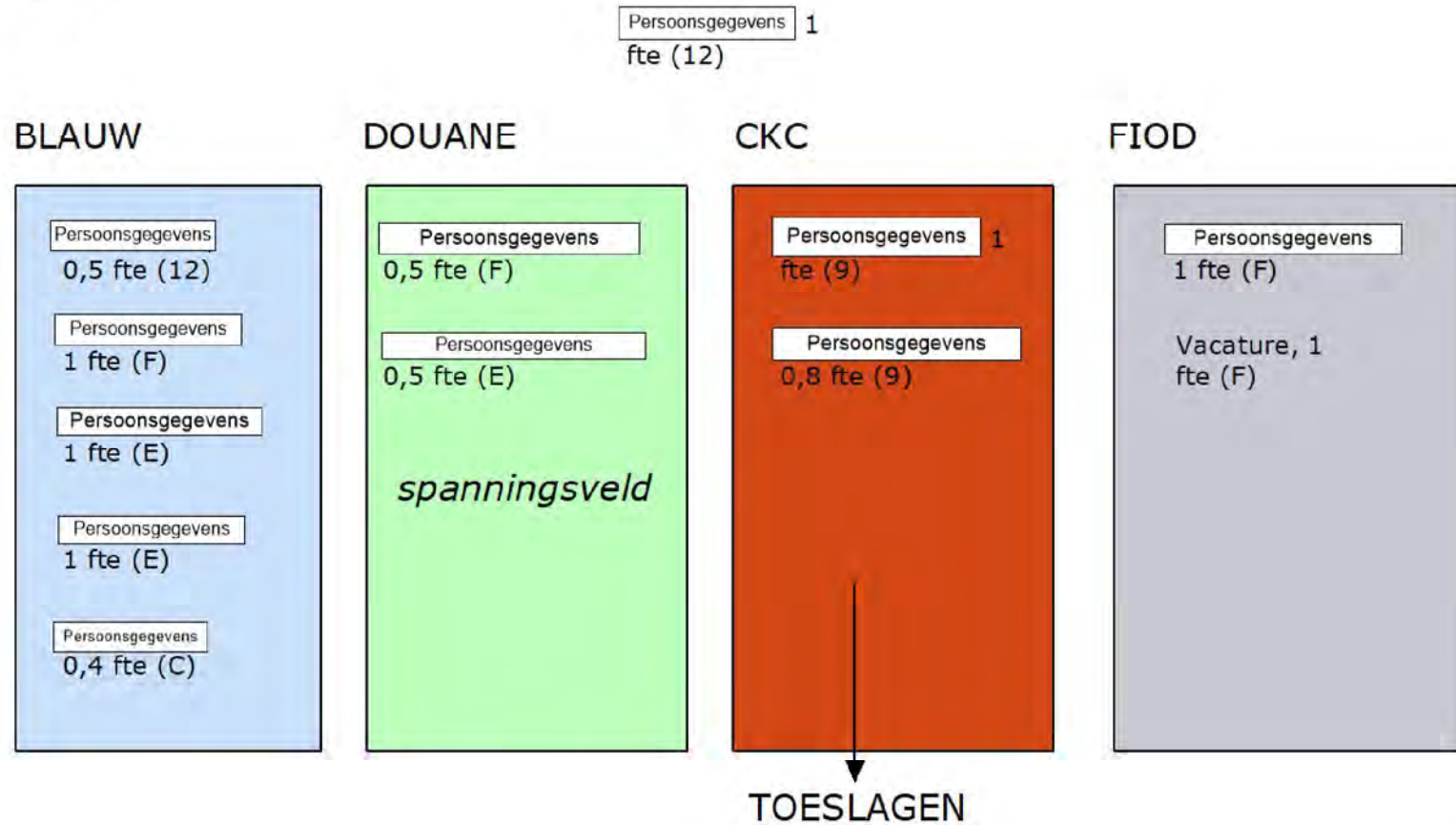


Personeelsbezetting



Personeelsbezetting ISC

9,7 FTE



Aandachtspunten/uitdagingen



Aandachtspunten/uitdagingen

- Samenwerking verstevigen met overheidspartners, rekening houdend met bezuinigingen, beperkte kennis, verschillende expertise; meewerken aan inrichting overheidsbrede technische ondersteuning (IRN) gefinancierd door BIZA/NCTB;
- Leerwerkplekken ingericht voor deze partners; dit jaar bemand door DNB, Consumenten Autoriteit en Nieuwe Voedsel en Waren Autoriteit;
- Steeds beter veredelen en identificeren met behulp van RAM-bestanden
- Uitdiepen proces fenomeenherkenning en risicodetectie;
- Opleiding internetonderzoekers regio's;
- Live Mediamonitoring en webcare ('wat' wordt 'waar' gezegd, welke impact, 'wie' actie in organisatie)



Leveringscriteria

'Intakeformulier LTO-BA (Business Analysis)'

Algemeen

De leveringscriteria zijn van toepassing op de levering(en) van elektronische data door het cluster Business Analysis van de Landelijke Toezicht Organisatie (LTO-BA) en de leveringen door de intelligence afdelingen van de kantoren Belastingdienst. De verzoekende partij gaat akkoord met deze criteria door het verwerken van de gevraagde elektronische data.

Met betrekking tot deze criteria zijn de gehanteerde kernbegrippen als volgt gedefinieerd:

- *Wbp*: Wet bescherming persoonsgegevens.
- *Elektronische data*: gegevens die op elektronische wijze zijn vastgelegd.
- *Verwerken*: alle handelingen die betrekking hebben op de elektronische data zoals onder andere het opvragen, ontvangen, bekijken, bewerken, (tijdelijk) kopiëren, bewaren, ter beschikking stelling, samenbrengen, ordenen, met elkaar in verband brengen, afschermen, vernietigen, doorleveren, uitwissen of verspreiden.
- *Verzoekende partij*: de indiener van het verzoek tot levering van data en informatie.
- *Ontvangende partij*: de ontvanger van de elektronische gegevens, die onder verantwoordelijkheid van bijbehorende organisatie werkzaam is en uit hoofde van zijn functie de elektronische data ontvangt.
- *Schade*: directe en indirecte schade van welke aard dan ook, onder meer, maar niet beperkt tot het verliezen van data, computervirussen of ander (economisch) nadeel.
- *Leveringsverzoek*: via het intakeformulier, waarin verzoekende partij expliciet onder meer kenbaar maakt met welk doel en door wie de elektronische gegevens worden verzocht; of via andere wijze kenbaar gemaakte verzoeken.
- *Convenant*: overeenkomst tussen overheden of overheidslichamen om op een bepaald terrein met een vastgesteld gezamenlijk doel op te treden.

1. Het verzoek tot levering van elektronische data geschiedt middels een leveringsverzoek.
2. De elektronische data die zijn/worden geleverd zijn eigendom van de Belastingdienst / Landelijke Toezicht Organisatie cluster Business Analysis (LTO-BA). De ter beschikking stelling van deze elektronische data is uitsluitend bestemd voor het doel dat door de verzoekende partij in het leveringsverzoek is omschreven.
3. Na ontvangst van de elektronisch data is de ontvangende partij verantwoordelijk voor verwerkingen conform de Wbp.
4. Conform de Wbp dient de geleverde elektronische data na het bereiken van het doel met inachtneming van bewaartermijnen en/of na beëindiging van het project onomkeerbaar vernietigd te worden door de ontvangende partij.
5. LTO-BA is niet aansprakelijk voor schade die is (of dreigt te worden) toegebracht en voortvloeit uit of in enig opzicht in verband staat met het al dan niet verwerken van de elektronische data. De LTO-BA volgt een actief beleid ter voorkoming en bestrijding van computervirussen, maar aanvaardt desondanks, geen enkele aansprakelijkheid indien, ondanks de zorgvuldigheid, de gegevensdragers en/of bestanden, een computervirus bevatten en (enigerlei) schade veroorzaakt.
6. Door de verzoekende partij is nagegaan en vastgesteld dat het leveringsverzoek voor elektronische data gedaan wordt binnen het op dat moment geldend juridisch kader (wet- en regelgeving). Indien het een levering van elektronische data naar andere onderdelen van de Belastingdienst of derden betreft, waarbij het verwerken van deze elektronische data in het kader van externe samenwerkingsverbanden beoogd is, dan is vanaf dat moment de verzoekende en/of ontvangende partij verantwoordelijk voor de verwerking en voor de controle op virussen.

Belastingdienst – Directie Handhaving
Landelijke Toezicht Organisatie – Business Analysis
Leveringscriteria v2.0 – 1 november 2013

Persoonsgegevens

Vragen en/of opmerkingen over dit document? Neem contact op met [LTO-BA](#)

Bespreking lopende zaken.

d.d. 2-11-2017

Deelnemers: Persoonsgegevens

Tijdens de bespreking over lopende zaken, kwam ter sprake dat er door medewerkers EHI dataleveringen worden gedaan aan segmenten en kantoren. Dit betreft ook persoonsgegevens. Deze leveringen gebeuren in vele gevallen ten behoeve van lopende processen en ten behoeve van de voortgang van werkzaamheden. Hiervan wordt niets vastgelegd.

In verband met de invoering van de AVG is het dringend gewenst om deze, niet geregistreerde leveringen, in kaart te brengen. Het ligt in de bedoeling, om deze manier van werken, voor te leggen aan de Persoonsgegevens en Persoonsgegevens. Dit teneinde een juiste, AVG proof, werkwijze te creëren. Dit is niet het enige doel. Het betreft ook een onderdeel, over het in bescherming nemen van de medewerker, wiens werkzaamheden met betrekking tot het leveren van data, een andere werkwijze behoeft. Het kan namelijk ook tot stopzetting van deze leveringen leiden. Bij ongewenste voortzetting, dus door betreffende medewerker op eigen titel doorgaan met de leveringen in de toekomst, is voor eigen verantwoording en risico. Voorts kan dit mogelijk leiden tot persoonlijke disciplinaire maatregelen.

Derhalve zal een nieuwe beschrijving van de werkwijze voor het leveren van data/gegevens voor deze werkprocessen moeten worden gemaakt.

Om dit te realiseren wordt allereerst een inventarisatie gemaakt van de huidige leveringen. Wij hebben de volgende vragen voor je.

1. Lever je, (zonder dat er een (RIT) registratie heeft plaatsgevonden, data (persoonsgegevens andere gegevens) uit?

Ja, aan medewerkers van de EH(i) wordt regelmatig op verzoek bestanden veredeld, of een kleine query aangeleverd.

Ook ben ik betrokken bij doorlopende projecten waarbij data wordt aangeleverd:

- 201500380 Blauwdruk OB project is inmiddels dicht geboekt maar de data leveringen lopen nog door tot DF&A kan leveren. Er worden diverse bestanden maandelijks geleverd aan Persoonsgegevens (SOC) en Persoonsgegevens (SOC). Deze gegevens worden dan in door hun in de database Heidi verwerkt (Heidi is de basis voor de blauwdruk OB)
 - 1 Logius bestanden aan Persoonsgegevens
 - 2 OB aangifte gegevens aan Persoonsgegevens
 - 3 Extractie uit kernsofi bevattende alle BSN's en aanvullende gegevens aan Persoonsgegevens
 - 4 Belasting consulenten gegevens aan Persoonsgegevens 1 x per jaar
 - 5 Branche codes gegevens OB nummers aan Persoonsgegevens 1 x per jaar
 - 6 Zie ook de bijgevoegde documenten "Aangeleverde bestanden.docx", "Bronnen Blauwdruk OB.docx" en "Velden in bronnen blauwdruk OB.xlsx".
- 201500379 Landelijke Aanpak Adresfraude rijksoverheid project loopt in ieder geval door tot 2023.
 - 1 Er worden regelmatig queries uitgeleverd over thema onderwerpen (Voorbeelden zijn schijnverlatingen, VOW)

2. Gebeurt dit in opdracht van een verantwoordelijke opdrachtgever? Zo ja, wie is de opdrachtgever?

Medewerkers EH(i) opdrachtgever is volgens mij dan altijd de leidinggevende van de aanvrager van de EH(i) (meestal is de leidinggevende ook de aanvrager). Daarbij ga ik er van uit dat de vraag in verband met een project bij de EH(i) wordt gesteld.

201500380 Blauwdruk OB is de opdrachtgever

Persoonsgegevens

Persoonsgegevens

201500379 Landelijke Aanpak Adresfraude is de opdrachtgever

Persoonsgegevens

Persoonsgegevens

3. In het geval er geen opdrachtgever is. Waarom en aan wie lever je de data? Welke data betreft het?

Er is in mijn ogen altijd een opdrachtgever, en ik ga ervan uit dat de medewerkers van de EH(i) geen verzoeken doen die niet werk gerelateerd zijn. Meestal wordt er ook een korte bespreking gehouden van het hoe en waarom. Met mijn leidinggevende (Persoonsgegevens) is in het verleden de afspraak gemaakt dat kleine verzoeken gewoon binnen de EH(i) gedaan kunnen worden. Die hoeven dan niet in RIT geboekt te worden. Alleen als het verzoek opeens meer werk mee brengt dan gedacht laten we het alsnog via een intake inboeken. De geleverde data betreft bijna altijd RAM-data en kan afhankelijk van de aanvragers binnen de EH(i) het hele scala aan RAM-data bevatten. Voorbeeld als het Ehi CI Team Signaalanalyse & Fraude data vraagt van bepaalde BSN die ze in onderzoek hebben krijgen ze soms een volledig klantbeeld uit RAM. In een klantbeeld zit dan alle data die in RAM bekend is van die BSN's.

4. Voor welk proces worden de data/gegevens geleverd en waar worden deze voor benodigd?

De processen zijn landelijke projecten of een vooronderzoeken van de EH(i) of iets een project moet worden.

Ook zijn er Adhoc vragen vanuit de EH(i) waarbij data wordt aangeleverd die te maken hebben met het beantwoorden van 2^{de} kamer vragen.

5. Wie zijn de gebruikers?

201500380 Blauwdruk OB zijn de uiteindelijke gebruikers van de database Heidi de fraudeanalisten bij het Ehi CI Team Signaalanalyse & Fraude en de fraudeanalisten op de kantoren. 201500379 Landelijke Aanpak Adresfraude uiteindelijk gaat er alleen naar doorselectie door de ICTU, een sofinummer(s) met adres naar de gemeenten die meedoen aan het project.

6. Hoe is de levering en archivering geregeld?

Voor het project 201500380 Blauwdruk OB is er een uitwisselingssite door (Persoonsgegevens) gemaakt waar ik de data kan neerzetten. Hier kunnen alleen ik, (Persoonsgegevens) P-gv. bij. De Bestanden blijven daar bewaard.

Voor het project 201500379 Landelijke Aanpak Adresfraude leveren wij (Persoonsgegevens)

(Persoonsgegevens)

de data/queries aan

(Persoonsgegevens)

(Persoonsgegevens)

die zorgt voor de verzending naar de ICTU. Archivering zijn we nog niet helemaal uit hoe we dat gaan regelen. Daar wordt nog over gesproken.

7. Hoe is de vastlegging van de levering geregeld?

Meestal per mail voor de adhoc vragen en kleine queries. Bij de maandelijkse leveringen wordt de query kalender bijgewerkt wanneer de laatste levering is geweest.

Bij de beantwoording van de vragen, wil je dan een zo uitgebreid mogelijke beschrijving geven. Dit om een zo juist en volledig mogelijk beeld te krijgen.
Mocht je nog zaken vergeten zijn dan kan je altijd nog een suppletie nasturen.

Naar Kernsofi overzicht van alle kolommen (654 kolommen_

[Link](#)

(2 pagina's)



Kernsofi: Zicht(integra

Per sofinr kern alle belangrijke

Basis voor: kerndossier, strategische tactische totalisatie

Opvragen via RAM Beeld en presentatie via flexviewer (kolom

Naar Kern Par(ameter) uitgebreid en beperkt overzicht van alle kolommen (300 kolommen en 20 kolommen)

[Link](#)

Kern par(ameter) volledig (300 kol) en beperkt (20 kol)

Per sofinummer wordt een weging op belang gemaakt: 0,7 x

Deze wolbsommen (0 posten) worden verdeeld in 10 bela

Per sofinummer wordt per "parametergroep" een weging op "risico" ge

Deze scores worden binnen iedere belangengroep (zie hiervo

Er zijn risicoparameters op: algemeen, toezicht, proces, UitWorpBeweringe

retour via link inksboven in betreffende bestand

Kernsofi: Zicht(integraal) op het subject en groepen subjecten. Hoe?

inr kern alle belangrijke bronnen, processen in een bestand (654 kolommen)

de tactische totalisaties, materialiteitsbestanden, Fiscaal Dienstverleners (FD) aanpak, Kern par(ameter).

via fleXviewer (kolomextracties, rij extracties, fleX tabel). Via fleX_tabel meerder bestanden te combine

00 kol) en beperkt (20 kol): zicht op subject via Kwadrantindeling (9_6) op belang en risico

op belang gemaakt: $0,7 \times \text{wolbsom sofinr} + 0,3 \text{ wolbsom dosnr} + 0,3(\text{wolbsom sofnr en dosnr})/2$

worden verdeeld in 10 belangen groepen van ieder 10 %. Particulieren van P zitten in groep 0

" een weging op "risico" gemaakt: zie weging belang maar lees voor wolbsom "totaal score sofinr en dosnr)

belangengroep (zie hiervoor) verdeel in risiconiveau groepen van ieder 10% inclusief de groep 0

proces, UitWorpBeweringen, stop, marge en overige per belanggroep. Totaal scores is Kwadrantindeling (9_6)

ak, Kern par(ameter).
bestanden te combineren.

dosnr)

eling (9_6)

Volg	Veldnaam EXCEL en retour	Kernsofi: Zicht(integraal) op het subject en groepen subjecten. Hoe? Per sofinr kern alle belangrijke bronnen, processen in een bestand (654 kolommen) Basis voor: kern dossier, strategische tactische totalisaties, materialiteitsbestanden, Fiscaal Dienstverleners (FD) aanpak, Kern par(ameter). Opvragen via RAM Beeld en presentatie via fleXviewer (kolomextracties, rij extracties, fleX tabel). Via fleX_tabel meerdere bestanden te combineren.			Pagina 1 van 2
1 Algemeen	71 Brk Uniek volgnummer ipv sofinummer	141 Begindatum DB activiteit	211 Brk einddatum laatstbekende SBI-code	281 Brk Aantal ontvangen aangiften VPB	.
2 Jaar	72 Postcode huisnr letter toevoeging BVR actueel	142 Einddatum DB activiteit	212 Brk aantal SBI-codes in betreffende jaar	282 Brk Aantal niet ontvangen aangiften VPB	.
3 Sofinummer	73 Brk Postcode Huis nummer toevoeging	143 Emigratiedatum	213 Brk SBI-codes in betreffende jaar	283 Brk Aantal uit te reiken aangiften VPB vervallen	.
4 Sofinaam	74 Brk Postcode huis nummer toevoeging vestiging adres	144 Emigratiedatum	214 Status dossier OB LH VPB IH	284 Brk Aantal feitelijk ingediende aangiften VPB	.
5 Sofinummer vervallen	75 Brk Postcode huis nummer toevoeging woonadres	145 Typologie natuurlijk persoon	215 Code VPB	285 Code soort bijlet van door FD ingeleverde bijletten_Dus niet alle	.
6 Dossiernummer	76 Brk Vergelijking vestiging adres woonadres	146 Natuurlijk persoon	216 Omschrijving code VPB	286 Omschrijving soort bijlet van door FD ingeleverde bijletten_Dus niet alle	.
7 Dossienaam	77 Postcode huisnr letter toevoeging BVR actueel voor vastgoed koppeling	147 Code beroepsgroep natuurlijk persoon	217 Brk Aantal OB nummers sofinummer	287 H en VPB Ambtshalve aangifteverzuim herinnering aanmaning	.
8 Indicatie leidend sofinummer binnen dossiernummer	78 Brk Postcode huis nummer letter toevoeging vestiging adres voor	148 Omschrijving beroepsgroep natuurlijk persoon	218 Brk Aantal LH nummers sofinummer	288 Brk Aantal ambtshalve opgelegde aanslagen IH binnen 1 jaar	.
9 Indicatie dossiernummer actief in jaar	79 Brk Postcode huis nummer letter toevoeging woonadres voor c	149 Segment dossier en sofinummer branche code	219 Aandeelhouders aantal per rechtsvorm taxhaven ja nee	289 Brk Aantal ambtshalve opgelegde aanslagen VPB binnen 1 jaar	.
10 Historisch dossiernummer behorend bij sofinummer ultimo jaar	80 Woon- en adresgegevens ultimo jaar uit BVR historie	150 Segment nummer	220 Brk Aantal aandeelhouders gevestigd woonachtig in taxhaven	290 Brk Aantal aangifteverzuimen VPB	.
11 Begindatum dossiernummer in betreffende jaar behorend bij so	81 Brk Postcode huisnr letter toevoeging vestiging adres uit jaar	151 Segmentnaam	221 Brk Aantal aandeelhouders rechtsvorm	291 Brk Aantal aangifteverzuimen IH	.
12 Einddatum dossiernummer in betreffende jaar behorend bij so	82 Brk Postcode huisnr letter toevoeging woonadres uit jaar	152 Begindatum economische activiteiten	222 Aandeelhoudersrelaties uit BVR	292 Datum laatste herinnering	.
13 Brk Indicatie 1=ja 0=nee of sofinummer meerdere dossiernumr	83 Brk Postcode huisnr letter toevoeging vestiging adres uit jaar	153 Einddatum economische activiteiten	223 Brk Totaal aantal directe aandeelhoudersrelaties uit BVR einde	293 Brk indicatie herinnering	.
14 Brk Aantal verschillende dossiernummers 2009-2015 behorend	84 Brk Postcode huisnr letter toevoeging woonadres uit jaar	154 Begindatum branche code sofinummer	224 Brk Totaal aantal indirecte aandeelhoudersrelaties uit BVR eind	294 Datum aanmaning aangifte IH of VPB	.
15 Brk Aantal verschillende dossiernummer in 1 jaar behorend bij	85 Brk aantal vestigingsadressen in betreffende jaar_Zie blok_WA_VP	155 Einddatum branche code sofinummer	225 Convenantgegevens	295 Brk indicatie aanmaning	.
16 Brk Splitsing tbv Oracle 1=MKB 2=VIP en 4=GO	86 Brk aantal woonadressen in betreffende jaar_Zie blok_WA_VP	156 Brk Aantal branche codes sofinummer	226 Convenant soort	296 Brk Aantal ontvangen aangiften	.
17 Brk segment sofinummer waarden GO MKB VIP SUP PAR	87 Becongegevens	157 Brk Alle branche codes sofinummer	227 Brk Indicatie of convenant fiscaal intermediair betreft	297 Brk Aantal te laat ingeleverde aangiften IH en VPB	.
18 Verzorgingsgebied	88 Beconnummer aangifte	158 Brk Verschil branche code dossier sofinummer	228 Convenant IH	298 Datum uitstel reactie klant	.
19 Regio code	89 Naam adviseur	159 Indicatie jaar geboorte/overlijden start/einde relatie oprichting/c	229 Convenant VPB	299 Datum reactie klant daadwerkelijk	.
20 Huidig kantoor nummer	90 BRK Indicatie fictief beconnummer	160 Brk Indicatie actief sofinr in dit jaar	230 Convenant OB	300 H en VPB Verzoek uitstel indiening aangifte	.
21 Huidig kantoor naam	91 Brk indicatie beconnummer in betreffende jaar	161 Brk Indicatie actief dossiernummer in dit jaar	231 Convenant LH	301 Brk laatstbekende beconnummer uitstel aangifte	.
22 Brk Kantoor nummer voormalig O kantoor	92 Brk indicatie geen beconnummer in betreffende jaar	162 Brk indicatie geboren in dit jaar	232 Convenant status	302 Brk Alle verschillende beconnummers uitstel aangifte	.
23 Brk Einddatum voormalig O-kantoor	93 Brk Laatste bekende beconnummer	163 Brk indicatie overleden in dit jaar	233 Begin jaar convenant	303 Brk aantal beconnummers met verzoek om uitstel aangifte	.
24 Brk Kantoor nummer voormalig P-kantoor	94 Brk Laatste bekende adviseur	164 Brk indicatie start relatie partner in dit jaar	234 Begindatum convenant	304 Brk indicatie beconnr betrokken bij verzoek om uitstel aangifte	.
25 Brk Einddatum voormalig P-kantoor	95 Brk Jaar laatste bekende adviseur	165 Brk indicatie einde relatie partner in dit jaar	235 Einde jaar convenant	305 Brk aantal verschillende beconnummers met verzoek om uitstel aangifte	.
26 Team nummer laatste bekende dossiernummer in BVR	96 Brk Aantal beconnummers	166 Brk indicatie oprichting in dit jaar	236 Einddatum convenant	306 Brk indicatie verschillende beconnummers met verzoek om uitstel aangifte	.
27 Teamnaam laatste bekende dossiernummer in BVR	97 Brk Aantal verschillende beconnummers	167 Brk indicatie opheffing in dit jaar	237 Middelen waarop convenant betrekking heeft	307 H en VPB aanvullingen (rubriek) aangifte	.
28 KvK nummer volgens BVR	98 Code softwarepakket aangifte IH of VpB	168 Woon- en vestigingsadresgegevens BVR actueel	238 Beconnummer betrokken bij convenant	308 Brk Alle beconnummers aanvullingen op aangifte	.
29 Doel groep nummer	99 Brk Aantal x wel beconuitstel maar geen becon aangifte	169 Vestigings adres	239 Sofinummer becon betrokken bij convenant	309 Brk Totaal aantal aanvullingen op aangifte	.
30 Doelgroepnaam	100 Brk Aantal x geen beconuitstel maar wel becon aangifte	170 Huis nummer vestigings adres	240 Brk indicatie convenant branche	310 Brk indicatie aanvulling op aangifte	.
31 Branche code dossiernummer	101 Brk Aantal x beconuitstel is becon aangifte	171 Huis letter vestiging adres	241 Brk Indicatie convenant fiscale intermediairs	311 Brk aantal verschillende beconnr met aanvullingen op aangifte	.
32 Brancheomschrijving dossiernummer	102 Brk Aantal x beconuitstel is niet becon aangifte	172 Huis nummer toevoeging vestigings adres	242 Brk indicatie convenant franchisenemers	312 Brk indicatie aantal verschillende beconnr met aanvullingen op aangifte	.
33 Branche code sofinummer	103 Indeling EHI	173 Huis nummer aanduiding vestigings adres	243 FSV Fraude Signalen Voorziening signaleringen	313 Brk Alle beconnummers aanvullingen rubriek aangifte	.
34 Brancheomschrijving sofinummer	104 Brk Team indeling actueel MKB EHI	174 Postcode vestigings adres	244 Brk Aantal signaleringen FSV	314 Brk Totaal aantal aanvullingen rubriek aangifte	.
35 Rechtsvorm code	105 Brk Team KO gesplitst in ARD HTR VGL binnen MKB EHI	175 Woonplaats vestigings adres	245 AKI Aangifte Klantbehandeling Informatie	315 Brk indicatie aanvulling rubriek aangifte	.
36 Rechtsvorm omschrijving	106 Brk Indicatie KO nadere verbijzondering MKB EHI	176 Brk Indicatie of vestigingadres binnenlands adres is	246 Brk Aantal rakingen in AKI incl fraude in jaar	316 Brk aantal verschillende beconnr met aanvullingen rubriek aangifte	.
37 Rechtsvorm groep	107 Brk Weging in 5 categorieën binnen MKB EHI	177 Brk Indicatie of vestigingadres buitenlandse adres is	247 Brk Aantal rakingen in AKI met fraude in jaar	317 Brk indicatie aantal verschillende beconnr met aanvullingen rubriek aangifte	.
38 Rechtsvorm land	108 Leeftijdsgroepen natuurlijke personen	178 Woonadres	248 GERS	318 H en VPB voorvastgestelde gegevens	.
39 VIP indicatie	109 Brk jonger dan 18 jaar	179 Huis nummer woonadres	249 Brk Aantal voorkomens in GEFIS alle jaren	319 Middel wvg	.
40 Algemeen extra	110 Brk 18 jaar of ouder maar jonger dan 24	180 Huis letter woonadres	250 GOSIP adressen EVAT Electronisch Verkeer Aangiften 1	320 Ontvangstdatum aangifte inkomstenbelasting	.
41 Begindatum kantoor	111 Brk 24 jaar of ouder maar jonger dan 65	181 Huis nummer toevoeging woonadres	251 Brk Aantal keren in jaar ingelogd in systeem Belastingdienst	321 Ontvangstdatum aangifte vennootschapsbelasting	.
42 Einddatum kantoor	112 Brk 65 jaar of ouder	182 Huis nummer aanduiding woonadres	252 H Categorieën uitworpenden	322 Inkomens box 1 vvg	.
43 Dossiernummer fictief	113 Begin einde entiteit en middelgegevens oprichtings overlijdens	183 Postcode woonadres	253 Brk Aantal IH gedetecteerde risico_s in jaar	323 Inkomens box 2 vvg	.
44 Particulier of Onderneming	114 Begindatum sofinummer	184 Woonplaats woonadres	254 Brk Aantal IH harde correctie in jaar	324 Inkomens box 3 vvg	.
45 Rechtspersoon ja nee	115 Einddatum sofinummer	185 Brk Indicatie of woonadres binnenlands adres is	255 Brk Aantal IH inconsistentie in aangifte in jaar	325 Verzamelinkomen vvg	.
46 Handelsnaam	116 Begindatum dossiernummer	186 Brk Indicatie of woonadres buitenlandse adres is	256 Brk IH aantal indeling GO MKB PART in jaar	326 Belastbare winst vvg	.
47 Geboortedatum	117 Einddatum dossiernummer	187 Brk Totaal aantal verschillende adressen woonadressen in BVR	257 Brk IH afgeven beschikking in jaar	327 Zelfstandigen aftrek vvg	.
48 Overlijdensdatum	118 Brk Starter OB laatste 4 jaar (incl lopend jaar)	188 Brk Totaal aantal verschillende adressen vestiging persoonsad	258 VPB Categorieën uitworpenden	328 Belastbaar bedrag VPB vvg	.
49 Brk Winstgenieter indicatie	119 Brk Staking OB laatste 4 jaar (incl lopend jaar)	189 Brk Totaal aantal verschillende adressen vestiging activiteitsad	259 Brk Aantal VPB gedetecteerde risico_s in jaar	329 Totaal vrijgestelde winstbestanddelen vvg	.
50 Brk indicatie ondernemer	120 Brk Starter LH laatste 4 jaar (incl lopend jaar)	190 KvK nummers behorende bij een sofinr volgens Handelsregister	260 Brk Aantal VPB harde correctie in jaar	330 Saldo investeringsregelingen vvg	.
51 Brk indicatie particulier	121 Brk Staking LH laatste 4 jaar (incl lopend jaar)	191 Brk KvK-nummers in betreffende jaar	261 Brk Aantal VPB inconsistentie in aangifte in jaar	331 Saldo wijziging reserves vvg	.
52 Nummer gemeentelijke basis administratie	122 Begindatum VPB	192 Brk Aantal KvK nummers in betreffende jaar	262 Brk VPB aantal indeling GO MKB PART in jaar	332 Totaalloon tegenwoordige arbeid vvg	.
53 Code soort veldtoets en jaar	123 Brk Starter VPB laatste 4 jaar (incl lopend jaar)	193 Brk Begindatum allereerste KvK nummer	263 Brk VPB afgeven beschikking in jaar	333 Totaalloon vroegere arbeid wvg	.
54 IKB WOLB som en aandachtscategorieën op dossiernummer	124 Einddatum VPB	194 Brk Einddatum allerlaatste KvK nummer	264 GBV Genereke Bezwaarschriften Voorziening	334 Bruto resultaat overige werkzaamheden wvg	.
55 IKB aandachts categorie	125 Brk Staking VPB laatste 4 jaar (incl lopend jaar)	195 Brk indicatie deponering in betreffende jaar	265 Brk Aantal bezwaarschriften in jaar	335 Winst uit onderneming wvg	.
56 IKB wolbsom	126 Begindatum IH	196 Vestigingsgegevens KvK nummers behorende bij een sofinr vol	266 Brk Aantal gehandhaafde bezwaarschriften in jaar	336 Bedrag MKB vrijstelling wvg	.
57 IKB wolbsom categorie	127 Brk Starter IH laatste 4 jaar (incl lopend jaar)	197 Brk aantal vestigingen KvK-nummers	267 Brk Aantal toegewezen (geheel/ged) bezwaarschriften in jaar	337 H en VPB voorvastgestelde gegevens woning	.
58 IKB wolbsom sub	128 Einddatum IH	198 Brk aantal hoofdvestigingen KvK-nummers	268 Brk Aantal overige behandelingen bezwaarschriften in jaar	338 Totaal eigenwoningforfait vvg	.
59 IKB risicoklasse	129 Brk Staking IH laatste 4 jaar (incl lopend jaar)	199 Brk aantal commerciële vestigingen KvK-nummers	269 Brk Aantal overige verzoeken in jaar	339 WOZ waarde eigen woning hoofdverblif vvg	.
60 Zwaarte categorie	130 Partner gegevens geslacht nationaliteit immigratie en emigrat	200 Brk aantal niet commerciële vestigingen KvK-nummers	270 Brk Aantal toegewezen (geheel/ged) overige verzoeken in jaar	340 EW rente schulden kosten geldlening vvg	.
61 Dossiernummer volgens IKB	131 Geslacht	201 Bestuurders en functies volgens Handelsregister	271 Brk Aantal overige behandelingen overige verzoeken in jaar	341 Totaal eigenwoningschuld vvg	.
62 WOLB-som RAM op sofinummerwv en RAM aandachtscateg	132 Sofinummer partner	202 Brk aantal bestuurders door in jaar	272 H en VPB In te dienen ingediende en niet ingediende aangifte	342 H en VPB voorvastgestelde gegevens ondernemingen	.
63 Brk RAM wolbsom sofinummer	133 Partnerrelatie	203 Brk aantal bestuurders door met KvK-nummer in jaar	273 Brk Aantal te ontvangen aangiften IH	343 Aantal ondernemingen in IH codes 0001 0002 etc max 10 vvg	.
64 Brk IH voor RAM wolbsom sofinummer	134 Begindatum partnerrelatie	204 Brk aantal bestuurders door met sofinummer in jaar	274 Brk Aantal ingeleverde aangiften IH voorvastgesteld	344 EW totaal immateriële vaste activa fisc vvg	.
65 Brk VpB voor RAM wolbsom sofinummer	135 Einddatum partnerrelatie	205 Brk aantal functies in jaar	275 Brk Aantal ontvangen aangiften IH	345 Totaal materiële vaste activa fisc vvg	.
66 Brk OB voor RAM wolbsom sofinummer	136 Code 1e nationaliteit BVR	206 Brk aantal functies als aandeelhouder in jaar	276 Brk Aantal niet ontvangen aangiften IH	346 Totaal financiële vaste activa fisc vvg	.
67 Brk LH voor RAM wolbsom sofinummer	137 Omschrijving 1e nationaliteit BVR	207 SBI-codes KvK-nummers volgens Handelsregister	277 Brk Aantal vervallen aangiften IH	347 EW totaal voorraden fisc vvg	.
68 Brk RAM Zwaartecategorie sofinummer	138 Code 2e nationaliteit BVR	208 Brk meest actuele SBI-code	278 Brk Aantal feitelijk ingediende aangiften IH	348 Totaal vorderingen fisc vvg	.
69 Anoniem werken	139 Omschrijving 2e nationaliteit BVR	209 Brk omschrijving meest actuele SBI-code	279 Brk Aantal uitgereikte aangiften VPB	349 Effecten fisc wvg	.

790	Brk Uniek volgnummer ipv dossiernummer	140	Reden begin of einde belastingplicht DB activiteit	210	Brk begindatum meest actuele SBI-code	280	Brk Aantal ingeleverde aangiften VPB voorvastgesteld	350	Totaal liquide middelen fisc vvg

416	Inkomen box 2 nav	486	Brk Waarde aangekochte vastgoedobjecten dit jaar	556	Brk Aantal verschillende werknemers FLG	626	Brondatum FSV
417	Inkomen box 3 nav	487	Brk Waarde verkochte vastgoedobjecten dit jaar	557	FLG gegevens werknemer persoonlijk op sofinummerniveau	627	Brondatum GBV
418	Verzamelinkomen nav	488	Brk Aantal aangekochte vastgoedobjecten dit jaar	558	Brk Totaalloon werknemer FLG	628	Brondatum GEFIS
419	Belastbaar bedrag VPB nav	489	Brk Aantal verkochte vastgoedobjecten dit jaar	559	Brk Loonheffing werknemer FLG	629	Brondatum GOA
420	Belastbare winst nav	490	Brk Totale waarde aangekochte vastgoedobjecten tot en met dit jaar	560	Brk Netto loon werknemer FLG	630	Brondatum GOA toeslagen

Veldnaam EXCEL en retour		Pagina 1 van 1		
Kern Par (volledig)		Kern par(ameter) volledig (300 kol) en beperkt (20 kol): (Integraal??) zicht op subject via Kwadrantindeling (9_6) op belang en risico Per sofinummer wordt een weging op belang gemaakt: 0,7 x wolbsom sofinr + 0,3 wolbsom dosnt + 0,3(wolbsom sofinr en dosnr)/2 Deze wolbsommen (O posten) worden verdeeld in 10 belangen groepen van ieder 10 %. Particulieren van P zitten in groep 0 Per sofinummer wordt per "parametergroep" een weging op "risico" gemaakt: zie weging belang maar lees voor wolbsom "totaal score sofinr en dosnr) Deze scores worden binnen iedere belangengroep (zie hiervoor) verdeeld in risiconiveau groepen van ieder 10% inclusief de groep 0 Er zijn risicoparameters op: algemeen, toezicht, proces, UitWorpBeweringen, stop, marge en overige per belanggroep. Totaal scores is Kwadrantindeling (9_6)		
1Algemeen	74Brk_TOT_Score totaal score proces risicoparameters op sofinummer	147Brk_STOP_Score geemigreerd in jaar of daarna en beroepsgroep 444	220Brk Aantal overige verzoeken in jaar	293Code 1e nationaliteit BVR
2Jaar	75Brk_TOT_Score totaal score toezicht risicoparameters op sofinummer	148Brk_STOP_Score overleden in jaar en beroepsgroep 4444 of 8888	221Brk Aantal signaleringen FSV	294Omschrijving 1e nationaliteit BVR
3Sofinummer	76Brk_TOT_Score totaal score uitworp risicoparameters op sofinummer	149UITW_score uitworpcategorie_risicoparameters	222Brk_Aantal rakingen in AKI incl fraude in jaar	295Code 2e nationaliteit BVR
4Sofinaam	77Brk_TOT_Score totaal score stop risicoparameters op sofinummer	150Brk_UITW_Score Aantal IH gedetecteerde risico_s in jaar	223Brk_Aantal rakingen in AKI met fraude in jaar	296Omschrijving 2e nationaliteit BVR
5Sofinummer vervallen	78Brk_TOT_Score totaal score overige risicoparameters op sofinummer	151Brk_UITW_Score Aantal IH harde correctie in jaar	224Brk Aantal boekenonderzoeken heffing code 50 met correctie	297Immigratiedatum
6Dossiernummer	79TOT_Totaal score risicoparameters per groep op dossiernummer	152Brk_UITW_Score Aantal IH inconsistente in aangifte in jaar	225Brk Aantal openstaande aanslagen in GOA_INL einde jaar	298Emigratiedatum
7Dossiernaam	80Brk_TOT_Score totaal score alle risicoparameters incl materieel op dossiernummer	153Brk_UITW_Score Aantal VPB gedetecteerde risico_s in jaar	226Brk Actueel openstaande bedrag GOA_INL	299Natuurlijk persoon
8Sofinummer partner	81Brk_TOT_Score totaal score alle risicoparameters excl materieel op dossiernummer	154Brk_UITW_Score Aantal VPB harde correctie in jaar	227Brk Aantal aanslagen met oninbare bedragen dit jaar	300Code beroepsgroep natuurlijk persoon
9Brk Splitsing tbv Oracle 1=MKB 2=VIP en 4=GO	82Brk_TOT_Score totaal score materialiteitsparamaters op dossiernummer	155Brk_UITW_Score Aantal VPB inconsistente in aangifte in jaar	228Brk Aantal WOZ objecten eigenaar	301Omschrijving beroepsgroep natuurlijk persoon
10Brk segment sofinummer waarden GO MKB VIP SUP PAR	83Brk_TOT_Score totaal score algemene risicoparameters op dossiernummer	156FRAUDE_score_fraude_risicoparameters	229Brk Waarde aangekochte vastgoedobjecten dit jaar	302Code VPB
11Huidig kantoor nummer	84Brk_TOT_Score totaal score proces risicoparameters op dossiernummer	157Brk_FRAUDE_score aantal signaleringen FSV	230Brk Waarde verkochte vastgoedobjecten dit jaar	303Begindatum VPB
12Huidig kantoornaam	85Brk_TOT_Score totaal score toezicht risicoparameters op dossiernummer	158Brk_FRAUDE_Score Team nummer fraude laatst bekende dosnr in B	231Brk Saldo aangekochte minus verkochte vastg_objecten in aantallen 2002	304Einddatum VPB
13Team nummer laatst bekende dossiernummer in BVR	86Brk_TOT_Score totaal score uitworp risicoparameters op dossiernummer	159MFD_score_materialiteit_FD_risicoparameters	232Brk Tot aantal voertuigen in bezit op 1 januari in jaar	305KB WOLB_som en aandachtscategorieën op dossiernummer
14Teamnaam laatst bekende dossiernummer in BVR	87Brk_TOT_Score totaal score stop risicoparameters op dossiernummer	160Brk_MFD_SCORE_mar Aantal branche codes sofinummer 6722 of 9899	233Brk Tot aantal gestolen geëxporteerd geschoopt in jaar	306KB aandachts categorie
15KWD_Kwadrant indeling_RISG_Belang en risicogroep indeling gewogen risicoparameters bijv 7_2	88Brk_TOT_Score totaal score overige risicoparameters op dossiernummer	161Brk_MFD_SCORE_mar sofinummer met boekenonderzoek behandelb	234Brk Totaal Sagitta invoer	307KB wolbsom
16Brk_KWD_BEL_RISG_Belang en risicogroep ind gewogen alle parameters incl materieel bijv 8	89RIG_score algemene risicoparameters	162Brk_MFD_Score totaal toezichtparameters FD gerelateerd aan catego	235Brk Totaal Sagitta uitvoer	308KB wolbsom categorie
17Brk_KWD_BEL_RISG_Belang en risicogroep ind gewogen alle parameters excl materieel bijv 7_2	90Brk_Alg_Score aantal verschillende dosnrs 2012-2017 behorend bij sofinr	163Brk_MFD_Score totaal procesparameters FD gerelateerd aan catego	236Brk Totaalbedrag van alle toeslagen	309KB risicoklasse
18Brk_KWD_BEL_RISG_Belang en risicogroep indeling gewogen materialiteitsparameters bijv 10_9	91Brk_Alg_Score aantal verschillende dosnrs in 1 jaar behorend bij sofinr	164VASTG_score_vastgoed_risicoparameters	237Basisgegevens materialiteit land	310Zwaarte categorie
19Brk_KWD_BEL_RISG_Belang en risicogroep indeling gewogen algemene parameters bijv 3_8	92Brk_Alg_Score indien buitenlandse rechtspersoon	165Brk_VASTG_SCORE_aantal WOZ objecten eigenaar	238Brk ROOD Totaal Aantal keren waarde 1 of 1_1 alle categorieën	311Anoniem werken
20Brk_KWD_BEL_RISG_Belang en risicogroep indeling gewogen proces parameters bijv 2_10	93Brk_Alg_Score indien ondernemer	166Brk_VASTG_Score Waarde aangekochte vastgoedobjecten dit jaar	239Brk ROOD Totaal aantal keren waarde 1 alle categorieën	312Brk Uniek volgnummer ipv dossiernummer
21Brk_KWD_BEL_RISG_Belang en risicogroep indeling gewogen toezicht parameters bijv 5_1	94Brk_Alg_Score Totaal aantal verschillende adressen vestiging aktiviteitsadressen in E	167Brk_VASTG_Score Waarde verkochte vastgoedobjecten dit jaar	240Brk ROOD Totaal aantal keren waarde 1_1 alle categorieën	313Brk Uniek volgnummer ipv sofinummer
22Brk_KWD_BEL_RISG_Belang en risicogroep indeling gewogen uitworp parameters bijv 7_8	95Brk_Alg_Score aantal rakingen in AKI incl fraude in jaar	168Categorieën uitworpredenen IH en VPB	241Brk ORANJE Aantal keren waarde 0_0100 of 0_0110 categorieën	314Adresgegevens BVR actueel
23Brk_KWD_BEL_RISG_Belang en risicogroep indeling gewogen stop parameters bijv 8_8	96Brk_Alg_Score aantal rakingen in AKI met fraude in jaar	169Brk Aantal IH gedetecteerde risico_s in jaar	242Brk ORANJE LAAG Totaal aantal keren waarde 0_0100 alle categorieën	315Brk Postcode Huis nummer toevoeging
24Brk_KWD_BEL_RISG_Belang en risicogroep indeling gewogen overige parameters bijv 9_8	97Brk_Alg_Score aantal ondernemingen in IH codes 0001_0002 etc_max 10 vvg	170Brk Aantal IH harde correctie in jaar	243Brk ORANJE HOOG Totaal aantal keren waarde 0_0110 alle categorieën	316Brk Postcode huis nummer toevoeging vestiging adres
25Ranking WOLB-sommen RAM	98Brk_Alg_Score Leeftijd jonger dan 16 in jaar en ondernemer	171Brk Aantal IH inconsistentie in aangifte in jaar	244Brk totaal aantal scores ROOD en ORANGE	317Brk Postcode huis nummer toevoeging woonadres
26Brk Ranking RAM wolbsom op sofinr Grote Ondernemingen	99Brk_Alg_Score Leeftijd ouder dan 65 in jaar en ondernemer	172Brk Aantal VPB gedetecteerde risico_s in jaar	245Brk GEEL Totaal aantal keren waarde 0_0001 alle categorieën	318Brk Vergelijking vestiging adres woonadres
27Brk Ranking RAM wolbsom op sofinr Niet Grote Ondernemingen	100Brk_Alg_Score immigrant niet EU en beroepsgroep 4444 of 8888	173Brk Aantal VPB harde correctie in jaar	246Brk GROEN Totaal aantal keren waarde 0 alle categorieën	319Brk Postcode huis nummer letter toevoeging vestiging adres voor o.a_vastgoed
28Brk Ranking RAM wolbsom op dosnr Grote Ondernemingen	101Brk_Alg_Score aantal verschillende beconns 2012-2017	174Brk Aantal VPB inconsistentie in aangifte in jaar	247Brk totaal aantal mogelijke totaalscores	320Brk Postcode huis nummer letter toevoeging woonadres voor o.a_vastgoed
29Brk Ranking RAM wolbsom op dosnr Niet Grote Ondernemingen	102Brk_Alg_Score tot aantal voertuigen in bezit begin jaar en aantal werken ultimo jaar	175Basisgegevens IH en VPB	248Basisgegevens materialiteit kantoor	321Brk Indicatie of vestigingadres buitenlands adres is
30Brk Ranking RAM wolbsom op sofinr dosnr Grote Ondernemingen	103Brk_Alg_Score tot aantal gestolen geëxporteerd gesloopt in jaar	176Brk Aantal amtsshalve opgelegde aanslagen IH binnen 1 jaar	249Brk ROOD Totaal Aantal keren waarde 1 of 1_1 alle categorieën	322Brk Indicatie of woonadres buitenlands adres is
31Brk Ranking RAM wolbsom op sofinr dosnr Niet Grote Ondernemingen	104Brk_Alg_Score tot Sagitta invoer gerelateerd aan omzet OB	177Brk Aantal amtsshalve opgelegde aanslagen VPB binnen 1 jaar	250Brk ROOD Totaal aantal keren waarde 1 alle categorieën	323Brk Totaal aantal verschillende adressen vestiging persoonsadressen in BVR
32WOLB_som RAM op sofinummer en dossiernummernrwo	105Brk_Alg_Score tot Sagitta uitvoer gerelateerd aan omzet OB	178Brk Indicatie herinnering	251Brk ROOD Totaal aantal keren waarde 1_1 alle categorieën	324Brk Totaal aantal verschillende adressen vestiging aktiviteitsadressen in BVR
33Brk RAM wolbsom sofinummer	106MATP_score_materialiteit risicoparameters	179Brk indicatie aanmaning	252Brk ORANJE Aantal keren waarde 0_0100 of 0_0110 categorieën	325Becongegevens
34Brk RAM wolbsom dossiernummer	107Brk_MATP_Score materialiteit land tot aantal rood oranje	180Brk Aantal te laat ingeleverde aangiften IH en VPB	253Brk ORANJE LAAG Totaal aantal keren waarde 0_0100 alle categorieën	326Becon categorie
35RAM_B_Belang en berekening_Bg_belanggroep van een sofinr_	108Brk_MATP_Score materialiteit kantoor tot aantal rood oranje	181Verzamelininkomen vvg	254Brk ORANJE HOOG Totaal aantal keren waarde 0_0110 alle categorieën	327Brk Aantal verschillende beconnummers
36Brk_B_Kleur Wolbsom 70 proc WS finr plus 30 proc WS dosnr en 30 proc x_WS finr plus dosnr	109Brk_MATP_Score materialiteit land geel	182Belastbare winst vvg	255Brk totaal aantal scores ROOD en ORANGE	328Brk Aantal x wel beconuitstel maar geen becon aangifte
37Brk_B_Wolbsom 70 proc WS finr plus 30 proc WS dosnr en 30 proc x_WS finr plus dosnr gede	110Brk_MATP_Score materialiteit kantoor geel	183Aantal ondernemingen in IH codes 0001_0002 etc_max 10 vvg	256Brk GEEL Totaal aantal keren waarde 0_0001 alle categorieën	329Brk aantal verschillende beconns met aanvullingen op aangifte
38Brk_Bg_Belanggroep opgedeeld in groepen 1 tm 10	111Brk_MATP_score materialiteit land geel en ob lh nummers	184Verzamelininkomen def	257Brk GROEN Totaal aantal keren waarde 0 alle categorieën	330Brk aantal verschillende beconns met aanvullingen rubiek aangifte
39RISG_Risicogroep indeling gewogen risicoparameters in cijfers	112PROC_score_proces_risicoparameters	185Belastbare winst def	258Brk totaal aantal mogelijke totaalscores	331Indeling EHI
40Brk_RISG_Risicogroep indeling gewogen alle parameters incl materieel	113Brk_PROC_Score Aantal bezwaarschriften in jaar	186Brk verschil verzamelininkomen vv en def	259Basisgegevens FD_Klanten	332Brk Team indeling actueel MKB EHI
41Brk_RISG_Risicogroep indeling gewogen alle parameters excl materieel	114Brk_PROC_Score Aantal overige verzoeken in jaar	187Brk verschil belastbaar bedrag vvg en def	260Brk mar Aantal branche codes sofinummer 6722 of 9899	333Brk Team KO gesplitst in ARD_HTR_VGL binnen MKB EHI
42Brk_RISG_Risicogroep indeling gewogen materialiteitsparamaters	115Brk_PROC_Score Aantal amtsshalve opgelegde aanslagen IH binnen 1 jaar	188Brk verschil belastbare winst vv en def	261Brk mar Aantal sofinummers met boekenonderzoek behandelopdracht 50	334Brk Indicatie KO nadere verbijzondering_MKB EHI
43Brk_RISG_Risicogroep indeling gewogen algemene parameters	116Brk_PROC_Score Aantal amtsshalve opgelegde aanslagen VPB binnen 1 jaar	189Brk indicatie navordering IH	262Brk pro Scoring alle procesparameters	335Brk Weging in 5 categorieën binnen MKB EHI
44Brk_RISG_Risicogroep indeling gewogen proces parameters	117Brk_PROC_Score indicatie herinnering	190Brk indicatie navordering VPB	263Brk toe Scoring alle toezichtparameters	336Brondatum
45Brk_RISG_Risicogroep indeling gewogen toezicht parameters	118Brk_PROC_Score indicatie aanmaning	191Belastbaar bedrag VPB nav	264Brk Scoring alle procesparameters en alle toezichtparameters	337Brondatum meest recent uitworp IH
46Brk_RISG_Risicogroep indeling gewogen uitworp parameters	119Brk_PROC_Score Aantal te laat ingeleverde aangiften IH en VPB	192Brk totaal inkomen box 1 2 3 nav	265Algemeen 2	338Brondatum meest recent uitworp VPB
47Brk_RISG_Risicogroep indeling gewogen stop parameters	120Brk_PROC_Score Aantal openstaande aanslagen in GOA_INL einde jaar	193Brk indicatie vermindering IH	266Indicatie leidend sofinummer binnen dossiernummer	339Brondatum SOFIKERN
48Brk_RISG_Risicogroep indeling gewogen overige parameters	121Brk_PROC_Score Aantal aangiften verzuimen LH	194Brk indicatie vermindering VPB	267Indicatie dossiernummer actief in jaar	
49RISK_Risicogroep indeling risicoparameters in kleur	122Brk_PROC_Score Aantal betaalverzuimen LH	195Belastbaar bedrag VPB verm	268Brk Aantal verschillende dossiernummers 2009-2015 behorend bij sofinummer	
50Brk_RISK_Risicogroep indeling in kleur alle parameters incl materieel	123Brk_PROC_Score aantal verschillende beconns met aanvullingen op aangifte	196Brk totaal inkomen box 1 2 3 verm	269Brk Aantal verschillende dossiernummer in 1 jaar behorend bij sofinummer	Kern par(ameter) beperkt
51Brk_RISK_Risicogroep indeling in kleur alle parameters excl materieel	124Brk_PROC_Score aantal verschillende beconns met aanvullingen rubrieken aangifte	197Basisgegevens OB en LH	270Verzorgingsgebied	1Algemeen
52Brk_RISK_Risicogroep indeling in kleur materialiteitsparamaters	125Brk_PROC_Score Aantal x wel beconuitstel maar geen becon aangifte	198Brk Aantal OB nummers sofinummer	271Regio code	2Jaar
53Brk_RISK_Risicogroep indeling in kleur algemene parameters	126Brk_PROC_Score Tot aantal niet ontv aangiften OB gerelateerd aan tot aangiften OB	199Brk Aantal LH nummers sofinummer	272KvK nummer volgens BVR	3Sofinummer
54Brk_RISK_Risicogroep indeling in kleur proces parameters	127Brk_PROC_Score Aantal aangiften verzuimen OB gerelateerd aan tot aangiften OB	200Brk Starter LH laatste 4 jaar (incl lopend jaar)	273Doel groep nummer	4Sofinaam
55Brk_RISK_Risicogroep indeling in kleur toezicht parameters	128Brk_PROC_Score Aantal betaalverzuimen OB gerelateerd aan tot aangiften OB	201Brk Totaal aantal te ontvangen aangiften OB	274Doelgroepnaam	5Dossiernummer
56Brk_RISK_Risicogroep indeling in kleur uitworp parameters	129Brk_PROC_Score Aantal verminderingen OB gerelateerd aan aantal naheffingen OB	202Brk Totaal aantal te ontvangen aangiften OB	275Branche code dossiernummer	6Dossiernaam
57Brk_RISK_Risicogroep indeling in kleur stop parameters	130Brk_PROC_Score boete verminderingen OB gerelateerd aan boete naheffingen OB	203Brk Totaal aantal niet ontvangen aangiften OB	276Brancheomschrijving dossiernummer	7Brk Splitsing tbv Oracle 1=MKB 2=VIP en 4=GO
58Brk_RISK_Risicogroep indeling in kleur overige parameters	131Brk_PROC_Score aantal nieuwe werknemers gerelateerd aan werknemers uit jaar	204Brk Aantal naheffingen OB	277Branche code sofinummer	8Brk segment sofinummer waarden GO MKB VIP SUP PAR
59RIS_Risicogroep indeling risicoparameters in cijfers	132Brk_PROC_Score aantal verschillende werknemers gerelateerd aan werknemers uit	205Brk Totaalbedrag boete naheffingen OB	278Brancheomschrijving sofinummer	9Huidig kantoor nummer
60Brk_RIS_Risicogroep indeling alle parameters incl materieel	133TOEZ_score_toezicht_risicoparameters	206Brk Aantal verminderingen OB	279Rechtsvorm code	10Huidig kantoornaam
61Brk_RIS_Risicogroep indeling alle parameters excl materieel	134Brk_TOEZ_Score Aantal gehandhaafde bezwaarschriften in jaar	207Brk Totaalbedrag boete vermindering OB	280Rechtsvorm omschrijving	11KWD_Kwadrant indeling_RISG_Belang en risicogroep indeling gewogen risicoparameters bijv 7_2
62Brk_RIS_Risicogroep indeling materialiteitsparamaters	135Brk_TOEZ_Score Belastbaar bedrag VPB nav	208Brk Aantal aangiften verzuimen OB	281Rechtsvorm groep	12Brk_KWD_BEL_RISG_Belang en risicogroep indeling gewogen alle parameters incl materieel bijv 8
63Brk_RIS_Risicogroep indeling algemene parameters	136Brk_TOEZ_Score Belastbaar bedrag VPB verm	209Brk Aantal betaalverzuimen OB	282Rechtsvorm land	13Brk_KWD_BEL_RISG_Belang en risicogroep indeling gewogen alle parameters excl materieel bijv 7_2
64Brk_RIS_Risicogroep indeling proces parameters	137Brk_TOEZ_Score verschil Belastbaar bedrag VPB vv en def	210Brk Totaal aantal te ontvangen aangiften LH	283VIP indicatie	14Brk_KWD_BEL_RISG_Belang en risicogroep indeling gewogen materialiteitsparameters bijv 10_9
65Brk_RIS_Risicogroep indeling toezicht parameters	138Brk_TOEZ_Score tot bedrag box 1 2 en 3 navordering IH	211Brk Totaal aantal niet ontvangen aangiften LH	284Algemeen extra	15Brk_KWD_BEL_RISG_Belang en risicogroep indeling gewogen algemene parameters bijv 3_8
66Brk_RIS_Risicogroep indeling uitworp parameters	139Brk_TOEZ_Score tot bedrag box 1 2 en 3 vermindering IH	212Brk Aantal nieuwe werknemers FLG	285Dossiernummer fictief	16Brk_KWD_BEL_RISG_Belang en risicogroep indeling gewogen proces parameters bijv 2_10
67Brk_RIS_Risicogroep indeling stop parameters	140Brk_TOEZ_Score Aantal boekenonderzoeken heffing code 50 met correctie	213Brk Aantal werknemers einde jaar FLG	286Particulier of Onderneming	17Brk_KWD_BEL_RISG_Belang en risicogroep indeling gewogen toezicht parameters bijv 6_1
68Brk_RIS_Risicogroep indeling overige parameters	141Brk_TOEZ_Score Actueel openstaande bedrag GOA_INL	214Brk Aantal verschillende werknemers FLG	287Rechtspersoon ja nee	18Brk_KWD_BEL_RISG_Belang en risicogroep indeling gewogen uitworp parameters bijv 7_8
69TOT_Totaal score risicoparameters per groep op sofinummer	142Brk_TOEZ_Score Aantal aanslagen met oninbare bedragen dit jaar	215Brk Aantal aangiften verzuimen LH	288Handelsnaam	19Brk_KWD_BEL_RISG_Belang en risicogroep indeling gewogen stop parameters bijv 8_8
70Brk_TOT_Score totaal score alle risicoparameters incl materieel op sofinummer	143Brk_TOEZ_Score Totaalbedrag van alle toeslagen	216Brk Aantal betaalverzuimen LH	289Geboortedatum	20Brk_KWD_BEL_RISG_Belang en risicogroep indeling gewogen overige parameters bijv 9_8
300929T_Score totaal score alle risicoparameters excl materieel op sofinummer	144Brk_TOEZ_Score verschil verzamelininkomen vv gerelateerd aan verzamelininkomen de	217Basisgegevens rest	290Overlijdensdatum	21WOLB_som RAM op sofinummer en dossiernummernrwo

72	Brk_TOT_Score totaal score materialiteitsparameters op sofinummer	145	Brk_TOEZ_Score verschil belastbare winst vv gerelateerd aan belastbare winst def	218	Brk Aantal bezwaarschriften in jaar	291	Brk indicatie ondernemer op sofinummernivo	22	Brk RAM wolbsom sofinummer	
73	Brk_TOT_Score totaal score algemene risicoparameters op sofinummer	146	Brk_TOEZ_Score verschil algemene risicoparameters	219	Brk Aantal gehandhaafde bezwaarschriften in jaar	292	Brk indicatie ondernemer op dossiernummernivo	23	Brk RAM wolbsom dossiernummer	

Zicht op het subject/subjecten Kern Par(ameter) uitgebreid en beperkt

Journaal verzoek RIT 201600483

Onderwerp : data voor ANBI analyse
Behandelaar : Persoonsgegevens
Datum : maandag 17 oktober 2016
Opdracht eigenaar : Persoonsgegevens
Analist :
Voorgaande verz. : 201400278
Categorie : 2
Doel : Verkrijgen actueel beeld ANBI's

1. Omschrijving verzoek:

Koppelen van extra gegevens aan een bestaande selectie. Bestaande subject selectie is bij verzoek bijgevoegd (Kopie van anbibestand (06-10-2016).xlsx).

Aan dit bestand moeten een aantal extra gegevens worden toegevoegd:

1. Segment en subsegment (Indeling Persoonsgegevens)
2. Vermogenspositie per subject per 1 jan 2015 en 2016
(banksaldi, beleggingen en waarde onroerend goed)
3. Fiscale info (voor welke middelen actief, actueel)
4. Fiscale kasstroom voor de jaren 2015 en 2016.

2. Voortgang

17 oktober 2016:

Gebeld met Persoonsgegevens

- Zij is vanuit EHi uitgeleend aan D&A en werkt daar o.a. aan het ontsluiten van het G.V.S. , het Geld Verkeer Systeem. Hieruit is onder andere de benodigde informatie te halen. Persoonsgegevens vertelde mij dat zij deze informatie niet mag delen met EHi en dat deze binnen D&A beperkt beschikbaar is i.v.m. privacy.

- Dit doorgegeven aan Persoonsgegevens

Mail gestuurd aan Persoonsgegevens

- Snelle reactie van Persoonsgegevens
 - heb merendeel van de data beschikbaar;
 - Persoonsgegevens is hier in het verleden ook mee bezig geweest;
- Woensdag ochtend 9:00 – 9:30 verder met P-gv. bespreken.

Persoonsgegevens gebeld:

- Heeft inderdaad 1,5 jaar geleden op basis van RAM een risico model ANBI's gemaakt voor een project ANBI's. Hiervoor waren 66 risico indicatoren bedacht waarin o.a. familie relaties waren meegenomen. Het gaat hier om een 'herhaalbaar' script, waarbij echter nog wel na gelopen moet worden of de data in Ram nog onder dezelfde noemers beschikbaar is. Kan dus niet zo 123 gedraaid worden en is niet actueel beschikbaar.

- Donderdag bij werkoverleg met P-gv. bespreken of we hier inspanning op gaan zetten.



VERTROUWELIJK
MT MKB

Naam dienstonderdeel
MKB.nl

Contactpersoon
Persoonsgegevens

Datum
27 november 2020

Auteur
Persoonsgegevens

memo

Intelligence Voorziening Toezicht – besluit en afspraken

Inleiding

In het MT MKB d.d. dinsdag 17 november 2020 is de memo Scenario's IVT¹ besproken. Het MT MKB heeft toen de sterke voorkeur uitgesproken om scenario 2 te volgen "beëindigen gebruik spoor 2 IVT per 1 januari 2021 en starten intakes en gezamenlijke verkenningen ten behoeve van ombouw producten".

Op 24 november jl. is in een gezamenlijk overleg op MT MKB en MT DF&A niveau de keuze voor scenario 2 gedeeld. Ook het MT DF&A heeft de sterke voorkeur voor dit scenario.

In dit memo wordt kort uiteengezet wat nu de te nemen stappen zijn om de benodigde voortgang te realiseren en te borgen dat het toezicht en de handhaving vanuit MKB doorgang kan vinden.

1. Voorkeur bestendigen in een besluit

De keuze voor scenario 2 wordt namens MT MKB en MT DF&A kenbaar gemaakt in de eerstkomende verandertafel en ketentafel GKT.

Een verdere uitwerking van dit gezamenlijke management besluit zal plaatsvinden in het Business Owner Overleg IVT. Concreet betekent dit een nadere invulling van:

- richting en architectuur IVT (waar werken we concreet naar toe)
- samenwerking (wat zijn onze gemeenschappelijke uitgangspunten)
- voorwaarden (welke spelregels hanteren we)

2. Werkzaamheden IVT borgen in portfolio GKT

De benodigde werkpakketten die ontstaan vanwege het beëindigen van het gebruik van spoor 2 IVT zijn reeds ingelegd bij de keten GKT. Deze werkpakketten hebben de hoogste prioriteit meegekregen (keten harde verplichting) in het portfolio GKT en zullen worden ingepland in het PI-event GKT d.d. 14 december 2020.

De werkpakketten betreffen op hoog niveau:

- IVT Uitmaken spoor 2 IVT per 1-1-2021 (gereed 1-1-2021)
- IVT Architectuur structurele IVT voorziening (gereed Q1 2021)

¹ Zie bijlage Memo scenario's IVT

- IVT GEB's ten behoeve van IVT producten en structurele IVT voorziening (gereed Q2 2021)
- IVT Ombouw structurele IVT producten MKB naar analytics domein (start Q1 2021 en verder)
- IVT Inrichten structurele IVT voorziening ten behoeve van eenmalige analyses en ad-hoc vragen (uitwerkingen architectuur zal bepalend zijn voor realisatie)
- IVT Doorontwikkeling Datafundament Subject (beheer en onderhoud / doorlopend)

In Q1 2021 zal de hoogste prioriteit gegeven worden aan het uitwerken van de benodigde architectuur ten behoeve van een voorziening voor het doen van fenomeenonderzoeken en eenmalige analyses. Daarnaast zal gestart worden met intakes en verkenningen ten behoeve van de ombouw van de structurele producten MKB.

Regie en sturing op voortbrenging en realisatie van deze werkpakketten IVT vindt plaats vanuit het Business Owner Overleg IVT.

3. Functionaliteiten MKB per 1-1-2021 inzichtelijk maken

Het MT MKB wil inzicht hebben in welke functionaliteiten en werkprocessen geraakt worden door het beëindigen van spoor 2 IVT per 1-1-2021. Wat is er gedekt per 1 januari 2021 en wat verliezen we eventueel (tijdelijk) aan functionaliteit? Deze analyse moet neerslaan in een feitelijke weergave met bijhorende tijdsplanning wanneer de vervanging op orde kan zijn.

De afspraak is gemaakt deze feitelijke weergave iteratief op te bouwen en wekelijks op inhoud en voortgang te communiceren.

Wat nu in beeld is:

- Output uit structurele MKB producten welke gebouwd zijn op spoor 2 IVT is afgedekt. DF&A staat garant voor de vervangende gegevensleveringen (zie punt 4)
- eenmalige analyses en fenomeenonderzoeken welke uitgevoerd worden door MKB analisten vallen stil per 1 januari 2021, tenzij een werkend samenwerkingsmodel MKB en DF&A operationeel is. De precieze vorm en invulling van dit samenwerkingsmodel moet zo spoedig mogelijk worden uitgewerkt. Hierbij kan gebruik worden gemaakt van eerdere ideeën en uitwerkingen op dit vlak (zie punt 7)

4. Gegevensleveringen ten behoeve van continuïteit

Het MT DF&A heeft toegezegd garant te staan voor de benodigde gegevensleveringen als gevolg van het beëindigen van de structurele MKB producten op spoor 2 IVT. Ook zij hechten belang aan het werk van de MKB behandelaar dat door moet kunnen gaan.

Hiertoe wordt een planningskalender opgesteld. Deze kalender maakt duidelijk op welk moment MKB een kant en klare gegevenslevering geleverd krijgt. Dit betekent concreet dat DF&A de huidige output uit de 9 geïnterpreteerde structurele MKB producten² zal verstrekken aan een door MKB geautoriseerd persoon dan wel personen. Een GEB aan MKB zijde is voor deze tijdelijke leveringen niet nodig, dit wordt afgedekt door de kwaliteitsprocedure aan DF&A zijde.

² Zie Bijlage Overzicht structurele MKB producten op Spoor 2 IVT

Regie en sturing hierop vindt plaats vanuit het Business Owner Overleg IVT.

5. Opstellen en accorderen GEB's

MKB heeft samen met IV&D vastgesteld dat er vier GEB's opgesteld en geaccordeerd dienen te worden ten behoeve van het toekomstige gebruik van structurele producten (voormalige MKB IVT producten) en een voorziening ten behoeve van het doen van fenomeenonderzoeken en eenmalige/ad-hoc analyses. Dit vraagt om benodigde capaciteit en prioriteit binnen de directie MKB om deze GEB's tijdig gereed te hebben.

De benodigde doorlooptijd die is afgegeven door Persoonsgegevens MKB voor het opstellen en geaccordeerd krijgen van deze vier GEB's betreft vijf maanden. Dit betekent dat de vier benodigde GEB's in mei 2021 op orde zijn.

Realisatie hiervan vindt plaats in de reguliere lijn.

6. Impact en gevolgen MKB analisten

De keuze voor scenario 2 zal een impact hebben op het totale werkpakket van de IVT analisten MKB. Het huidige werkpakket zal afnemen dan wel op langere termijn elders worden uitgevoerd. Een nadere uitwerking hiervan inclusief de impact op medewerkersniveau is nodig.

Gezien het langslappende karakter van dit dossier is het zeer aan te raden om hier vanuit het MT MKB persoonlijke aandacht voor te hebben. Betrokken en gedreven MKB medewerkers ervaren al een geruime tijd onzekerheid en onduidelijkheid met betrekking tot hun werkzaamheden.

Het advies is dan ook om zo spoedig mogelijk in gesprek te gaan met de analisten IVT MKB. Met hen de richting te delen en in gesprek te gaan over het te volgen proces. In individuele gesprekken oog te hebben voor de mogelijke gevolgen die het heeft voor de persoon in kwestie.

7. Samenwerking MKB en DF&A inrichten

Per 1-1-2021 zal een samenwerkingsverband gaan ontstaan tussen de MKB analisten en DF&A medewerkers op het vlak van het doen van fenomeenonderzoeken en eenmalige/ad-hoc analyses. Dit samenwerkingsverband zal in de komende weken nader uitgewerkt moeten worden. Het betreft een concrete uitwerking in de zin van spelregels, processen en procedures die we volgen, transparantie in werkzaamheden, buddy-schap etc..

Regie en sturing hierop vindt plaats vanuit het Business Owner Overleg IVT.

Inhoudsopgave Deel A HIB-BBN 2003 Belastingdienst: HIB-BBN en Maatregelenet

1. Inleiding	2
1.1 Totstandkoming normatiek	2
1.2 Inhoud van dit document	2
1.3 Opbouw van dit document	3
1.4 Doel en reikwijdte van het handboek	3
1.5 Afwijkingen van de Maatregelenet door een regio-eenheid	4
1.6 Indeling beveiligingsnormatiek	4
1.7 Modellen en Sjablonen	5
1.8 Overzicht wijzigingen HIB-BBN	6
1.8.1 Planning en control	6
1.8.2 Gebouwen en installaties	6
1.8.3 Personeel en organisatie	7
1.8.4 Informatiesystemen	8
1.8.5 Nieuwe aanduidingen	9
1.9 Relatietabel Normatiek en Intern Controle Programma	9
1.10 Onderhoud van het HIB-BBN	10
2. Strategisch beleidskader	11
2.1 Het belang van informatiebeveiliging en integriteitsaspecten	11
2.2 Uitgangspunten	12
2.2.1 Basisbeveiligingsniveau en eventuele afwijkingen daarop	12
2.2.2 Aanvaardbaar risico	12
2.2.3 Samenhang informatiebeveiligingsmaatregelen	12
2.2.4 Analyse van verhoogde risico's	14
2.3 Verantwoordelijkheden	14
2.3.1 Integraal management	14
2.3.2 Delegeren van verantwoordelijkheden	15
2.4 Borging	15
2.4.1 Communicatie	15
2.4.2 Toetsing	16
3. HIB-BBN	17
3.1 Planning en Control	17
3.1.1 Planning en organisatie	18
3.1.2 Uitbesteding	20
3.1.3 Beheersing	22
3.1.4 Continuïteit van de organisatie	23
3.2 Gebouwen en Installaties	26
3.2.1 Fysieke inrichting	27
3.2.2 Toegangsbeveiliging	28
3.3 Personeel en Organisatie	32
3.3.1 Aanstelling en benoeming	33
3.3.2 Inrichting organisatie	36
3.3.3 Informatie en communicatie	39
3.3.4 Werkplekbeveiliging	41
3.3.5 Vertrek / verandering van functie	43
3.3.6 Overige integriteitsaspecten	45
3.3.7 Risico's en buitengewone voorvallen	48
3.3.8 Gebruik en terbeschikkingstelling bedrijfsmiddelen	51
3.4 Informatiesystemen	53
3.4.1 Gebruik van informatiesystemen	54
3.4.2 Logische toegangsbeveiliging	56
3.4.3 Gebruik en beheer van gegevens	59

1. Inleiding

1.1 Totstandkoming normatiek

Tot maart 2001 was de geldende normatiek van de Belastingdienst op het gebied van informatiebeveiliging op strategisch/tactisch niveau verwoord in het Handboek Informatiebeveiliging Belastingdienst (hierna aangeduid als HIB) uit 1996. Dit handboek gaf invulling aan de vanuit het Voorschrift Informatiebeveiliging Rijksdienst (VIR) gestelde eis dat elke overheidsdienst een beleidsdocument voor informatiebeveiliging dient vast te stellen en uit te dragen.

De normatiek in het HIB is gebaseerd op de verdeling van taken, bevoegdheden en verantwoordelijkheden zoals die toentertijd waren belegd. Sedert 1996 zijn hierin belangrijke wijzigingen doorgevoerd c.q. staan er belangrijke wijzigingen gepland. Voorbeelden hiervan zijn de Belastingdienst-Straks ontwikkelingen en de totstandkoming van het Centrum voor Proces- en Productontwikkeling (B/CPP) en het Centrum voor Informatie en Communicatie Technologie (B/CICT). Ook als gevolg van maatschappelijke en technologische ontwikkelingen (internetskoppelingen, openheid van systemen voor belastingplichtigen e.d.) is actualisering noodzakelijk.

Om de manier waarop binnen de Belastingdienst wordt omgegaan met informatiebeveiliging en integriteit op een hoger niveau te brengen en te houden is door de voormalige Directieraad het programma ARG1 (Aandacht voor Risicobeheersing Gegevensbeveiliging en Integriteit) ingesteld, dat bestaat uit een negental projecten. Het project HIB-BBN (Handboek Informatiebeveiliging Belastingdienst - Basis Beveiligings Niveau) heeft tot doel het actualiseren, structureren en concretiseren van de beveiligingsnormatiek binnen de Belastingdienst. De andere ARG1-projecten geven vanuit hun verschillende expertisegebieden inbreng aan de normatiek.

Binnen het ARG1-project is in 2001 al een nieuwe versie opgeleverd van de normatiek op het gebied van informatiebeveiliging en integriteit, het HIB-BBN 2001 Eenheden. In deze versie was reeds rekening gehouden met de bepaalde ontwikkelingen, zoals de totstandkoming van B/CPP, B/CICT en de ontwikkelingen op technologisch en maatschappelijk gebied. Onder andere door de Belastingdienst-Straks ontwikkelingen en het op peil houden van het basis beveiligingsniveau is besloten om het HIB-BBN 2001 Eenheden per 1 januari 2003 te updaten naar het HIB-BBN 2003 Belastingdienst.

De beschreven normatiek voor het verantwoordelijkheidsgebied regio-eenheden zal worden gehanteerd als toetsingskader voor het ARG1-project CI² (Certificering Informatiebeveiliging en Integriteitsaspecten).

1.2 Inhoud van dit document

Dit document beschrijft de normatiek op het gebied van informatiebeveiliging en integriteit voor het verantwoordelijkheidsgebied regio-eenheden binnen de Belastingdienst. Met ingang van 1 januari 2003 vervangt dit document de normatiek van het verantwoordelijkheidsgebied eenheden (nu regio-eenheden) uit het HIB-BBN 2001 Eenheden.

Voor de andere verantwoordelijkheidsgebieden, belegd bij de verschillende ondersteunende diensten (zoals B/CPP en B/CICT), wordt momenteel gewerkt aan een actualisering, structurering en concretisering van de normatiek zoals die is vastgelegd in het HIB 1996. Bij het gereed komen van deze normatiek zal een nieuw Handboek Informatiebeveiliging Belastingdienst worden uitgebracht, inclusief een aangepast strategisch beleidskader.

Voor de regio-eenheden is in dit handboek naast de richtlijnen en normen ook een maatregelenet opgenomen. De set van maatregelen is zodanig van opzet dat bij het realiseren van deze maatregelen het basisbeveiligingsniveau wordt gehaald. Daarnaast is een, op de maatregelenet aansluitend, Intern Controle Programma ontwikkeld. Dit is separaat bijgevoegd.

1.3 Opbouw van dit document

Hoofdstuk 1 behandelt de achtergrond en het doel van het handboek. Ook geeft het een overzicht van de structuur, de inrichting van het handboek en zegt het iets over het onderhoud.

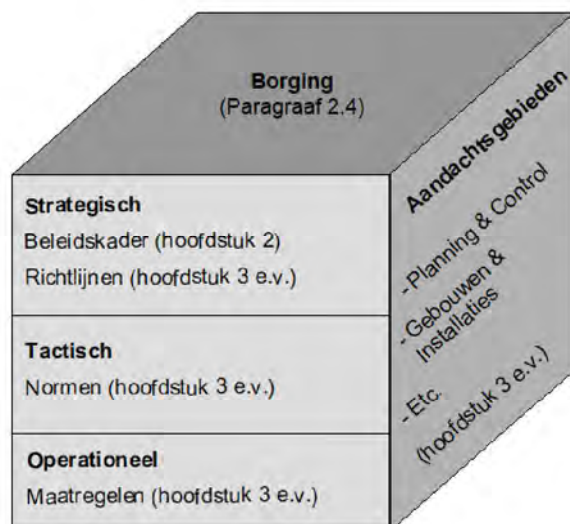
Hoofdstuk 2 omvat het strategisch beleidskader: de vastlegging van het geformuleerde en gewenste beleid op het gebied van informatiebeveiliging en integriteitsaspecten. Aangegeven wordt onder meer het belang van informatiebeveiliging en integriteit voor de Belastingdienst, de uitgangspunten, verantwoordelijkheden en de borging van het strategisch beleidskader binnen de Belastingdienst

In hoofdstuk 3 worden vanuit het strategisch beleidskader door middel van richtlijnen en normen eisen gesteld aan de inrichting van de informatiebeveiliging en integriteitsaspecten. De normatiek voor het verantwoordelijkheidsgebied regio-eenheden is opgedeeld in de volgende aandachtsgebieden:

- Planning en control (P&C);
- Gebouwen en installaties (G&I);
- Personeel en organisatie (P&O);
- Informatiesystemen (INF).

De inrichting van het HIB-BBN kan schematisch als volgt worden weergegeven:

Figuur 1: Structuur HIB-BBN



1.4 Doel en reikwijdte van het handboek

De primaire en ondersteunende processen van de Belastingdienst zijn in hoge mate afhankelijk van adequate informatievoorziening en betrouwbare informatiesystemen.

Het informatiebeveiligings- en integriteitsbeleid is er op gericht de beschikbaarheid, de integriteit en de vertrouwelijkheid van de (geautomatiseerde) informatievoorziening te waarborgen.

Om een beheersbare en betrouwbare informatievoorziening te realiseren is het van belang een aantal gemeenschappelijke uitgangspunten te hanteren en uit te dragen.

De doelstelling van het handboek is het vastleggen van het informatiebeveiligings- en integriteitsbeleid van de Belastingdienst en is daarmee de basis voor de implementatie van de concrete operationele beveiligingsmaatregelen.

Het handboek is bedoeld voor het management van de Belastingdienst, omdat het management primair verantwoordelijk is voor de (geautomatiseerde) bedrijfsprocessen en voor de betrouwbare en ongestoorde werking daarvan. Daarnaast is het handboek bedoeld voor management en medewerkers op het gebied van informatiebeveiliging, integriteit en informatiemanagement. Tevens is het handboek de basis voor de toetsing van de concrete operationele beveiligingsmaatregelen.

1.5 Afwijkingen van de Maatregelenet door een regio-eenheid

Het is een regio-eenheid toegestaan een alternatieve maatregelenet te hanteren mits voldaan wordt aan de volgende criteria:

- Motivatie
De regio-eenheid geeft gemotiveerd aan waarom voor een alternatieve maatregelenet is gekozen.
- Toereikendheid
De regio-eenheid geeft aan waarom zij van opvatting is dat de alternatieve maatregelenet een gelijkwaardig beveiligingsniveau realiseert als invulling van de normatiek zoals vastgelegd in het BBN.
- Sanctioneren
Het verantwoordelijke management sanctioneert de alternatieve maatregelenet.
- Documentatie
De alternatieve maatregelenet dient te zijn gedocumenteerd (inclusief de meer algemene eisen op het gebied van motivatie, toereikendheid en sanctionering, zie hiervoor).

1.6 Indeling beveiligingsnormatiek

De gehanteerde indeling van beveiligingsnormatiek kan worden onderverdeeld in een strategisch, tactisch en operationeel niveau (zie tabel). Deze niveaus worden aangeduid met respectievelijk richtlijnen, normen en maatregelen. Binnen de Belastingdienst worden deze uitgewerkt in het Handboek Informatiebeveiliging (HIB), Basis Beveiligings Niveau (BBN) en maatregelenet (ook wel MS genoemd). Deze set is zodanig van opzet dat bij het realiseren van deze maatregelen het basisbeveiligingsniveau wordt gehaald. Daarnaast is nog een op de maatregelenet aansluitend Intern Controle Programma (ook wel ICP genoemd) opgesteld.

<i>Niveau</i>	<i>Aanduiding</i>	<i>Uit te werken in</i>
Strategisch	Richtlijnen	Handboek Informatiebeveiliging Belastingdienst (HIB)
Tactisch	Normen	Basis Beveiligings Niveau (BBN)
Operationeel	Maatregelen	• Maatregelenet voor regio-eenheden • Intern Controle Programma

Voor de normatiek is binnen elk aandachtsgebied de volgende structuur gehanteerd:

Structuur normatiek informatiebeveiliging en integriteit per aandachtsgebied		
DEEL A DOCUMENT HIB-BBN 2003 BELASTINGDIENST EN MAATREGELENSET		
<i>Niveau</i>	<i>Stramien</i>	<i>Toelichting</i>
Strategisch	Aandachtsgebied	Clustering van richtlijnen, normen en maatregelen die binnen het aandachtsgebied moeten worden getroffen.
	Richtlijn	Richtlijnen (HIB) Om onderscheid aan te brengen tussen richtlijnen wordt de volgende syntax gehanteerd: <aandachtsgebied R(ichtlijn) – volgnummer> <i>Voorbeeld: de syntax van een richtlijn binnen het aandachtsgebied Planning & Control is: P&C R-1.</i>
	Risicoafweging	Tekstuele beschrijving van risico's die met de richtlijn worden afgedekt.
Tactisch	Norm	Normen (Basis Beveiligings Niveau) als nadere uitwerking van een richtlijn. Om onderscheid aan te brengen wordt de volgende syntax gehanteerd: <aandachtsgebied N(orm) – volgnummer – doorloopnummer> <i>Voorbeeld: de syntax van een norm binnen een richtlijn van het aandachtsgebied Planning & Control is: P&C N-1-1.</i>
Operationeel	Maatregelen	Operationeel te treffen set van maatregelen die, uitgaande van een standaard risicoprofiel, in opzet tegemoet komen aan de gestelde norm. Door invoering van de maatregelen wordt voldaan aan het basis beveiligingsniveau. Een regio-eenheid mag – onder strikte voorwaarden – een alternatieve maatregel treffen zolang daarmee wordt voldaan aan de norm.
Deel B DOCUMENT ICP HIB-BBN		
	Intern Controle Programma (ICP)	Beschrijving van de intern uit te voeren controlevragen ter toetsing van de maatregelen.

1.7 Modellen en Sjablonen

In dit document is regelmatig sprake van modellen en sjablonen (bijv. Aanvraagformulier logische autorisaties). Tevens dienen de regio's, conform de normatiek, in een aantal beschreven gevallen rapporten, registraties, plannen en overeenkomsten op te zetten en bij te houden (bijv. BIP, calamiteitenplan, SNO/SNR, registratie buitengewone voorvallen, etc). Vanuit diverse onderdelen van de Belastingdienst zijn inmiddels modellen en sjablonen ontwikkeld om hieraan invulling te geven. Daarnaast zijn vanuit het ARG1-project HIB-BBN aan de regio-eenheden een aantal modellen ter beschikking gesteld. Om te voorkomen dat het wiel telkenmale opnieuw wordt uitgevonden en om de regio-eenheden een handreiking te bieden bij het opzetten van de diverse modellen en sjablonen, is medio 2002 vanuit het ARG1-project HIB-BBN een set modellen en sjablonen aangeboden aan de eenheden in de vorm van een modellenboek met de naam 'Modellenboek HIB-BBN 2001 Eenheden'. Tegelijk met het uitbrengen van dit HIB-BBN is een nieuwe set modellen uitgebracht onder de naam 'Modellenboek HIB-BBN 2003 Belastingdienst', die voldoet aan de eisen van het nieuwe HIB-BBN 2003 Belastingdienst.

De modellen en sjablonen hebben geen verplichtend karakter. Dit wil zeggen dat een regio-eenheid vrij is om de modellen en sjablonen te gebruiken. Daarbij wordt opgemerkt dat een regio-eenheid die gebruik maakt van de aangeleverde modellen en sjablonen, er zeker van kan zijn dat deze voldoen aan de eisen die het HIB-BBN 2003 Belastingdienst daaraan stelt.

1.8 Overzicht wijzigingen HIB-BBN

In de hierna opgenomen tabellen wordt globaal aangegeven welke wijzigingen in het HIB-BBN 2003 Belastingdienst zijn doorgevoerd ten opzichte van het HIB-BBN 2001 Eenheden .

1.8.1 Planning en control

HIB-BBN Eenheden 2001		HIB-BBN Belastingdienst 2003		Globale wijzigingen met ingang van 1 januari 2003 geldend
<i>HIB-richtlijn</i>	<i>BBN-norm</i>	<i>HIB-richtlijn</i>	<i>BBN-norm</i>	
P&C ER-1	P&C EN-1-1	P&C R-1	P&C N-1-1	Marginale A-analyse is Analyse Verhoogd Risico geworden, methode is uitgewerkt en maatregelen zijn daarop aangepast
	P&C EN-1-2		P&C N-1-2	SBO-monitor is vervallen, rapportages Testteam toegevoegd
	P&C EN-1-3		P&C N-1-3	Geen wijzigingen
P&C ER-2	P&C EN-2-1	P&C R-2	P&C N-2-1	Facilitaire diensten gewijzigd in interne dienstverleners, extra maatregel omtrent totaaloverzicht uitbesteding (1 ^e bullet)
	P&C EN-2-2		P&C N-2-2	Bullet 1: woord 'schriftelijk' toegevoegd
P&C ER-3	P&C EN-3-1	P&C R-3	P&C N-3-1	Bullet 1: afstemmen van wijzigingen op ICP is toegevoegd in 1 ^e bullet
			P&C N-3-2	Nieuwe norm over taken en verantwoordelijkheden op het gebied van informatiebeveiliging en integriteit
P&C ER-4	P&C EN-4-1	P&C R-4	P&C N-4-1	Verwijzing Modellenboek HIB-BBN 2003 Belastingdienst opgenomen NB opgenomen over HCB
	P&C EN-4-2		P&C N-4-2	Verwijzing Modellenboek HIB-BBN 2003 Belastingdienst opgenomen, SNO-afspraken over onderhoudswerkzaamheden toegevoegd, verwijzing naar MTU's opgenomen
	P&C EN-4-3		P&C N-4-3	Bullet toegevoegd: afspraken B/CFD, B/CICT over testen, bullet 1: 'éénmaal' gewijzigd in 'minimaal één keer'

1.8.2 Gebouwen en installaties

HIB-BBN Eenheden 2001		HIB-BBN Belastingdienst 2003		Globale wijzigingen met ingang van 1 januari 2003 geldend
<i>HIB-richtlijn</i>	<i>BBN-norm</i>	<i>HIB-richtlijn</i>	<i>BBN-norm</i>	
G&I ER-1	G&I EN-1-1	G&I R-1	G&I N-1-1	DRB-notitie verwerkt in maatregelen, informeren medewerkers over risico's, toelaten onbekende personen

G&I ER-2	G&I EN-2-1	G&I R-2	G&I N-2-1	Aan risicoafweging risico van ondersteunende diensten toegevoegd. Geen wijzigingen aan norm en maatregelen
	G&I EN-2-2		G&I N-2-2	3 ^e liggend streepje: 'in een bepaalde tijdspanne' toegevoegd
	G&I EN-2-3		G&I N-2-3	Afspraken B/CFD en machtiging interne dienstverleners toegevoegd, audittrail uitgebreid, Belastingdienstkaart geïntroduceerd
	G&I EN-2-4		G&I N-2-4	Belastingdienstkaart geïntroduceerd
	G&I EN-2-5		G&I N-2-5	Bezoekers melden bij receptie i.p.v. B/CFD
	G&I EN-2-6		G&I N-2-6	Belastingdienstkaart geïntroduceerd, extra zin toegevoegd over vergeten kaart
	G&I EN-2-7		G&I N-2-7	Belastingdienstkaart geïntroduceerd, melding bewonersservice toegevoegd

1.8.3 Personeel en organisatie

In de inleidende tekst op het aandachtsgebied Personeel en Organisatie is de definitie van extern personeel gewijzigd. Extern personeel dat niet valt onder een mantelcontract is toegevoegd.

HIB-BBN Eenheden 2001		HIB-BBN Belastingdienst 2003		Globale wijzigingen met ingang van 1 januari 2003 geldend
<i>HIB-richtlijn</i>	<i>BBN-norm</i>	<i>HIB-richtlijn</i>	<i>BBN-norm</i>	
P&O ER-1	P&O EN-1-1	P&O R-1	P&O N-1-1	Verduidelijkt voor wie norm geldt (internen/externen) en wat als identiteitsbewijs wordt gezien
	P&O EN-1-2		P&O N-1-2	Verduidelijkt wanneer een belastingdienstmedewerker aangesteld mag worden en wat voor externen geldt m.b.t. VOG, doelgroep antecedentenonderzoek aangepast
	P&O EN-1-3		P&O N-1-3	Datum in norm en maatregelen opgenomen, aangegeven binnen welke termijn eed/belofte afgelegd moet zijn
	P&O EN-1-4		P&O N-1-4	Mantelovereenkomst opgenomen
P&O ER-2	P&O EN-2-1	P&O R-2	P&O N-2-1	Risicoafweging: risico's toezicht toegevoegd, term mobiliteit gewijzigd Norm: bullet 1 verwijderd en vervangen door de noodzaak van taak- en functiebeschrijvingen, beoordeling beschrijvingen aangepast
	P&O EN-2-2		P&O N-2-2	Voorbeelden conflicterende taken toegevoegd, bij twijfel wordt ook leidinggevende ingelicht en niet alleen PFC/P&O
	P&O EN-2-3		P&O N-2-3	Term mobiliteit gewijzigd in roulatie, verduidelijkt dat het gaat om roulatie i.h.k.v. informatiebeveiliging en integriteit, norm is herschreven
	P&O EN-2-4		P&O N-2-4	Verduidelijking verantwoordelijkheid regio-eenheid, definitie intern en extern personeel verwijderd
P&O ER-3	P&O EN-3-1	P&O R-3	P&O N-3-1	Bewustzijnsverhogende hulpmiddelen toegevoegd, SBO-monitor is vervallen, actieve communicatie toegevoegd

	P&O EN-3-2		P&O N-3-2	Modules toegevoegd
P&O ER-4	P&O EN-4-1	P&O R-4	P&O N-4-1	Procedure toegevoegd
	P&O EN-4-2		P&O N-4-2	Verduidelijken tijdelijke afwezigheid, piekperiode toegevoegd, laatste bullet is herschreven, bullet toegevoegd over toezicht op schoonmaakwerkzaamheden
P&O ER-5	P&O EN-5-1	P&O R-5	P&O N-5-1	Acties B/CICT/DV en B/CFD opgenomen in 3 ^e bullet
P&O ER-6	P&O EN-6-1	P&O R-6	P&O N-6-1	Verduidelijkt voor wie norm geldt en of de medewerker verplicht is nevenwerkzaamheden te melden
	P&O EN-6-2		P&O N-6-2	Guldens omgezet naar euro's
	P&O EN-6-3		P&O N-6-3	Actieve communicatie toegevoegd
P&O ER-7	P&O EN-7-1	P&O R-7	P&O N-7-1	Voorbeelden risico's en informeren medewerkers toegevoegd
	P&O EN-7-2		P&O N-7-2	Incidenten gewijzigd in buitengewone voorvallen, informeren medewerkers toegevoegd
	P&O EN-7-3		P&O N-7-3	Melding aan FIOD toegevoegd, verwijzing opgenomen naar notitie DRB
P&O ER-8	P&O EN-8-1	P&O R-8	P&O N-8-1	Bullet 1 is herschreven, PFC verwijderd, richtlijnen gebruikerskaart aangepast
	P&O EN-8-2		P&O N-8-2	Voorbeelden bedrijfsmiddelen en ontheffingen opgenomen, splitsing IT-voorzieningen en overige bedrijfsmiddelen

1.8.4 Informatiesystemen

HIB-BBN Eenheden 2001		HIB-BBN Belastingdienst 2003		Globale wijzigingen met ingang van 1 januari 2003 geldend
<i>HIB-richtlijn</i>	<i>BBN-norm</i>	<i>HIB-richtlijn</i>	<i>BBN-norm</i>	
INF ER-1	INF EN-1-1	INF R-1	INF N-1-1	IM-lijst gewijzigd in 'ILA-database', afspraken maken met B/CICT/DV opgenomen, audittrail uitgebreid
	INF EN-1-2		INF N-1-2	Actieplan toegevoegd
INF ER-2	INF EN-2-1	INF R-2	INF N-2-1	Bullet toegevoegd over de onmogelijkheid van splitsing autorisaties in informatiesystemen
	INF EN-2-2		INF N-2-2	Verantwoordelijkheid regio-eenheid voor ondersteunende diensten verduidelijkt, afspraken maken met B/CICT/DV opgenomen
INF ER-3	INF EN-3-1	INF R-3	INF N-3-1	Structurele gegevens verstrekking gewijzigd in structurele informatieverstrekking, Wbp toegevoegd, houden van toezicht op uitwisseling gegevensdragers verwijderd, regels gegevensdragers herschreven, controle legitimatiebewijzen toegevoegd, werkinstructie toegevoegd, Wbp-coördinator en privacyfunctionaris geïntroduceerd, nadere onderverdeling gemaakt
			INF N-3-2	Nieuwe norm over gegevensintegriteit toegevoegd

	INF EN-3-2		INF N-3-3	Verklaring internetwerkplek is geen verplichting meer, maar een optie
	INF EN-3-3		INF N-3-4	Actieve communicatie toegevoegd

1.8.5 Nieuwe aanduidingen

Door de herstructurering van de organisatie van de Belastingdienst zijn een aantal aanduidingen die in het HIB-BBN Eenheden 2001 opgenomen waren niet meer van toepassing. In de plaats daarvan zijn nieuwe rollen en functies ontstaan die gebruikt worden in het nieuwe HIB-BBN. Voor de duidelijkheid is in de volgende tabel aangegeven welke aanduidingen zijn vervangen.

HIB-BBN Eenheden 2001	Wijzigingen met ingang van 1 januari 2003 geldend
<i>Oude aanduiding</i>	<i>Nieuwe aanduiding</i>
Doelgroep	Managementteam
Directie	Managementteam
Eenheid	Regio-eenheid
Hoofd van de eenheid	Managementteam van de regio-eenheid
FIB	Functionaris belast met informatiebeveiliging
DGBEL	DGBD
(V)ICP	ICP
(V)MS	MS
Facilitaire dienst	Ondersteunende dienst

1.9 Relatietabel Normatiek en Intern Controle Programma

In de navolgende tabel is per norm opgenomen welke Informatiebeveiliging & Integriteit (I&I) IC-vragen daarbij behoren. De I&I IC-vragen zijn opgenomen in deel B van het HIB-BBN 2003 Belastingdienst en het Handboek Bestuurlijke Informatie Verzorging (HBIV). Let hierbij op dat de I&I- nummering niet meer overeenkomt met de nummering van de versie van maart 2001, doordat er twee normen zijn toegevoegd in het HIB-BBN 2003 Belastingdienst (P&C N-3-2 en INF N-3-2).

Norm	ICnr	Omschrijving IC
P&C N 1-1	I&I-1-01	Controle op uitvoering Analyse Verhoogd Risico (AVR)
P&C N 1-2	I&I-1-02	Controle op Beveiligings- en integriteitsplan (BIP)
P&C N 1-3	I&I-1-03	Controle op voortgangsbewaking uitvoering van het BIP
P&C N-2-1	I&I-1-04	Controleren op vastlegging afspraken met ondersteunende diensten in SNO's
P&C N-2-2	I&I-1-05	Controle op gerealiseerde dienstverlening ondersteunende diensten
P&C N 3-1	I&I-1-06	Controle op uitvoering interne controles
P&C N-3-2	I&I-1-07	Controle op beleggen van taken en verantwoordelijkheden op het gebied van informatiebeveiliging en integriteit
P&C N 4-1	I&I-1-08	Controle op BHV-organisatie
P&C N 4-2	I&I-1-09	Controle op calamiteitenorganisatie
P&C N 4-3	I&I-1-10	Controle op werking van de BHV- en calamiteitenorganisatie
G&I N 1-1	I&I-1-11	Controle op fysieke inrichting gebouw
G&I N 2-1	I&I-1-12	Controle op organisatorische procedures bij fysieke toegangsmaatregelen
G&I N 2-2	I&I-1-13	Controle op vaststelling autorisatieprofielen
G&I N 2-3	I&I-1-14	Controle op verleende toegangsrechten
G&I N 2-4	I&I-1-15	Controle op aanvraagprocedure verstrekken van Belastingdienstkaart/derdenpas
G&I N 2-5	I&I-1-16	Controle op hanteren bezoekersprocedure
G&I N 2-6	I&I-1-17	Controle op draagplicht Belastingdienstkaart-/derdenpas/bezoekerspas
G&I N 2-7	I&I-1-18	Controle op meldingsprocedure van verlies, diefstal en defect raken van Belastingdienstkaart/derdenpas/toegangspas/bezoekerspas
P&O N 1-1	I&I-1-19	Controle op formele vereisten bij aanstelling, benoeming en tewerkstelling

P&O N 1-2	I&I-1-20	Controle op onderzoek bij de aanstelling, benoeming en tewerkstelling
P&O N 1-3	I&I-1-21	Controle op afleggen ambtseed of belofte
P&O N 1-4	I&I-1-22	Controle op ondertekening geheimhoudingsverklaring extern personeel
P&O N 2-1	I&I-1-23	Controle op vastlegging taken, bevoegdheden en verantwoordelijkheden
P&O N 2-2	I&I-1-24	Controle op conflicterende functies
P&O N 2-3	I&I-1-25	Controle op roulatie
P&O N 2-4	I&I-1-26	Controle op het houden van toezicht op extern personeel
P&O N 3-1	I&I-1-27	Controle op informeren personeel over informatiebeveiligings- en integriteitsregels
P&O N 3-2	I&I-1-28	Controle op volgen verplichte trainings- en opleidingsprogramma's
P&O N 4-1	I&I-1-29	Controle op het classificeren van informatie
P&O N 4-2	I&I-1-30	Controle op clean desk policy
P&O N 5-1	I&I-1-31	Controle op hanteren procedure bij vertrek of functieverandering
P&O N 6-1	I&I-1-32	Controle op verrichten van nevenwerkzaamheden
P&O N 6-2	I&I-1-33	Controle op accepteren geschenken/uitnodigingen
P&O N 6-3	I&I-1-34	Controle op bekendheid met vertrouwenspersoon integriteit
P&O N 7-1	I&I-1-35	Controle op registratie en afhandeling informatiebeveiligings- en integriteitsrisico's
P&O N 7-2	I&I-1-36	Controle op registratie en afhandeling buitengewone voorvallen
P&O N 7-3	I&I-1-37	Controle op omgaan met bedreigingen door agressie en geweld
P&O N 8-1	I&I-1-38	Controle op gebruik en terbeschikkingstelling bedrijfsmiddelen
P&O N 8-2	I&I-1-39	Controle op verlening ontheffingen
INF N 1-1	I&I-1-40	Controle op gebruik toegestane informatiesystemen
INF N 1-2	I&I-1-41	Controle op goed gebruik informatiesystemen
INF N 2-1	I&I-1-42	Controle op vaststelling autorisatieprofielen
INF N 2-2	I&I-1-43	Controle op verleende toegangsrechten
INF N 3-1	I&I-1-44	Controle op toepassing VIV (incidentele/structurele informatieverstrekking)
	I&I-1-45	Controle op toepassing VIV (privacybescherming)
	I&I-1-46	Controle op toepassing VIV (Wet Openbaarheid Bestuur)
INF N-3-2	I&I-1-47	Controle op integriteit van gegevens
INF N 3-3	I&I-1-48	Controle op naleving voorschriften gebruik van e-mail en Internet-werkplek
INF N 3-4	I&I-1-49	Controle op back-up procedure

1.10 Onderhoud van het HIB-BBN

Beleid in het algemeen en beleid op het gebied van de informatiebeveiliging en integriteitsaspecten in het bijzonder is voortdurend aan verandering onderhevig. De veranderingen in de informatietechnologie en de veranderende bedreigingen, vragen van de Belastingdienst een alerte en anticiperende houding. De in dit handboek vastgestelde richtlijnen, normen en maatregelen dienen dan ook periodiek op hun inhoud en op hun uitvoerbaarheid te worden getoetst. Dit proces van control en beheer heeft een continu karakter.

Het HIB-BBN 2003 Belastingdienst is in nauwe samenwerking met vertegenwoordigers van de gehele Belastingdienst tot stand gekomen. Bij het onderhoud zullen uiteraard dezelfde partners worden betrokken, te weten vertegenwoordigers van de proceseigenaren met kennis op het gebied van informatiebeveiliging en integriteit.

De onderhoudsslag van dit document is nog tot stand gekomen onder verantwoordelijkheid van het ARG1-project HIB-BBN. Het project loopt tot en met 2002, daarna zal bij B/CPP de verantwoordelijkheid voor beheer en onderhoud zijn belegd.

2. Strategisch beleidskader

2.1 Het belang van informatiebeveiliging en integriteitsaspecten

De primaire- en ondersteunende processen van de Belastingdienst zijn in hoge mate afhankelijk van goed functionerende informatiesystemen. Schade aan gebouwen en/of installaties als gevolg van menselijke of natuurlijke invloeden, uitval van computers/netwerken, het in ongerede raken van gegevensbestanden of het onbevoegd kennis nemen, dan wel manipuleren van gegevens kunnen ernstige gevolgen hebben voor de continuïteit van de bedrijfsprocessen van de Belastingdienst en de persoonlijke levenssfeer van belastingplichtigen.

De genoemde afhankelijkheid wordt mede beïnvloed door technologische ontwikkelingen op het gebied van de informatievoorziening. Vergaande deconcentratie van apparatuur, programmatuur, gegevens en de daarmee gepaard gaande decentralisatie van het beheer, maar ook de koppeling tussen voorheen losstaande informatiesystemen, leiden tot complexe situaties met diffuse verantwoordelijkheden. De beschikbaarheid, integriteit en vertrouwelijkheid van informatie zijn derhalve van essentieel belang voor het behoud van het betrouwbare imago van de Belastingdienst. Naast infrastructurele/technische maatregelen is ook de houding en het gedrag van medewerkers een belangrijke factor. Een belastingplichtige moet er te allen tijde vanuit kunnen gaan dat zijn/haar gegevens in goede handen zijn.

De ontwikkelingen laten zich als volgt samenvatten:

Interne ontwikkelingen

- klantgerichte benadering betekent onder meer integratie van processen en daardoor een concentratie van taken bij één of enkele medewerkers;
- (steeds meer) werken in de actualiteit eist juistheid, volledigheid en tijdigheid van de gebruikte gegevens en processen;

Externe ontwikkelingen

- samenwerking met externe instellingen in het kader van fraudebestrijding. De vertrouwelijkheid van gegevens over of gebruikt bij het (fraude)onderzoek moeten zowel bij de Belastingdienst als bij de externe instellingen zijn gewaarborgd;
- toenemende elektronische gegevensuitwisseling met intermediairs en belastingplichtigen. Hierbij is van belang het waarborgen van de integriteit en de vertrouwelijkheid van de gegevens;
- toenemend elektronisch betalingsverkeer stelt hogere eisen aan de beschikbaarheid van de geautomatiseerde processen en gegevens;

Technologische ontwikkelingen

- toenemende automatisering in combinatie met decentralisatie van processen kan een verhoging van de risico's van het onbevoegd kennis nemen dan wel manipuleren van gegevens betekenen;
- standaardisatie van de gegevensuitwisseling betekent een verruiming van de koppelingsmogelijkheden waardoor de risico's van onbevoegde kennisneming bij gegevensuitwisseling toenemen.

Tenslotte is er ook het toenemend belang van de externe verantwoording. De omgeving van de Belastingdienst stelt steeds hogere eisen aan het afleggen van verantwoording over het gevoerde beleid en de uitvoering daarvan. Dat geldt zeker ook voor de aspecten informatiebeveiliging en integriteit.

Samengevat is het doel van informatiebeveiliging de risico's ten aanzien van integriteit, beschikbaarheid en vertrouwelijkheid van gegevens en van gegevensverwerkende processen te beheersen. Belangrijk is

dus dat binnen de Belastingdienst helder is wat het gewenste niveau van informatiebeveiliging en integriteit is.

2.2 Uitgangspunten

Bij het beschrijven van de normatiek voor regio's zijn de volgende uitgangspunten gehanteerd:

2.2.1 Basisbeveiligingsniveau en eventuele afwijkingen daarop

Het belang van de continuïteit van de bedrijfsprocessen en de privacybescherming vereisen voor de Belastingdienst een hoog niveau van informatiebeveiliging. De processen en gegevens zijn binnen de Belastingdienst vanuit een oogpunt van informatiebeveiliging voor een groot deel gelijkwaardig. Derhalve kiest de Belastingdienst ervoor het hoge niveau van informatiebeveiliging te effectueren met een set van richtlijnen en normen en een daarbij vereiste minimum basismaatregelenet. Hiermee is het hoge niveau van beveiliging dat de Belastingdienst nastreeft, tevens het basisbeveiligingsniveau. Voordeel hiervan is ook dat het basisbeveiligingsniveau met generieke beveiligingsmaatregelen kan worden ingevuld. Dit vereenvoudigt het beheer en beperkt de kosten.

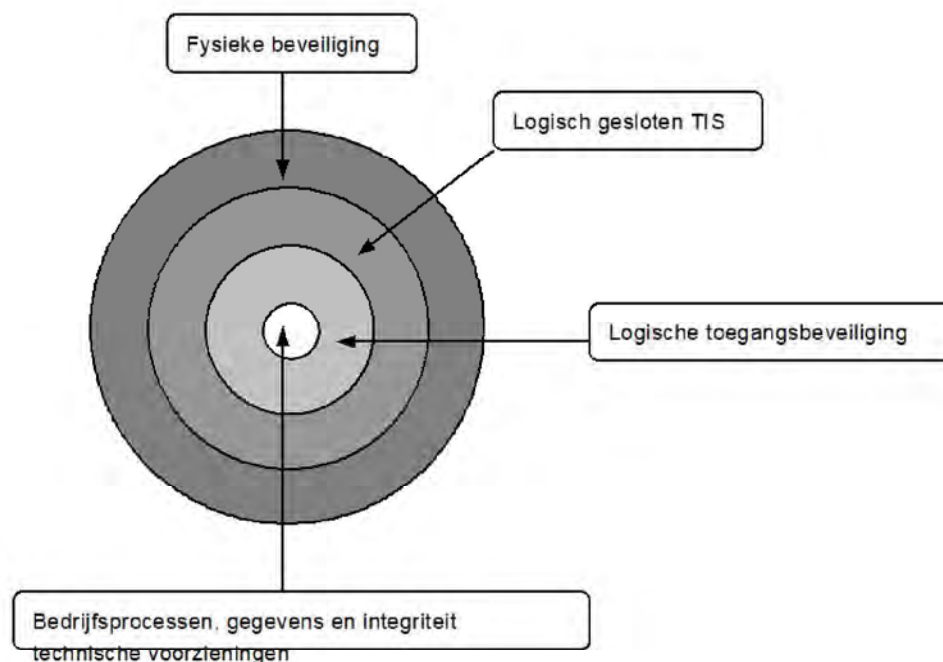
Per norm worden de maatregelen gegeven die nodig zijn om het basis beveiligingsniveau te halen. Afwijking van de maatregelen is mogelijk, doch slechts met een adequate onderbouwing van de redenen tot afwijking. Tevens zullen aanvullende of intensiever uitgevoerde maatregelen moeten worden getroffen teneinde de norm te halen.

2.2.2 Aanvaardbaar risico

Bij het ontwikkelen van de beveiligingsnormatiek is het begrip aanvaardbaar risico gehanteerd. Als uitgangspunt is genomen dat buitengewone voorvallen nooit kunnen worden uitgesloten; een "honderd procent-filosofie" is geen realistische norm. Wel dient gestreefd te worden naar het beheersen van de risico's tot op een aanvaardbaar niveau. Risico wordt daarbij gedefinieerd als het product van kans en gevolg. Daarbij moeten afwegingen worden gemaakt tussen risico's die wel en niet aanvaardbaar zijn in relatie tot de lasten die nodig zijn voor de vermindering van risico's. Het HIB-BBN is de vertaling van het aanvaardbaar risico.

2.2.3 Samenhang informatiebeveiligingsmaatregelen

De samenhang tussen de beveiligingsmaatregelen kan globaal worden beschreven met het zogenaamde "schillenmodel". Het model geeft weer dat te beveiligen objecten (gegevens, processen en technische voorzieningen) met behulp van een drietal algemene beveiligingsmaatregelen worden beschermd. Het model ziet er als volgt uit:

Figuur 2: Schillenmodel*Fysieke beveiliging*

De eerste beveiligingsschil wordt gevormd door de fysieke beveiliging. Deze is vooral gericht op het weren van onbevoegden uit de gebouwen van de Belastingdienst, primair ter bescherming van het handmatige deel van de gegevensverwerking. Hierbij ligt het accent op de aspecten beschikbaarheid en vertrouwelijkheid van de objecten. Onbevoegden mogen geen kennis nemen van de in de dossiers opgeslagen informatie en geen toegang krijgen tot de computerruimten en de daarin opgestelde apparatuur.

Logisch gesloten TIS

De tweede beveiligingsschil bestaat uit de logisch gesloten technische infrastructuur, die ervoor zorgt dat de gegevensuitwisseling binnen de Belastingdienst wordt geïsoleerd van de buitenwereld.

Uitwisseling van gegevens met systemen buiten de logisch gesloten TIS zal via een per situatie vastgestelde beveiligde en gecontroleerde wijze plaatsvinden.

Logische toegangsbeveiliging

De derde schil bestaat uit de logische toegangsbeveiliging: de gebruiker kan, nadat toegang tot de informatievoorziening van de Belastingdienst is verkregen, slechts beschikken over die toepassingen en gegevens, waarvoor hij of zij specifiek geautoriseerd is.

2.2.4 Analyse van verhoogde risico's

In de normatiek is uitgegaan van een 'standaard regio-eenheid', dat wil zeggen dat de normatiek is geënt op een standaardrisicoprofiel. Als gevolg van bijzondere omstandigheden kan binnen bepaalde onderdelen van de Belastingdienst een hoger risicoprofiel aanwezig zijn, dan waar in de normatiek vanuit is gegaan. Daarom wordt jaarlijks een analyse van verhoogde risico's uitgevoerd. Deze analyse bestaat uit de volgende drie onderdelen:

- Generieke analyse, Belastingdienstbreed;
- Vaststellen van een 'vermoeden van een verhoogd risico';
- Specifieke analyse per regio-eenheid.

De generieke analyse heeft tot doel Belastingdienstbreed inzicht te krijgen in de aanwezigheid of een vermoeden van een verhoogd risicoprofiel op het gebied van informatiebeveiliging en integriteit binnen (bepaalde onderdelen van) de Belastingdienst. Op grond van de uitkomsten van de generieke analyse wordt door de Groepsraad (en het Managementteam Belastingdienst) eventueel een 'vermoeden van een verhoogd risico' vastgesteld en eventuele generieke aanvullende maatregelen voorgeschreven.

Vervolgens wordt door iedere regio-eenheid de specifieke analyse uitgevoerd. Deze analyse heeft tot doel de regio-eenheid inzicht te bieden in de aanwezigheid van een verhoogd risicoprofiel op het gebied van informatiebeveiliging en integriteit. De uitkomsten van de gehele analyse van verhoogde risico's (generiek en specifiek) vormen voor de regio-eenheid een input voor het beveiligings- en integriteitsplan. Vervolgens worden de verbeteracties aan de hand van dit plan uitgevoerd.

2.3 Verantwoordelijkheden

2.3.1 Integraal management

Bij de Belastingdienst is informatiebeveiliging en integriteit als onderdeel van integraal management een verantwoordelijkheid van het management op de diverse niveaus in de organisatie. Concreet betekent dit dat de richtlijnen en normen voor informatiebeveiliging en integriteit uit het Handboek worden vastgesteld door de Groepsraad en het Managementteam Belastingdienst en dat uitwerking en uitvoering plaatsvindt in de lijn.

Het management op de diverse niveaus wordt ondersteund door deskundigen op het terrein van de informatiebeveiliging en integriteit die zijn opgenomen in de staf (sector PFC). In het kader van de informatiebeveiliging en integriteit zijn zij verantwoordelijk voor de ontwikkeling van de te hanteren kaders en de planning van en de control op de uitvoering.

Uitgangspunt is dus dat het lokale management van de regio-eenheden integraal verantwoordelijk is voor het niveau van informatiebeveiliging en de zorg voor integriteit binnen de regio-eenheid. Om deze verantwoordelijkheid te kunnen dragen is er binnen de regio-eenheid een zodanige planning- en controlcyclus ingericht dat het management van de regio-eenheid op basis daarvan de processen op een regio-eenheid kan beheersen.

Ten aanzien van door de regio-eenheid zelf uitgevoerde maatregelen wordt de juiste uitvoering daarvan gewaarborgd door een stelsel van (controle- en/of kwaliteits-) maatregelen en procedures en de rapportage daarover aan de leiding als basis voor (bij)sturing. Daarnaast heeft het lokale management de eindverantwoordelijkheid voor de producten/diensten die door ondersteunende diensten worden geleverd, (onder meer het B/CFD en B/CICT/DV). Deze verantwoordelijkheid krijgt gestalte door in een

Service Niveau Overeenkomst (SNO) het kwaliteitsniveau met de betreffende ondersteunende dienst af te spreken en de kwaliteit van de dienstverlening te bewaken met behulp van Service Niveau Rapportage (SNR). Op basis van deze rapportage en de ervaringen binnen de regio-eenheid krijgt het management een beeld van de wijze van nakoming van de afgesproken dienstverlening.

Inherent aan het uitgangspunt dat informatiebeveiliging een integrale managementverantwoordelijkheid is, komen de (extra) kosten van informatiebeveiliging en integriteit ten laste van de budgetten van de verantwoordelijke regio's en ondersteunende diensten. De financiering geschiedt daarmee via de reguliere budgetcyclus van de Belastingdienst.

Bij de ontwikkeling van nieuwe informatiesystemen en bij de voorbereidingen van investeringen in infrastructurele voorzieningen (hardware, datacommunicatie, gebouwen, inrichting) dient het niveau en de wijze van informatiebeveiliging een belangrijk aspect te zijn en daarmee een onderdeel van die investeringsbeslissing te vormen.

2.3.2 Delegeren van verantwoordelijkheden

In het HIB-BBN 2003 Belastingdienst is aan het Managementteam van een regio-eenheid een aantal taken toebedeeld. Een voorbeeld daarvan is het accorderen van de aanvraag voor het toekennen, muteren en intrekken van aanvullende logische toegangsrechten die buiten het standaardprofiel vallen. Het is vanzelfsprekend dat het Managementteam dergelijke verantwoordelijkheden kan delegeren aan een Belastingdienst-medewerker binnen de eigen regio-eenheid. Het principe van integraal management mag daarbij niet uit het oog verloren gaan.

2.4 Borging

2.4.1 Communicatie

Voor het realiseren van informatiebeveiliging en integriteit is het borgen van informatiebeveiliging en integriteit cruciaal. Het gaat naast technische maatregelen uiteindelijk vooral om het bewerkstelligen van gedragsbeïnvloeding bij medewerkers. Dat veronderstelt niet alleen bewustwording, kennis en vaardigheden, maar ook overtuiging en een welwillende houding ten aanzien van de onderwerpen risicobeheersing, gegevensbeveiliging en integriteit. Communicatie speelt hierbij een belangrijke rol. Om deze reden kiest de Belastingdienst voor een structurele periodieke voorlichting aan haar medewerkers. In de communicatie is een sleutelrol weggelegd voor de leidinggevenden. Zij zijn immers verantwoordelijk voor het stelselmatig bevorderen en stimuleren van het beveiligingsbewustzijn.

In de normatiek is dit uitgewerkt met het begrip 'actieve communicatie'. Actieve communicatie houdt o.a. in dat,

- het managementteam (MT) van een regio-eenheid de norm of maatregelen (bijv. een procedure) heeft goedgekeurd en;
- de norm of maatregel planmatig en gebaseerd op de organisatiespecifieke situatie onder de aandacht van de medewerkers is gebracht (via bijv. e-mail, nieuwsbrieven et cetera) en;
- de norm of maatregel minimaal wordt besproken binnen de diverse teamoverleggen, zoals blijkt uit de verslaglegging van deze overleggen.

Daarnaast moet uit navraag bij verschillende medewerkers blijken dat zij op de hoogte zijn van aan de norm of maatregel gerelateerde afspraken.

2.4.2 Toetsing

Conform het Voorschrift Informatiebeveiliging Rijksdienst (VIR) zullen de uit het informatiebeveiligings- en integriteitsbeleid voortvloeiende maatregelen worden getoetst op hun implementatie en werking.

De toetsing van de invoering van het beleid is een onderdeel van de reguliere planning en controlcyclus van de Belastingdienst. Jaarlijks wordt door elke regio-eenheid een Beveiligings- en integriteitsplan (BIP) opgesteld dat een overzicht geeft van de binnen de regio-eenheid uit te voeren activiteiten ter verbetering van de informatiebeveiliging en integriteit.

Het ARGI-project Certificering Informatiebeveiliging en Integriteitsaspecten (CI²) beoogt op het niveau van individuele regio's van de Belastingdienst jaarlijks een uitspraak te doen over de mate waarin een regio-eenheid invulling geeft aan de (beheersing van) informatiebeveiliging en (de zorg voor) integriteit. Het project staat niet op zich zelf, doch maakt deel uit van een integrale benadering van informatiebeveiliging, die past binnen de reguliere planning- en controlcyclus van de Belastingdienst. De Interne Accountantsdienst Belastingen (IAB) is gevraagd in het project CI² het voortouw te nemen.

3. HIB-BBN

3.1 Planning en Control

Inleiding

Informatiebeveiliging en integriteit verdienen continu de aandacht en moeten gestructureerd worden aangepakt. Beide onderwerpen dienen derhalve onderdeel uit te maken van de planning- en controlcyclus. Deze cyclus heeft niet alleen tot doel te toetsen of het gewenste beveiligings- en integriteitsniveau wordt gehaald, maar ook om tijdig in te kunnen spelen op veranderende omstandigheden en/of nieuwe ontwikkelingen en de daarmee gepaard gaande (nieuwe) risico's en bedreigingen.

In het kader van het principe van integraal management is het belangrijk dat het management acties op het terrein van de informatiebeveiliging en integriteit zelf ter hand neemt. Indien dit niet gebeurt wordt afbreuk gedaan aan een belangrijk uitgangsprincipe hetgeen een grotere reikwijdte heeft dan de uitvoering sec, namelijk het ontbreken van voldoende draagvlak en voorbeeldfunctie. In dit hoofdstuk wordt de planning- en controlcyclus voor informatiebeveiliging en integriteit nader uitgewerkt.

Verantwoordelijkheden Managementteam van de regio-eenheid

Het Managementteam van de regio-eenheid is verantwoordelijk voor het coördineren en bewaken van de uitvoering van de maatregelen op het gebied van informatiebeveiliging en integriteit binnen de regio-eenheid door middel van de planning- en controlcyclus.

Verantwoordelijkheden binnen de regio-eenheid voor Planning en Control

Managementteam van de regio-eenheid	Eindverantwoordelijk voor maatregelen binnen de regio-eenheid op het gebied van Planning & Control.
Leidinggevenden	Uitvoering taken gedelegeerd door Managementteam van de regio-eenheid en het afleggen van verantwoording over de uitvoering.
Functionaris belast met informatiebeveiliging	Adviserende rol bij het opstellen van het beveiligings- en integriteitsplan, BHV- en calamiteitenplan. Bewaking van de voortgang van de uitvoering van het BIP.

3.1.1 Planning en organisatie

Richtlijn

P&C R-1	<i>Het Managementteam van een regio-eenheid dient jaarlijks een beveiligings- en integriteitsplan voor de regio-eenheid op te stellen en zorg te dragen voor de uitvoering daarvan.</i>
---------	---

Risicoafweging

Als een regio-eenheid onvoldoende inzicht heeft in de verhoogde risico's die worden gelopen op het gebied van informatiebeveiliging en integriteit, bestaat het risico dat niet de juiste maatregelen worden getroffen om deze risico's te beheersen.

De regio-eenheid dient inzicht te hebben in verbeteringen die zij kan realiseren op het niveau van informatiebeveiliging en integriteit. Bij een niet structurele aanpak van deze verbeteringen, bestaat het risico dat deze verbeteringen niet (tijdig) worden gerealiseerd, bijvoorbeeld doordat het onduidelijk is wie verantwoordelijk is voor de uitvoering. Dit risico speelt ook bij de uitvoering van maatregelen door ondersteunende diensten, zoals B/CFD en B/CICT.

Norm

P&C N-1-1	Jaarlijks wordt een specifieke analyse van verhoogde risico's uitgevoerd waarbij wordt bepaald of de regio-eenheid verhoogde risico's loopt op het gebied van informatiebeveiliging en integriteit.
-----------	---

Maatregelen

- Bij het uitvoeren van de specifieke analyse wordt minimaal gebruik gemaakt van de volgende documentatie:
 - Vastlegging uitkomsten generieke analyse;
 - Vaststellen 'vermoeden van een verhoogd risico';
 - Vastlegging voorgeschreven aanvullende maatregelen;
 - Omgevingsanalyse(s) waarbij wordt bepaald of de gebouwen en/of installaties verhoogde risico's lopen op het gebied van informatiebeveiliging;
 - Risicoanalyse(s) uitgevoerd in het kader van Business Continuity Management (BCM);
 - Uitkomsten van conform norm P&C N-3-1 uitgevoerde interne controles;
 - Registratie van risico's en buitengewone voorvallen op het gebied van informatiebeveiliging en integriteit conform de normen P&O N-7-1 en P&O N-7-2;
 - Uitkomsten van door de IAB uitgevoerde certificeringsonderzoeken;
 - Uitkomsten van overige door de IAB uitgevoerde onderzoeken, zoals jaarrekeningcontroles, operational audits, etc.;
 - Uitkomsten van voorgaande specifieke analyses;
 - Rapportages van ondersteunende diensten over de geleverde dienstverlening;
 - Overige relevante informatie, zoals bijvoorbeeld uitkomsten van eigen uitgevoerde risicoanalyses.
 Deze documentatie wordt ook gebruikt als verwijzing ter onderbouwing van de antwoorden.
- De vragenlijst 'specifieke analyse' wordt voor de specifieke situatie van de regio-eenheid ingevuld, bijvoorbeeld door het houden van een brainstormsessie.
- De uitkomsten van de invulling van de vragenlijst worden besproken met de integraal management verantwoordelijke van de regio-eenheid.
- De rapportage van de specifieke analyse wordt formeel vastgesteld door het management team van de regio-eenheid.
- Indien er voor de regio-eenheid verhoogde risico's van toepassing zijn verklaard, wordt vastgelegd welke aanvullende maatregelen zijn getroffen om deze risico's te beheersen. Deze maatregelen worden opgenomen in het beveiligings- en integriteitsplan (zie P&C N-1-2) van de regio-eenheid.

Norm

P&C N-1-2	Jaarlijks wordt een beveiligings- en integriteitsplan (BIP) opgesteld dat een overzicht geeft van de binnen de regio-eenheid uit te voeren activiteiten ter verbetering van het niveau van informatiebeveiliging en integriteit.
-----------	--

Maatregelen

- In het BIP worden per aandachtsgebied (P&C, G&I, P&O en INF) de activiteiten vastgelegd ter realisatie van maatregelen die binnen de regio-eenheid nog moeten worden geïmplementeerd in het komende jaar. Deze activiteiten zijn gebaseerd op de resultaten en bevindingen van:
 - uitgevoerde interne controles (structurele verbeteractiviteiten) (zie P&C N-3-1);
 - de uitgevoerde Analyse Verhoogd Risico (zie P&C N-1-1);
 - tests op het BHV- en calamiteitenplan;
 - rapportages Testteam;
 - de registratie van risico's en buitengewone voorvallen op het gebied van informatiebeveiliging en integriteit (P&O N-7-1 en P&O N-7-2);
 - het eventueel uitgevoerde certificeringsonderzoek.
 - In het BIP wordt tevens aandacht besteed aan:
 - trainings- en opleidingsprogramma's op het gebied van informatiebeveiliging en integriteit (zie P&O N-3-2);
 - de wijze waarop binnen de regio-eenheid periodiek aandacht wordt geschonken aan informatiebeveiliging en integriteit (zie P&O N-3-1).
 - Per activiteit wordt vastgelegd wie verantwoordelijk is voor het (laten) realiseren daarvan. Daarbij wordt onderscheid gemaakt of de uitvoering ligt bij de regio-eenheid zelf of bij een ondersteunende dienst (B/CFD, B/CICT/DV, etc.). Ten aanzien van de door ondersteunende diensten te treffen maatregelen kan worden verwezen naar gemaakte SNO/SNR-afspraken (zie P&C N-2-1).
 - Per maatregel wordt vastgelegd:
 - de status van de maatregel;
 - de termijn waarbinnen de implementatie van de maatregel gerealiseerd wordt;
 - wie de actiehouders is voor de implementatie van de maatregel.
 - De functionaris belast met informatiebeveiliging vervult een adviserende rol ten aanzien van het BIP en brengt dit advies schriftelijk in.
 - Het Managementteam van de regio-eenheid accordeert formeel het beveiligings- en integriteitsplan. Hij wordt hierbij ondersteund door het advies van de functionaris belast met informatiebeveiliging.
- (Modellenboek HIB-BBN: BIP-template en BIP-toelichting)*

Norm

P&C N-1-3	De voortgang in de uitvoering van het beveiligings- en integriteitsplan (BIP) wordt zichtbaar bewaakt.
-----------	--

Maatregelen

- De functionaris belast met informatiebeveiliging stelt ten behoeve van het Managementteam van de regio-eenheid minimaal eenmaal per kwartaal een voortgangsrapportage op over de uitvoering van de in het beveiligings- en integriteitsplan opgenomen activiteiten.
 - De voortgangsrapportage wordt besproken in het managementoverleg van de regio-eenheid.
 - Indien maatregelen niet zijn gerealiseerd binnen de daartoe gestelde termijn, worden de actiehouders daarop aangesproken door het Managementteam van de regio-eenheid.
- (Modellenboek HIB-BBN: Voortgangsrapportage BIP)*

3.1.2 Uitbesteding

Richtlijn

P&C R-2	<i>Afspraken over uitbesteding van (onderdelen van) taken dienen schriftelijk te worden vastgelegd en bewaakt.</i>
---------	--

Risicoafweging

Indien er geen afspraken gemaakt worden over de uitbesteding van (onderdelen van) taken op het gebied van informatiebeveiliging en integriteit, bestaat het risico dat de dienstverlening niet aan de gewenste kwaliteit voldoet. Tevens wordt het risico gelopen dat de regio-eenheid niet wordt geïnformeerd over de uitvoering van uitbestede taken.

Norm

P&C N-2-1	Afspraken over (interne) dienstverlening (uitbesteding van (onderdelen van) taken) zijn schriftelijk vastgelegd in actuele Service Niveau Overeenkomsten (SNO's).
-----------	---

Maatregelen

- Op de regio-eenheid is een overzicht aanwezig van alle vormen van uitbesteding en mandatering (bij mandatering wordt de verantwoordelijkheid gelegd bij de dienstverlenende en bij uitbesteding blijft de verantwoordelijkheid bij de regio-eenheid zelf) van taken waarbij duidelijk is aangegeven:
 - met wie een SNO is afgesloten;
 - de datum waarop de SNO is afgesloten;
 - met wie geen SNO is afgesloten met vermelding van de reden en op welke wijze de afspraken dan zijn vastgelegd.
- Bij (interne) dienstverlening (uitbesteding van (onderdelen van) taken of mandatering) worden afspraken jaarlijks vastgelegd in een SNO.
- Voor het maken van afspraken over de standaarddienstverlening wordt gebruik gemaakt van het model SNO. Hierin wordt een verwijzing opgenomen naar een document waar de maatregelen binnen de standaarddienstverlening zijn beschreven.
- In de SNO worden expliciet afspraken gemaakt over:
 - de periodieke rapportage (Service Niveau Rapportage - SNR) over de uitvoering van de dienstverlening (vorm, inhoud, frequentie, verspreiding, etc.);
 - de wijze waarop zekerheid wordt verkregen over de betrouwbaarheid van de uitvoering van de uitbestede taken (bijvoorbeeld interne controle door de dienstverlener, SNR's);
 - de verantwoordelijkheden en aansprakelijkheden van de regio-eenheid en de dienstverlener.
- Indien in de dienstverlening aanvullende diensten worden overeengekomen, bijvoorbeeld op basis van voor de regio-eenheid specifieke zaken, worden deze expliciet in de SNO-specificatie opgenomen, waarbij wordt vastgelegd:
 - aan welke minimale norm de aanvullende diensten moeten voldoen;
 - welke beveiligingsmaatregelen daarbij in acht moeten worden genomen;
 - welke prestatie-indicatoren worden gehanteerd om te meten of aan de norm wordt voldaan;
 - op welke wijze over de aanvullende dienstverlening wordt gerapporteerd.
- De SNO(-specificatie) wordt geaccordeerd door het Managementteam van de regio-eenheid.

(Modellenboek HIB-BBN: SNO – Aandachtspunten)

Norm

P&C N-2-2	Er wordt periodiek overleg gevoerd met de ondersteunende diensten over de gerealiseerde dienstverlening aan de hand van Service Niveau Rapportages (SNR's) en er wordt zichtbaar vervolg gegeven aan de uitkomsten daarvan.
-----------	---

Maatregelen

- Periodiek (minimaal twee keer per jaar) wordt door of namens het management van de regio-eenheid overleg gevoerd met de ondersteunende diensten over de gerealiseerde dienstverlening aan de hand van schriftelijke rapportages (SNR's).
- De belangrijkste uitkomsten van het overleg worden vastgelegd in een besprekingsverslag.
- Er wordt een overzicht opgesteld van door de ondersteunende dienst en door de regio-eenheid uit te voeren actiepunten en deze wordt opgenomen als bijlage van het besprekingsverslag.
- Er wordt vastgelegd op welke termijn actiepunten moeten zijn afgehandeld.
- Het management van de regio-eenheid bewaakt de tijdige afhandeling van actiepunten.

(Modellenboek HIB-BBN: SNR – Aandachtspunten)

3.1.3 Beheersing

Richtlijn

P&C R-3	<i>Het Managementteam van de regio-eenheid dient de uitvoering van de maatregelen op het gebied van informatiebeveiliging en integriteit te beheersen als een integraal onderdeel van zijn managementtaak.</i>
---------	--

Risicoafweging

De uitvoering van beveiligings- en integriteitsmaatregelen heeft het Managementteam van de regio-eenheid doorgaans gedelegeerd aan anderen binnen de regio-eenheid of uitbesteed aan ondersteunende diensten buiten de regio-eenheid. Het risico bestaat dat maatregelen niet naar behoren worden uitgevoerd of niet effectief zijn. Aangezien het Managementteam van de regio-eenheid verantwoordelijk blijft voor de uitvoering van maatregelen, zal hij voor de beheersing daarvan, interne controles (laten) uitvoeren. Een onvoldoende beheersing van de uitvoering van maatregelen kan ertoe leiden dat de regio-eenheid hogere risico's loopt dan aanvaardbaar wordt geacht.

Norm

P&C N-3-1	Er worden planmatig interne controles uitgevoerd die gericht zijn op de toetsing van de juiste uitvoering van beveiligings- en integriteitsmaatregelen.
-----------	---

Maatregelen

- De uitvoering van interne controles op het gebied van informatiebeveiliging en integriteit wordt als onderdeel van de algehele IC-uitvoering ingepland. Wijzigingen die de regio-eenheid hanteert op het Intern Controleprogramma 'Beheer van Informatiebeveiliging en Integriteit' (I&I) worden afgestemd met de Interne Accountantsdienst Belastingen (IAB).
- Het Intern Controle Programma (ICP) 'Beheer informatiebeveiliging en integriteit' wordt uitgevoerd door medewerkers binnen de regio-eenheid die niet betrokken zijn bij de uitvoering van maatregelen.
- De tijdige uitvoering van het ICP wordt bewaakt binnen het PFC-team.
- Er worden rapportages van de uitgevoerde interne controle opgesteld waarbij de opgenomen bevindingen zijn afgestemd met de betrokkenen.
- De interne controle rapportages worden binnen het PFC-team beoordeeld waarbij wordt bepaald of de resultaten aanleiding geven tot korte termijn dan wel structurele verbeteracties.
- De uit te voeren verbeteracties worden gerapporteerd en besproken in het managementoverleg binnen de regio-eenheid.
- In de management verslagen wordt vastgelegd op welke termijn actiepunten moeten zijn afgehandeld.
- De functionaris belast met informatiebeveiliging bewaakt de tijdige afhandeling van vastgestelde actiepunten.

(Modellenboek HIB-BBN: IC-planning en rapportage, Registratie afwijkingen MS en ICP)

Norm

P&C N-3-2	De taken en verantwoordelijkheden op het gebied van informatiebeveiliging en integriteit binnen een regio-eenheid zijn belegd.
-----------	--

Maatregelen

- De taken en verantwoordelijkheden op het gebied van informatiebeveiliging en integriteit binnen een regio-eenheid zijn vastgelegd en goedgekeurd door het Managementteam. Hierbij dient aandacht te zijn besteed aan taken als coördineren, adviseren, uitvoeren en controleren van informatiebeveiliging en integriteit.
- Specifiek coördinerende taken en verantwoordelijkheden op het gebied van informatiebeveiliging en integriteit zijn toegekend aan een (of meer) medewerker(s) binnen de regio-eenheid.

3.1.4 Continuïteit van de organisatie

Richtlijn

P&C R-4	<i>Het Managementteam van de regio-eenheid draagt zorg voor het, in afstemming met de ondersteunende diensten, treffen van maatregelen ter waarborging van de continuïteit van de bedrijfsprocessen.</i>
---------	--

Risicoafweging

Door het ontbreken van een calamiteitenorganisatie is het mogelijk dat de bewoners van een pand niet op de hoogte zijn van maatregelen en/of voorzieningen ingeval van calamiteiten. Hierdoor kan schade ontstaan bij medewerkers(bewoners) en aan apparatuur waardoor de beschikbaarheid en continuïteit van de primaire processen in gevaar kan komen. Een onderbreking van de primaire processen kan grote financiële en mogelijk personele gevolgen hebben.

N.B.: Op het moment van de update van het HIB-BBN 2001 Eenheden was B/CPP bezig met het analyseren en aanpassen van het HCB. In de loop van 2003 zal dit leiden tot een aangepast HCB met onderliggende modellen.

Norm

P&C N-4-1	Er is een Bedrijfs Hulp Verlenings (BHV) organisatie ingericht voor het in veiligheid brengen van personen in geval van calamiteiten.
-----------	---

Maatregelen

- In nauw overleg met B/CFD, eventuele mede-gebouwbewoners en eventueel lokale hulpverleningsdiensten wordt op het niveau van een gebouw een BHV-organisatie ingericht.
- De BHV-organisatie is beschreven in een BHV-plan waarbij gebruik wordt gemaakt van het sjabloon uit het Modellenboek HIB-BBN 2003 Belastingdienst.
- In het BHV-plan is duidelijk aangegeven:
 - op welk moment of bij welke gebeurtenissen het BHV-plan in werking moet treden;
 - wie verantwoordelijk is voor het in werking stellen van het BHV-plan;
 - welke verantwoordelijkheden de regio-eenheid en B/CFD hebben in het kader van BHV;
 - welke taken medewerkers in het kader van BHV hebben;
 - aan welke medewerkers de taken binnen de BHV-organisatie zijn toebedeeld.
- De inrichting van de BHV-organisatie en de inhoud van het BHV-plan is bekend gemaakt aan de leden van de BHV-organisatie.
- Voor alle medewerkers is een instructiekaart beschikbaar die aangeeft hoe gehandeld moet worden bij (naderende) calamiteiten.
- De functionaris belast met informatiebeveiliging vervult een adviserende rol ten aanzien van het BHV-plan en brengt dit advies schriftelijk in.
- Het Managementteam van de regio-eenheid accordeert formeel het BHV-plan. Hij wordt hierbij ondersteund door het advies van de functionaris belast met informatiebeveiliging.
- Het Managementteam van de regio-eenheid wijst een verantwoordelijke aan die zorgdraagt voor het actueel beheer en onderhoud van het BHV-plan.
- Bij inwoning van (delen van) de organisatie bij derden buiten de Belastingdienst blijft het de verantwoordelijkheid van de regio-eenheid om de BHV-organisatie zoveel als mogelijk conform deze norm in te richten. Daarbij dient aangesloten te worden bij de BHV-organisatie van deze derde, de hoofdbewoner. De BHV-organisatie van de hoofdbewoner wordt beoordeeld op de mate waarin wordt voldaan aan bovenstaande maatregelen. Indien de BHV-organisatie van de hoofdbewoner niet voldoet, dient de regio-eenheid al het mogelijke te doen om de omissies in de BHV-organisatie teniet te doen.

(Modellenboek HIB-BBN: Alarmkaart, BHV-plan, Ontruimingsplan)

Norm

P&C N-4-2	Er is een calamiteitenorganisatie ingericht die zich richt op de waarborging van de continuïteit van het primaire proces.
-----------	---

Maatregelen

- In nauw overleg met B/CICT, B/CFD, eventuele mede-bewoners van het gebouw en eventueel lokale hulpverleningsdiensten wordt op het niveau van de regio-eenheid een calamiteitenorganisatie ingericht die minimaal bestaat uit een:
 - calamiteiten managementteam;
 - schade inventarisatieteam;
 - recoveryteam.
- De calamiteitenorganisatie is beschreven in een calamiteitenplan dat bestaat uit de volgende onderdelen:
 - preventieplan;
 - ontruimingsplan (hierbij kan worden verwezen naar het BHV-plan, waarin dit als onderdeel kan zijn opgenomen);
 - continuïteitsplan;
 - herstelplan.

Hierbij kan gebruik worden gemaakt van de handreikingen die voor deze plannen worden gegeven in het Handboek Calamiteitenplan Belastingdienst (HCB) en het Modellenboek HIB-BBN 2003 Belastingdienst. Tevens dient daarbij rekening te worden gehouden met de Maximaal Toegestane Uitvalsduur (MTU) van processen, zoals deze is vastgesteld door de voormalige Directieraad op 20 december 2001.

- Per team is de bemensing en de toewijzing van taken en verantwoordelijkheden vastgelegd. Per onderdeel c.q. plan zijn de uit te voeren maatregelen beschreven en deze zijn gekoppeld aan de taken en verantwoordelijkheden.
- In het calamiteitenplan is duidelijk aangegeven op welk moment of bij welke gebeurtenissen het calamiteitenplan in werking moet treden en wie verantwoordelijk is voor het nemen van deze beslissing.
- De inrichting van de calamiteitenorganisatie en de inhoud van het calamiteitenplan is bekend gemaakt aan de leden van de calamiteitenorganisatie.
- Voor alle medewerkers is een instructiekaart beschikbaar die aangeeft hoe gehandeld moet worden bij (naderende) calamiteiten.
- De functionaris belast met informatiebeveiliging vervult een adviserende rol ten aanzien van het calamiteitenplan en brengt dit advies schriftelijk in.
- Met ondersteunende diensten (zoals B/CFD en B/CICT) zijn afspraken gemaakt en vastgelegd in een SNO over het uitvoeren van (onderhouds)werkzaamheden. (Onderhouds)werkzaamheden moeten zodanig worden uitgevoerd dat deze de normale werkprocessen zo min mogelijk onderbreken, hinderen of verstoren.
- Het Managementteam van de regio-eenheid accordeert formeel het calamiteitenplan. Hij wordt hierbij ondersteund door het advies van de functionaris belast met informatiebeveiliging.
- Het Managementteam van de regio-eenheid wijst een verantwoordelijke aan die zorgdraagt voor het actueel beheer en onderhoud van het calamiteitenplan.

(Handboek Calamiteitenplan Belastingdienst)

Norm

P&C N-4-3	Periodiek wordt de werking van de BHV- en calamiteitenorganisatie getest en geëvalueerd.
-----------	--

Maatregelen

- Minimaal één keer per jaar worden alle onderdelen van de BHV- en calamiteitenplannen getest op de goede werking.
- Het testen vindt in nauw overleg plaats met B/CICT, B/CFD, eventuele mede-gebouwbewoners en eventuele externe hulpverleningsdiensten.
- Voor de gekozen onderdelen zijn specifieke testplannen opgesteld.
- Eventueel worden SNO-afspraken gemaakt met B/CFD en/of B/CICT over het testen van het BHV- en/of calamiteitenplan.
- Het Managementteam van de regio-eenheid is verantwoordelijk voor (laten) uitvoeren van de tests.
- Van de test wordt een evaluatierapportage opgemaakt, waarbij tevens een relatie wordt gelegd met die onderdelen van het plan die niet getest zijn. Ten behoeve van het actueel houden van deze plannen worden eventuele tekortkomingen in de BHV- en calamiteitenplannen aangepast.

3.2 Gebouwen en Installaties

Inleiding

De fysieke beveiliging is gericht op het weren van onbevoegden uit de gebouwen en installaties van de Belastingdienst en op het beschikbaar zijn en blijven van de gebouwen en vitale technische voorzieningen om een ongestoorde procesgang te waarborgen. Uitgangspunt hierbij is dat onbevoegden geen toegang hebben tot de in de gebouwen opgeslagen gegevens en geen toegang krijgen tot de (computer)ruimten en de daarin opgestelde apparatuur.

Verantwoordelijkheden Managementteam van de regio-eenheid

Het Managementteam van de regio-eenheid is verantwoordelijk voor de vaststelling of de standaard dienstverlening, zoals verleend door B/CFD voor gebouwen en installaties, voldoende is voor de specifieke situatie van de regio-eenheid. Op basis van deze vaststelling komt het Managementteam van de regio-eenheid met B/CFD tot overeenstemming over de te treffen beveiligingsmaatregelen. Het uitgangspunt daarbij is het Basis beveiligingsniveau (BBN).

Daarnaast is het Managementteam van de regio-eenheid verantwoordelijk voor het gedrag van de eigen medewerkers met betrekking tot de gebouwen en installaties.

NB: Indien aan de regio-eenheid geen dienstverlening door B/CFD plaatsvindt, is het Managementteam van de regio-eenheid verantwoordelijk voor het realiseren van minimaal hetzelfde niveau van maatregelen, zoals die in de standaard dienstverlening van B/CFD zijn vastgelegd. Het Managementteam van de regio-eenheid treedt hiertoe in overleg met de teamleider van het B/CFD, waaronder zijn regio-eenheid resulteert.

Verantwoordelijkheden binnen de regio-eenheid voor gebouwen en installaties

Managementteam van de regio-eenheid	Eindverantwoordelijk voor beveiligingsmaatregelen binnen de regio-eenheid op het gebied van gebouwen en installaties
Direct leidinggevende	Uitvoering taken gedelegeerd door Managementteam van de regio-eenheid
Medewerker	Zorgvuldig gebruik van gebouwen en installaties, dat wil zeggen: • goed huisvaderschap; • gebruik van gebouwen conform de doelstelling waarvoor ze zijn ingericht; • gebruik van installaties conform de instructies die daarvoor zijn gegeven.
Functionaris belast met informatiebeveiliging	Toetsen van en adviseren over toekenning (speciale) bevoegdheden en ontheffingen