

(3) Er wordt een e-mail door een belastingdienstmedewerker aangemaakt met daarin twee Excel bijlages waarin overzichten met metadata over intracommunautaire Prestaties (ICP) van verschillende kantoren. Deze e-mail wordt verzonden naar een andere Belastingdienstmedewerker welke de e-mail op haar beurt doorzet naar buiten. Deze laatste actie is verdacht. Hier wordt geen data van burgers en of bedrijven gedeeld. Het betreft een overzicht met de prestaties van kantoren.

- Van de ruim 105.000 pogingen connectie te maken met het internet worden er ruim 12.000 geblokkeerd. De 3 users die de meeste blokkades kregen (288, 278 en 257 Blocks) zijn nader onderzocht. De handelingen van de medewerker zijn door de onderzoeker geclassificeerd als experimentele handelingen zonder dat er data naar buiten is gebracht.
- Content servers worden vooral gebruikt om te downloaden. Geen verdachte upload activiteiten waargenomen.
- Het scannen van een aantal bijzondere blue coat categorieën levert niets bijzonders op (verdachte en illegale sites).
- Er zijn veel pogingen om een file storage faciliteit op internet te bereiken. 594 van de 642 pogingen zijn geblokkeerd. De resterende 48 geslaagde pogingen gebruiken de volgende file storage sharing faciliteiten:

dropbox.com
scribd.com
google.com
icloud.com
filepicker.io
dropboxusercontent.com
wetransfer.net
backblaze.com
capgemini.com
live.com
google.nl
wikimedia.org
huddle.com
getfilecloud.com
github.com

Bovenstaande externe voorzieningen worden vooral gebruikt om data op te halen. De hoeveelheid data die naar buiten wordt gebracht is te verwaarlozen en kan verklaard worden als invulling van een communicatieprotocol.

Inspectie, controle, toezicht

6.3.4. 'Standalone' onderzoek: 2012 PoC Accenture

De doelstelling van deze PoC was: ontwikkel een voorspellend model voor niet compliant gedrag van belastingplichtigen (preparation: 12-4-2012 – final document: 28-8-2012. Tot en met oktober 2012 nog evaluatie).

Het onderwerp van het onderzoek naar deze standalone: het ten onrechte buiten de Belastingdienst brengen en oneigenlijk gebruik van gegevens

Bevindingen

- De gebruikte server voor de PoC was de [inspectie, controle, toezicht] en was fysiek geplaatst binnen het rekencentrum van de Belastingdienst. Ook vindt er registratie in ITSM (service tool voor B/CIE) voor deze server plaats. Het betrof dus *geen standalone*.
 - (1) De server wordt met het beëindigen van de PoC Accenture niet meteen opgeheven.
 - (2) Van de opruiming van data en software van de PoC Accenture hebben we geen evidence aangetroffen.
 - (3) Accenture benoemt het opruimen van de omgeving wel in de startmeeting van 11 april 2012.
- Beperkt beheer werd door B/CIE uitgevoerd. De belangrijkste taken waren het maken van een back-up, toegangsbeheer en een initiële inrichting. Daarnaast een best effort voor incidentmeldingen. Verdere inrichting van de server werd door medewerkers van Accenture gedaan.
- De PoC Accenture kende een gedoogstatus bij B/CIE en dit is later (december 2012, dus achteraf) geformaliseerd in een: 'Maatwerkafspraken'. In de maatwerkafspraken wordt onder andere het beveiligingsprobleem bij de afnemende partij (B/CA) belegd.
- In 2013 spreekt de Rijksinspectie de Belastingdienst in 2013 vertrouwelijk aan op de voor deze PoC gebruikte server. 'Op het systeem [inspectie, controle, toezicht] zijn fiscale gegevens benaderbaar op een [inspectie, controle, toezicht] zonder authenticatie/authorisatie.' Dat wil zeggen dat iedereen die de correcte link heeft kan bij deze fiscale data. Deze melding komt voort uit de KWAS-rapportage waarvoor de Ministerraad de opdrachtgever was en de rijksinspectie de uitvoerende partij. De analyse van het probleem is: 'Verouderde server inrichting'. Daarnaast is ook in een interview bevestigd dat: 'De beveiliging van de AWS'en was niet op orde.'
- Voor deze PoC is data uit bronsystemen van de Belastingdienst gebruikt. Waarbij gold: 'De klant is zelf verantwoordelijk voor het plaatsen van bestanden in de betreffende omgevingen. Hiervoor hebben vertegenwoordigers van de klant de noodzakelijke autorisaties ontvangen.'
- Voor data & datatransporten geldt het volgende.
 - (1) Vastgesteld is dat er meerdere manieren van datatransport gebruikt zijn: RAM en Wisselland. Daarnaast is er rechtstreeks data geplaatst op de [inspectie, controle, toezicht] waarschijnlijk met FTP. Data werd geplaatst middels opdrachten via e-mail en werkopdrachten via [inspectie, controle, toezicht]. Overdracht van data via HDD is niet vastgesteld en lijkt ook niet waarschijnlijk vanwege de hardware welke bij B/CIE geplaatst is.
 - (2) In Harvest zijn 6 opdrachten uit september 2012 aangetroffen welke bevestigen dat data uit de bronsystemen van de Belastingdienst worden gehaald en richting de PoC Accenture geleverd moet gaan worden voor een refresh. Deze opdracht is de administratieve vastlegging van dit feit maar bevat niet de manier waarop deze data overdracht uiteindelijk is gedaan.
 - (3) Vastgesteld is dat de volgende data gebruikt is uit Belastingdienst bronsystemen: [inspectie, controle, toezicht] [inspectie, controle, toezicht] en Toeslagen. De data is niet versleuteld. Er geen indicatie dat deze lijst volledig is. De oorspronkelijke vraaglijst aan data is aanzienlijk langer.
 - (4) De levering van metadata over de data (begrip toekennen aan de velden) is een issue en het is niet inzichtelijk geworden hoe dit is geleverd.
- Voor toegangsrechten tot de data en systemen is een proces ingericht via een loket. Er is vastgesteld dat dit loket ook daadwerkelijk gebruikt is voor de toekenning van rechten.
- In de periode 18 tot en met 27 juni 2012 hebben alleen beheerders in het systeem ingelogd.
- De combinatie van een anonieme netwerkshare en het niet ingelogd zijn van medewerkers voor meer dan een week maakt het gebruik van de netwerkshare waarschijnlijk.
- Er is gebruik gemaakt van functionele user-id voor het laden van fiscale data (mei en juni 2012) in de PoC Accenture omgeving. Functionele users zorgen voor een ontkoppeling met de feitelijke gebruiker.
- De [inspectie, controle, toezicht] is bekend vanaf 9-6-2012 en buiten dienst vanaf 27-1-2015.

Niet vastgesteld is dat er data via dit project naar buiten is gelekt of oneigenlijk is gebruikt. Wel vastgesteld dat er hoge risico's werden gelopen.

Inspectie, controle, toezicht

6.3.5. Standalone onderzoek: 2013 Labtest OB-Carrousel Fraude

Labtest t.b.v. nieuwe manier van werken die bijdraagt aan het effectiever en efficiënter opsporen van fraudeurs, zowel bij gebruik van historische als bij het gebruik van actuele data.

Betrokken leverancier: CAP Gemini

Fase 1 maart-oktober 2014, fase 2 juli 2014 tot eind 2015

- NB1. Tijdens de uitvoering van dit onderzoek zijn we gestuit op een stukje: 'mogelijke relevante evidence'. Het betreft een backup van een NAS welke gebruikt is in deze LAB omgeving (de backup is niet encrypted). Nader onderzoek naar deze Back-up wordt, vanwege een krappe planning, uitgevoerd na uitvoering van de geplande onderzoeksmogelijkheden.
- NB2. Daarnaast zijn er tijdens het onderzoek loggings gevonden van de SNA server (Social Network analyser). Deze server is een migratie van de LAB omgeving zoals we deze hier onderzoeken naar een in eigen beheer genomen OB-carrousel omgeving. Daarmee valt deze logging buiten de 3 als risicovol geduide projecten cq. standalone's.

Het onderwerp van het onderzoek naar deze standalone: het ten onrechte buiten de Belastingdienst brengen en oneigenlijk gebruik van gegevens.

Bevindingen.

- Initieel kan de omgeving als standalone betiteld worden. Standalone is in dit geval een separaat subnetwerk met daarin een (SAS)server, NAS, router, 6 werkplekken en 2 beheerwerkplekken.
- Een formele goedkeuring voor het gebruik van SAS servers en SAS software en overige hardware hebben we niet aangetroffen.
- Sponsor voor fase 1 is onbekend en voor fase 2 van het project is dit Persoonsgegevens
- Persoonsgegevens Dit blijkt uit een SAS PVA waarin dit een randvoorwaarde is.
- Bestuurlijke aandacht:
 - (1) Focus bestuurlijke aandacht ligt op de inhoud van OB carrousel; het resultaat.
 - (2) Bestuurlijke aandacht voor de *inzet van BD vreemde machines* en infrastructuur is niet aangetroffen. Resultaat: geen risico inventarisatie en mogelijke mitigerende maatregelen aangetroffen. Bijvoorbeeld : geen beeld hoe er wordt omgesprongen met een risicovolle maar bijna 'compulsory' cq. verplichtte internetconnectie voor de standalone omgeving? Verplicht vanwege de vele updates die via internet worden verspreid. En als die internet connectie er ligt hoe wordt voorkomen dat fiscale data daar weglekken.
 - (3) Bestuurlijke aandacht voor de *inrichting van standalone omgeving* met gebruikte software was er niet. Resultaat bijvoorbeeld: inzet van werkplekken waar gebruikers admin rechten hebben en zelf USB en WIFI zaken konden regelen.
 - (4) Bestuurlijke aandacht voor de *inzet van SAS als beheerder* van de standalone machines met fiscale data is niet aangetroffen. Ook hier geen risico inventarisatie en/of mitigerende maatregelen aangetroffen. Resultaat bijvoorbeeld: geen toezicht op de taken van de SAS beheerders door de ICS beheerders.
 - (5) Pas achteraf na afronding van deze POC is er bestuurlijke aandacht voor de infrastructuur van OB-carrousel waarbij goedkeuring voor financiering van een versie van OB-carrousel binnen de BD-omgeving gevraagd wordt. Dit betreft een migratie van de LAB omgeving (standalone) naar een BD omgeving.
- Aandacht voor beveiliging van de fiscale gegevens aan de ons verstrekte documenten komt vooral vanuit SAS, de leverancier van de servers welke bij de BD worden ingezet. Deze aandacht is er in de vorm van ontwerpen (met aandacht voor functie scheiding) en mailtjes over schoning als SAS de hardware wil ophalen.
- Met een koppeling van de standalone omgeving aan de BD omgeving via een extra (tweede) NAS kan deze niet meer als standalone betiteld worden en worden nieuwe risico's zonder een formele vastlegging en besluit genomen. Een waarneming terplekke (HG 5 zesde verdieping) door een CIE medewerker leidt ertoe dat een zeer risicovolle situatie gemitigeerd wordt door de inzet van een firewall.

- Data overdracht vindt zowel direct via een gekoppelde NAS server plaats. Deze worden uitgevoerd door de ISC beheerders in samenwerking met B/CA. Ook wordt een harddisk voor overdracht gebruikt ook nog ten tijde van de directe koppeling.
- Waargenomen risico's, het volledig uit handen geven van beheer en het gebruik van servers zonder toezicht of mitigerende maatregelen.
 - (1) Onzekerheid wie er aan de fiscale data komt: geactiveerde gebruikers van de standalone omgeving kunnen afwijken van de ontwerpen zonder dat dit door de BD wordt waargenomen.
 - (2) Onzekerheid of fiscale data niet lekt: werkplekken gekoppeld aan de standalone omgeving (welke fiscale data bevat) kunnen middels WIFI en/of USB data downloaden naar eigen devices (mobile, harddisk, USB-sticks), zonder dat dit door de BD wordt waargenomen.
 - (3) Onzekerheid over inrichting van de server, Inbreng SAS servers zonder toezicht op implementatie conform ontwerp.
 - (4) Bescherming fiscale gegevens bij een koppeling van het LAB aan internet. Dit laatste is sowieso nodig voor de broodnodige updates.
 - (5) Besmetting BD vanuit een LAB-Tis¹⁷ omgeving door een koppeling aan de BD-Tis.
- Opruimen LAB omgeving; geen formele vastleggingen en constatering dat schoning juist is uitgevoerd. Wel informele communicatie in de vorm van mails hierover aangetroffen. Vanwege het feit dat het een SAS server betreft en deze weer door SAS weer wordt meegenomen is een juiste schoning extra kritisch.

6.3.6. Standalone onderzoek: 2014 Labtest Fraude OB-negatief

Doelstelling van dit project: IBM zal op basis van historische, geanonimiseerde data een model ontwikkelen, mede op basis van de IBM advanced analytici; oplossingen uit Denemarken (SKAT), dat negatieve OB aangiftes zal kunnen prioriteren op de kans op fraude.

Betrokken leverancier: IBM.

Periode: mei 2014 - augustus 2014

Het onderwerp van het onderzoek naar deze standalone: het ten onrechte buiten de Belastingdienst brengen en oneigenlijk gebruik van gegevens

Bevindingen

- Er is voor de Labtest Fraude OB Negatief een omgeving gebruikt die los stond van de Belastingdienst omgeving (standalone bij IBM). IBM was in dit onderzoek betrokken om een model te ontwikkelen en heeft voor deze Labtest een tijdelijke data analyse omgeving ingericht bij IBM waar de IBM consultants op konden werken.
- Aangegeven is dat gegevens van ondernemers zoals aangiftes, teruggaven, verminderingen, rechtsvorm en branche ten behoeve van deze Labtest op de AWS van BI&A zijn geselecteerd en geanonimiseerd (FInr) en vervolgens zijn gedeeld met IBM.
- Transport van de data via: USB en harde schijven.
- De Broedkamer is betrokken bij het selecteren van data uit de Belastingdienstsystemen en het anonimiseren van gegevens alsmede het transport ervan naar IBM. Niet duidelijk is geworden hoe dit transport heeft plaatsgevonden.
- In de overeenkomst met IBM is afgesproken de data van de Belastingdienst door de Belastingdienst zal worden geanonimiseerd en dat IBM de gebruikte omgeving zou gaan beveiligen en de gegevens van de ondernemers na afronding van de Labtest door IBM zou worden vernietigd. Niet vast kunnen stellen of vernietiging ook is gedaan.
- In opzet zijn er maatregelen doorgevoerd om de vertrouwelijkheid van de met IBM gedeelde gegevens te borgen. Dit blijkt uit de gemaakte afspraken en toegezonden documenten.
- We hebben geen vastleggingen ontvangen waarmee aangetoond wordt dat de maatregelen volledig en juist hebben gewerkt. Een proces verbaal van vernietiging van de Belastingdienstgegevens is bijvoorbeeld niet ontvangen.

¹⁷ Technische Infrastructuur

Niet vastgesteld is dat er data via dit project naar buiten is gelekt of oneigenlijk is gebruikt.

Inspectie, controle, toezicht

CONCEPT

Bijlage 1: Geïnterviewde rollen

Voor het onderzoek is met de volgende rollen gesproken:

Rol	Org.	Datum
Persoonsgegevens	IV-Accent	08-03-2017
	B/CIE	23-03-2017
	CAO en CIE	27-03-2017
	D&A	28-03-2017
	D&A	28-03-2017
	D&A	28-03-2017 08-05-2017
	D&A	28-03-2017 07-04-2017
	D&A	28-03-2017
	D&A	28-03-2017
	D&A	28-03-2017
	Dir. Belastingen	07-04-2017
	Dir. Belastingen	12-04-2017
	D&A	14-04-2017
	D&A	25-04-2017
	DGBel	14-04-2017
	D&A	08-05-2017
	ISC	15-06-2017
	B/CAP	22-06-2017
	D&A	28-06-2017
	B/CIE	18-07-2017

Bijlage 2: Begrippen

Begrip	Toelichting
AWS+	De AWS+ is een infrastructuur uitgerust met analytics capabilities, geleverd in de ICT-service XBA.
BI&A	De afdeling Business Intelligence & Analytics levert informatie over de prestaties van de processen van Belastingen, waardoor bestuurders in staat zijn om op basis van feiten en inzichten te sturen, te verantwoorden en besluiten te nemen.
Broedkamer	De Broedkamer is een project/programma. Een broedkamer biedt een team met een innovatief idee een geschikte plek, in termen van faciliteiten en expertise, om hun ideeën te ontwikkelen en ze te transformeren in een duurzame oplossing.
D&A	Data & Analytics, organisatie opgericht voor het maken van innovatieve informatietoepassingen voor burgers en bedrijven (t.b.v. de interactie), voor toezichtmedewerkers en medewerkers in de administratieve processen (t.b.v. informatie-gestuurde handhaving en/of inning), en voor bestuurders en managers (t.b.v. sturing, verantwoording en effectmeting). D&A vormt - naast Implementatie Operatie (IO) en IV accent - één van de pijlers van de Innovatiedriehoek data&analytics die de realisatie ondersteunt van de in de 'Investeringsagenda' beschreven visie en doelen van de Belastingdienst.
DWB	De Digitale Werkruimte Belastingdienst is gedefinieerd als: "De IT-faciliteiten die een eindgebruiker nodig heeft om het dagelijks werk te doen". Het gaat hierbij om pc-werkplekken en mobiele devices.
IMS	Identity Management System Via IMS worden de eindgebruiker-autorisaties aangevraagd door de manager. In veel gevallen kent IMS automatisch profielen toe op basis van de functie en/of het team. Verder kan de manager zelf (functie-)profielen en bijzondere taken toekennen in IMS.
PIA	Een Privacy Impact Assessment (PIA) is een hulpmiddel om bij ontwikkeling van beleid, en de daarmee gepaard gaande wetgeving of bouw van ICT-systemen en aanleg van databestanden, privacy risico's op gestructureerde en heldere wijze in kaart te brengen.
SAS	Is de merknaam van markconforme statistische software die onderdeel uitmaakt van een AWS+.
Teradata	Is de merknaam van een Data Warehouse Appliance.

Bijlage 3: Referentiekader Handboek Beveiliging Belastingdienst (HBB)

Voor het onderzoek naar de beveiligingsmaatregelen, is een subset gehanteerd uit het HBB 2011, te weten die doelstellingen die gerelateerd zijn aan gegevensgebruik t.b.v. data-analytics.

Het referentiekade is als volgt tot stand gekomen:

- Geldend beleid voor de Belastingdienst (en dus ook D&A) t.a.v. beveiliging is het HBB.
- We hanteren de normen uit het HBB (deel C) om te toetsen hoe de 'operationele invulling' van beveiliging was in de onderzoeksperiode.

Niet alle normen/ beheersmaatregelen uit deel C zijn relevant voor het onderzoek. Nadere scoping is gedaan, waarbij de vertrouwelijkheid van de gegevens centraal staat:

- preventieve en repressieve normen/ beheersmaatregelen;
- normen/ beheersmaatregelen zijn gerelateerd aan 'gegevensgebruik';
- relevante HBB-aspecten: fysieke beveiliging, logische beveiliging en personele veiligheid & integriteit (BCM-aspecten worden niet meegenomen);
- professional judgement van de auditors.

Norm/ maatregel (deel C HBB 2011)	Bevindingenoverzicht
Risicoanalyse (of Afhankelijkheidsanalyse)	3.3.1 Algemeen
C.1.3 Betrokkenheid management bij beveiliging	3.3.2.1 Betrokkenheid management bij beveiliging
C.2.5 Toegangsbeleid	3.3.2.2 Toegangsbeleid
C.2.6 Beleid voor informatie-uitwisseling	3.3.2.3 Beleid voor informatie-uitwisseling
C.2.7 Beleid voor draagbare computers en communicatievoorzieningen	3.3.2.4 Beleid voor draagbare computers en communicatievoorzieningen
C.2.8 Beleid voor telewerken/ thuiswerken	3.3.2.5 Beleid voor telewerken/ thuiswerken
C.2.12 'Clear desk'- en 'clear screen'-beleid	3.3.2.6 'Clear desk'- en 'clear screen'-beleid
C.2.14 Beleid voor geheimhouding	3.3.2.7 Beleid voor geheimhouding
C.2.16 Beleid voor algemeen beveiligingsgedrag personeel	3.3.2.8 Beleid voor algemeen beveiligingsgedrag personeel
C.2.17 Beleid voor aanvaardbaar gebruik van bedrijfsmiddelen	3.3.2.9 Beleid voor aanvaardbaar gebruik van bedrijfsmiddelen
C.6.2 Screenen	3.3.2.10 Screenen
C.6.4 Bewustzijn, opleiding en training t.a.v. beveiliging	3.3.2.11 Bewustzijn, opleiding en training t.a.v. beveiliging
C.6.5 Naleving gedragsregels voor beveiliging	3.3.2.12 Naleving gedragsregels voor beveiliging
C.6.6 Kritische en risicovolle functies	3.3.2.13 Kritische en risicovolle functies
C.6.7 Beëindiging dienstverband en functiewisseling	3.3.2.14 Beëindiging dienstverband en functiewisseling
C.6.8 Afhandelen beveiligingsmeldingen	3.3.2.15 Afhandelen en evalueren beveiligingsmeldingen
C.6.9 Evalueren beveiligingsmeldingen	3.3.2.15 Afhandelen en evalueren beveiligingsmeldingen
C.9.4 Verstrekken authenticatiemiddelen	3.3.2.16 Autorisaties
C.9.5 Aanvragen autorisaties	3.3.2.16 Autorisaties
C.9.6 Beheren groepering autorisaties	3.3.2.16 Autorisaties
C.9.7 Beheren decentrale autorisaties gebruikers	3.3.2.16 Autorisaties
C.9.8 Controleren van systeemgebruik	3.3.2.17 Controleren van systeemgebruik
C.12.12.7 Leveren van gegevens buiten overeengekomen productiedoeleinden	3.3.2.18 Leveren van gegevens buiten overeengekomen productiedoeleinden
C.13.7 Toegangsdiensten	3.3.2.19 Toegangsdiensten
C.14.4 Overeenkomsten inhuur derden	3.3.2.20 Overeenkomsten inhuur derden
C.16.3.1 (Controle-technische) functie- en processcheidingen	3.3.2.21 (Controle-technische) functie- en proces-scheidingen en zonering technische infrastructuur
C.16.4.1 Zonering technische infrastructuur	3.3.2.21 (Controle-technische) functie- en proces-scheidingen en zonering technische infrastructuur
C.17.6 Inrichting verbijzonderde ruimten	3.3.2.22 Inrichting verbijzonderde ruimten

Bijlage 4: Onderzoeks- en adviesrapporten

- Mei 2015: rapport Persoonsgegevens¹⁸. Gevraagd richting en visie Investeringsagenda te beoordelen en te adviseren. In grote lijnen: richting is nodig, passend, redelijk en implementeerbaar; wordt ook gekozen door andere organisaties (banken en andere belastingdiensten in UK, VS, Ierland, Australië, Nieuw Zeeland etc); de meerwaarde in relatie tot die landen is door de Belastingdienst conservatief ingeschat.
- Augustus 2015: rapport van LiquidHub¹⁹. Algemeen advies over hoe een data & analytics organisatie opgezet kan worden en waar daarbij op gelet moet worden, onder andere datamanagement. Het betreft geen analyse van de tot dan toe gehanteerde werkwijze, maar een advies voor de opbouw van een robuuste data & analytics afdeling. Opmerking: het document is nooit vastgesteld (versie 0.3).
De voornaamste bevindingen uit dit rapport in relatie met dit onderzoek zijn:

Organiseer Data Governance binnen BI&A en de bedrijfsvoering waardoor zorgvuldige omgang met gegevens wordt geborgd met afdoende aandacht voor beveiliging en er een auditeerbare situatie ontstaat.

Investeer in de robuustheid van processen om zowel de ontwikkeling ervan als de operationele werking volwassen te maken en de beschikbaarheid van het platform te optimaliseren. Stuur op proces discipline. Voorbeelden hiervan zijn het toepassen van Change- & Release Management processen waardoor op een gecontroleerde wijze deze succesvol kunnen worden geïmplementeerd (OTAP) zonder dat de beschikbaarheid en performance worden beïnvloed. Ook reproduceerbaarheid & traceability zijn van groot belang.

- September 2015: onderzoek naar datastromen en datamanagement door Persoonsgegevens²⁰ in opdracht van Persoonsgegevens. Vier datastromen zijn geanalyseerd: Vooringevulde Aangifte (VIA), Beheer van Relaties (BVR), gegevensverstrekking aan Centraal Bureau voor de Statistiek (CBS) en Databank Auto.

De bevindingen van dit onderzoek onderschrijven de noodzaak om belangrijke aspecten van het datamanagement te verbeteren, waaronder:

- *het opstellen van een eenduidig en overkoepelend kader voor databeheer;*
- *standaardisatie van de definities voor data binnen de bedrijfsonderdelen en de IT;*
- *beheer van de data over haar gehele levenscyclus.*

Bovenstaande is aanleiding geweest voor de interne memo 'Data Management Forum' (15 juni 2016), die een voorstel bevat voor het ontwerp en de inrichting van een Data Management Forum.

De RvB gaat op 20 juni 2016 akkoord met de instelling van het Data Management Forum, de benoeming van de leden van de stuurgroep van het Forum en het mobiliseren van de benodigde externe expertise om de start van het Forum te ondersteunen.

(Raad van Bestuur 20 juni 2016 Besluitenlijst)

¹⁸ 'Review of Investeringsagenda De Belastingdienst', 20 mei 2015

¹⁹ 'Belastingdienst BIA Observaties & Aanbevelingen', 26 maart 2015

²⁰ Investigating Data Streams, december 2015

Bijlage 5: Ontwerpkeuzes en beveiliging van de DWB werkplek en mobiele devices

Digitale Werkplek Belastingdienst (DWB)

De Digitale Werkruimte Belastingdienst, ook bekend als DWB, is gedefinieerd als:
"De IT-faciliteiten die een eindgebruiker nodig heeft om het dagelijks werk te doen".

DWB biedt digitale technologie aan eindgebruikers, waarmee deze in staat worden gesteld om hun dagelijks werk op een effectieve, efficiënte en veilige manier te kunnen uitvoeren, zowel vanaf pc-werkplekken als mobiele devices.

DWB biedt eindgebruikers de mogelijkheden om digitaal samen te werken met anderen, toegang te krijgen tot de Belastingdienst informatiesystemen en dit niet alleen in het Belastingdienstkantoor, maar ook vanaf andere lokaties.

Bij de Digitale Werkruimte Belastingdienst wordt de eindgebruiker centraal gesteld. Dit betekent dat het gebruikersgemak van DWB hoog in het vaandel staat en essentieel is voor succes.

DWB is gebaseerd op een aantal principes. Zoals het inzetten van de standaard producten op de manier zoals het vanuit de leverancier bedoeld is en het op een beheerbare en veilige manier continue veranderen en up-to-date houden van de digitale mogelijkheden.

Het doel hiervan is het faciliteren van de medewerkers om optimaal en veilig hun werk te kunnen uitvoeren.

De Belastingdienst komt vanuit een situatie waarbij alles technisch geblokkeerd was, gebaseerd op het mijden van risico's. Om toch de noodzakelijke werkzaamheden uit te kunnen voeren, zonder noodzaak tot schaduw-IT, moesten mogelijkheden gecreëerd worden. **Het uitgangspunt van DWB was dan ook om de medewerkers te enablen in plaats van te disablen. Hierbij is niet het technisch maximaal beperken als uitgangspunt genomen, maar een afweging tussen risico's, maatregelen en eigen verantwoordelijkheid en bewustzijn.**

Om het dagelijks werk op een veilige en productieve wijze te kunnen uitvoeren, is een aantal maatregelen genomen vanuit een set basisrisico's, te weten, verlies van informatie (verlies/diefstal devices), infectie met kwaadaardige software, ongeautoriseerde toegang, afluisteren/onderscheppen van informatie en gebruik van illegale programmatuur.

Een aantal voorbeelden van maatregelen: De informatiedragers zijn encrypted, denk hierbij aan harddisk, USB stick, data op mobile devices (Pas na autorisatie van een medewerker door de leidinggevende is het mogelijk de data op een USB stick via een bewuste actie te decrypten, zodat specifieke werkprocessen ondersteund konden worden). De devices zijn locked down en managed. Het communiceren en uitwisselen van informatie met derden kan middels beveiligde data uitwisseling en het samenwerkingsplatform vanuit het Belastingdienst Overheidsdatacenter. Indien een mobile device verloren is, kan deze op afstand worden gewist. Op de pc-werkplekken kan de automatische screensaver alleen middels een wachtwoord worden ontgrendeld. Deze diensten van DWB zijn door derde partijen op reguliere basis getoetst op aanval en penetratie.

(Bron: toelichting door architecten DWB)

Bijlage 6: De 10 geboden van informatiebeveiliging



DE 10 GEBODEN VAN INFORMATIE BEVEILIGING!



- ✓ Gebruik niet meer gegevens dan noodzakelijk voor de uitvoering van de analyse/rapportage/onderzoek. Maak rapportages anoniem tenzij.....
- ✓ Analyseer niet op basis van Persoonsgegevens omtrent iemands godsdienst of levensovertuiging, ras, politieke gezindheid, seksuele leven.



Personen, deze informatie is alleen voor intern gebruik

Persoonsgegevens

- ✓ Neem bij twijfel of vragen over datagebruik contact op met de Data Guardian en/of Dataprotectie Functionaris



DE 10 GEBODEN VAN INFORMATIE BEVEILIGING!



- ✓ Laat de data centraal staan op Teradata en/of de AWS. Distribueer data zo weinig mogelijk.
- ✓ Maak geen gebruik van wisselland. Maak gebruik van de uitwisselingsmap. Inspectie, controle, toezicht voor het uitwisselen van data. Verwijder de gegevens direct uit de uitwisselingsmappen. Gebruik geen Clouddiensten.

Persoonsgegevens

- ✓ Heb je niet de juiste autorisaties? Neem dan contact op met de Data Guardian en/of Dataprotectie Functionaris!



DE 10 GEBODEN VAN INFORMATIE BEVEILIGING!



- ✓ Verwijder data die je niet meer nodig hebt van je laptop. Ruim de data op Teradata en de AWS die je niet meer gebruikt regelmatig op.
- ✓ Stel persoons- en bedrijfsgegevens wanneer je deze buiten D&A gebruikt alleen beschikbaar aan de daarvoor geautoriseerde medewerker. In alle overige rapportages, analyses en presentaties die buiten D&A worden gebruikt zijn de persoons- en bedrijfsgegevens geanonimiseerd.



Persoonsgegevens

- ✓ Moet er toch data naar derden dan altijd via de Data Guardian en/of Dataprotectie Functionaris



DE 10 GEBODEN VAN INFORMATIE BEVEILIGING!



- ✓ Werk altijd met je eigen wachtwoord. Leen je wachtwoord(en) nooit uit, schrijf ze niet op en verander ze regelmatig.
- ✓ Vergrendel je scherm wanneer je de werkplek verlaat.

Persoonsgegevens

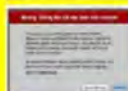
- ✓ Neem bij incidenten of vragen contact op met de Data Guardian en/of Dataprotectie Functionaris



DE 10 GEBODEN VAN INFORMATIE BEVEILIGING!



- ✓ Laat vertrouwelijke documenten niet slingeren. Gooi ze in de afgesloten papierbak wanneer ze niet meer nodig zijn. Houd je aan de Cleandesk policy.
- ✓ Klik nooit op hyperlinks in e-mails van onbekende afzenders. Rapporteer zo'n e-mail als spam/phishing bericht.



Persoonsgegevens

- ✓ Neem bij incidenten of vragen contact op met de Data Guardian en/of Dataprotectie Functionaris!

Betreft opdrachtnr. 201800001.

In dit dossier is aanwezig:

Naam	Gewijzigd op	Type	Grootte
2018-03-26 Verzoek Persoonsgegevens Onderzoek betrekken OB en Inni...	30-3-2018 13:20	Adobe Acrobat D...	54 kB
2018-03-27 Bestanden Persoonsgegevens	30-3-2018 13:19	Adobe Acrobat D...	106 kB
2018-03-27 P-gv. doet onderzoek OB en Inning ihkv HIA	30-3-2018 13:20	Adobe Acrobat D...	51 kB
2018-03-30 Persoonsgegevens Betr. Uitbreiding risicodetectie	30-3-2018 11:55	Adobe Acrobat D...	71 kB
2018-03-30 P-gv toestemming Persoonsgegevens	30-3-2018 11:54	Adobe Acrobat D...	63 kB
Ondbest_f116	27-3-2018 14:42	Microsoft Excel 97...	6.008 kB
Rapport Verband Tijdigheid en Juistheid MKB	9-1-2017 15:16	Adobe Acrobat D...	740 kB

Type: Adobe Acrobat Document

Start van de analyse

Het onderzoek richt zich op de vraag of het al dan niet corrigeren in de aangifte IH in relatie staat tot het verschil in de omzet OB met de omzet IH. Maw kan zo'n aansluitingsverschil in de omzet een trigger zijn dat er vaker een correctie plaatsvindt in de IH.

Er is een bestand ter beschikking gesteld van EHI (Persoonsgegevens) dat gebruikt wordt bij de Steekproef 2016. Het bevat met name gegevens over het jaar aangiftejaar 2014, van alle middelen.

Het bestand bevat kolommen die zien op belastingplicht van de diverse middelen, het al dan niet aanwezig zijn van correcties, de doelgroepindeling, omzet , bvr gegevens enz.

Vanwege de aanwezigheid van de omzet (verondersteld IH/VPB) is mbv het finr de omzet OB uit RAM gehaald. Er is een vergelijk gemaakt tussen de omzet OB en omzet IH en er is gekeken naar de al dan niet corrigeren. De uitwerking van de analyse is op 4 april besproken met Persoonsgegevens , de analyse gaf diverse onlogische inzichten. Daarop is Persoonsgegevens geraadpleegd met de vraag wat de omzet in het bestand betekende. De uitkomst was dat dit de berekende omzet OB was ipv de veronderstelde omzet IH/VPB. De analyse kan opnieuw worden uitgevoerd.

Aanpak:

IH: Omzet

Verzamel de omzet IH in RAM IH/VPB van het jaar 2013, 2014 en 2015, behorende bij 14.546 finrs uit het steekproefbestand. Creer een sleutelveld jaar en sofinr. Match dit sleutelveld met hetzelfde sleutelveld uit het steekproefbestand met IH plicht = J en voeg deze kolommen toe. Verwijder de niet matchende regels. Het bestand bevat 2.784 records. Voeg doelgroepcode toe. Maak teller op sleutelveld via draaitabel om te beoordelen of er meerdere winstaangiften/ondernemingen zijn en voeg de teller toe aan het bestand. Bepaal de som van de omzet per sleutelveld via draitable en voeg dit toe aan het bestand. Maak ook een variable met een uniek sleutelveld om inzicht te krijgen in de unieke finrs met totaalomzet. Voeg aan het bestand toe of er een correctie is geweest J/N op basis van bedrag van de correctie. Volgens de correctierichtlijnen is er een correctie indien sprake is van een correctiebedrag > € 500. In het geval dat er een negatieve correctie is wordt altijd gecorrigeerd.

Persoonsgegevens
OB Omzet

Verzamel de omzet OB 2013, 2014 en 2015 behorende bij de 14.546 finrs uit het bestand steekproef. Voeg er aan toe via sleutelveld jaar finr uit het steekproefbestand de volgende velden IHplicht J, correctie, doelgroep, Subnr OB, Omschrijving OB en alle velden met code Ob (00 t/m 88). Op basis van IH plicht is J is de verdeling van de ob plicht over de betreffende jaren als volgt:

omschrijving OB	2013	2014	2015	Eindtotaal
actief	229	1139	20	1388
actief/ lb vrijstelling	1	2		3
actief/vrijstellingadmin		1		1
afgevoerd	46	283	1	330
afgevoerd/actief	2	4		6
dochter		1		1
onbekend	14	246	9	269
vrijgesteld	1	9		10
vrijstelling admin		22		22
Eindtotaal	293	1707	30	2030

Vergelijking Omzet OB met Omzet IH.

Het bestand omzet IH is vergeleken met de omzet OB. Verschillen kleiner dan € 1000 worden als geen verschil aangemerkt. Er zijn een aantal mismatches, veroorzaakt doordat de ondernemer een firmant is. De OB wordt in dat geval op een afwijkend finr aangegeven. Via Metacode 4458 is uit tabel AFPWia 2014 heeft OB nummer opgehaald. Muv dit OB is uit RAM de OmzetTotaal van de jaren 2013,2014 en 2015 opgehaald .Deze zijn vervolgens gekoppeld aan het finr van de IH ondernemer.

```
%_eg_conditional_dropds(WORK.QUERY_FOR_AFP_WIA);
```

```
PROC SQL;
```

```
CREATE TABLE WORK.QUERY_FOR_AFP_WIA AS
SELECT t1.SOFINUMMER,
       t1.BEHANDELDOS_VOLGNR,
       t1.METACODE,
       t1.METACODE_VOLGNR,
       t1.onderneming VOLGNR,
       t1.MIDDELAANDUIDING,
       t1.BELASTINGJAAR,
       t1.AANGEGEVEN_WAARDE_NUMERIEK,
       t1.AANGEGEVEN_WAARDE_DATUM,
       t1.AANGEGEVEN_WAARDE_X_RUBRIEK,
       t1.AANGEGEVEN_WAARDE TEKST,
       t1.VOORVASTGESTELDE_WAARDE_NUM,
       t1.VOORVASTGESTELDE_WAARDE_DATUM,
       t1.VOORVASTGESTELDE_WAARDE X RUB,
       t1.VOORVASTGESTELDE_WAARDE TEKST,
       t1.VASTGESTELDE_WAARDE_NUMERIEK,
       t1.VASTGESTELDE_WAARDE DATUM,
       t1.VASTGESTELDE_WAARDE_X_RUBRIEK,
       t1.VASTGESTELDE_WAARDE TEKST,
       t1.OMSCHRIJVING_METACODE,
       t1.VALUTACODE,
       t1.VALUTAFACTOR,
       t2.Sofinummer AS Sofinummer1,
       t2.Jaar,
```

```

        t2.sleutel
FROM TI_AFP.AFP_WIA_2014 t1
    INNER JOIN WORK.OMZET_IH_2013_2015__AUTOMATISCH_ t2 ON
(t1.SOFINUMMER = t2.Sofinummer)
WHERE t1.METACODE = 4458;
QUIT;

```

Uitwerking

```

%_eg_conditional_dropds(WORK.QUERY_FOR_AFP_WIA_0000);

PROC SQL;
    CREATE TABLE
WORK.QUERY_FOR_AFP_WIA_0000(label="QUERY_FOR_AFP_WIA") AS
    SELECT t1.SOFINUMMER,
        t1.BEHANDELDOS_VOLGNR,
        t1.METACODE,
        t1.METACODE VOLGNR,
        t1.ONDERNEMING_VOLGNR,
        t1.MIDDELAANDUIDING,
        t1.BELASTINGJAAR,
        t1.AANGEGEVEN_WAARDE_NUMERIEK,
        t1.AANGEGEVEN_WAARDE_DATUM,
        t1.AANGEGEVEN_WAARDE_X_RUBRIEK,
        t1.AANGEGEVEN_WAARDE TEKST,
        t1.VOORVASTGESTELDE_WAARDE_NUM,
        t1.VOORVASTGESTELDE_WAARDE DATUM,
        t1.VOORVASTGESTELDE_WAARDE_X RUB,
        t1.VOORVASTGESTELDE_WAARDE TEKST,
        t1.VASTGESTELDE_WAARDE NUMERIEK,
        t1.VASTGESTELDE_WAARDE DATUM,
        t1.VASTGESTELDE_WAARDE_X RUBRIEK,
        t1.VASTGESTELDE_WAARDE TEKST,
        t1.OMSCHRIJVING_METACODE,
        t1.VALUTACODE,
        t1.VALUTAFACTOR,
        t2.VC_jaar,
        t2.'FINR(org)'n,
        t2.FINR,
        t2.sleuteljaarfinr,
        t2.ibl4
    FROM TI_AFP.AFP_WIA_2014 t1
        INNER JOIN WORK.SELECTIE_IH_NUMMERS t2 ON (t1.SOFINUMMER
= t2.FINR)
        WHERE t1.METACODE IN
            (
                1760,
                1795,
                4458
            );
QUIT;

```

Opvraag van de OB gegevens:

```
%_eg_conditional_dropds(WORK.QUERY_FOR_OB_AANGBET_UR5031A1);
```

```
PROC SQL;
```

```
CREATE TABLE
```

```
WORK.QUERY_FOR_OB_AANGBET_UR5031A1(label="QUERY_FOR_ob_aangbet_ur5031a1") AS
```

```
SELECT t1.AG_VASTNO,  
t1.AG_SUBNO,  
t1.AG_TYDVAK,  
t1.AG_GROEP,  
t1.AG_SOORT,  
t1.AG_VOLGNR,  
t1.AG_OB_INSP,  
t1.AG_DB_INSPONTVK,  
t1.AG_SCHATTER,  
t1.AG_SYS_INSP,  
t1.AG_UITSTEL,  
t1.AG_INSP_UITSTEL,  
t1.AG_DAGNR_VOLGNR,  
t1.AG_DATUM_BINNEN,  
t1.AG_CORRECTIES,  
t1.AG_OB_HOOG,  
t1.AG_OB_LAAG,  
t1.AG_OMZET_OVERIG,  
t1.AG_OB_OVERIG,  
t1.AG_OMZET_PRIVE,  
t1.AG_OB_PRIVE,  
t1.AG_OMZET_NUL,  
t1.AG_OMZET_HEFF_VERLEGD,  
t1.AG_OB_HEFF_VERLEGD,  
t1.AG_AFTR_VOORBEL,  
t1.AG_VERM_KO_REG,  
t1.AG_REEDS_GESCHAT,  
t1.AG_GESCHAT_BEDRAG,  
t1.AG_SALDO_OB,  
t1.AG_BESCHIKKINGSNR,  
t1.AG_POST_DATUM,  
t1.AG_DATUM_TYDIG,  
t1.AG_DATUM_TE_LAAT,  
t1.AG_TYDIG_BET,  
t1.AG_TE_LAAT_BET,  
t1.AG_VERREKEND,  
t1.AG_GENNOBETBIN,  
t1.AG_JRWERK_SEL,  
t1.AG_EXP_IMP_IND,  
t1.AG_ICT_IND_AANG,  
t1.AG_CBS_IND_AANG,  
t1.AG_AANG_IND,  
t1.AG_VALUTACODE,  
t1.AG_BEZORGIND,  
t1.AG_CIV_SELDATUM,  
t2.'Finr(org) 'n,  
t2.Finr
```

```
FROM TI_OB.ob_aangbet_ur5031a1 t1
```

```
INNER JOIN WORK.QUERY_FOR_AFP_WIA__2013_2014_201 t2 ON  
(t1.AG_VASTNO = t2.Finr)
```

```
WHERE t1.AG_TYDVAK BETWEEN 201240 AND 201601;  
QUIT;
```

2015

Het Regio Data Model(RDM)

Een beschrijving van de geschiedenis tot heden

In dit document wordt beschreven wat het RDM is en wat de (on) mogelijkheden zijn

Persoonsgegevens

Ministerie van Financiën
3-3-2015



Inhoud

Ontstaan RDM:.....	3
Basis.....	3
Gedrag:.....	4
MLTP 2011-2015:.....	4
Zachte info:.....	4
Verstoringen:.....	4
AANGIFTEGEDRAG.....	4
BETALINGSGEDRAG.....	4
JUISTHEID VOLLEDIGHEID.....	4
Compliance.....	5
Kleuren:.....	5
Wit:.....	5
Groen:.....	5
Geel:.....	5
Oranje:.....	5
Rood:.....	5
SCORE:.....	5
Werking Kleuren in het RDM:.....	6
Voorbeeld verzuimen Omzetbelasting:.....	6
WERKING KWADRANTEN IN RDM:.....	7
Werking schermen in het RDM:.....	8
Schermen:.....	8
Query- en selectieschermen:.....	8
Fiscaalnummer:.....	8
Algemeen:.....	8
Voorbeeld selectie Algemeen:.....	9
Omzetbelasting:.....	12
Controle:.....	13
Gemeente en Nationaliteiten:.....	14
Ondernemerscodes:.....	14
Vergelijkingen:.....	14
Omzetloon:.....	14
ATA:.....	15
Negatieve Norm:.....	15
A.Overzichtsscherm.....	16
B: Het informatiescherm:.....	17
Op Entiteit.....	17
Op fiscaalnummer.....	18
BIJLAGE:.....	20
Bestuurlijke informatie:.....	20

Ontstaan RDM:

In 2009 werd in de voormalige regio Rivierenland een 1^e aanzet gegeven, door het instellen van een werkgroep, tot de inrichting van Intelligence binnen de regio.

Intelligence zou zich bezig moeten houden met het doen van uitspraken over het gedrag van ondernemers/ondernemingen en groepen van deze.

Als leidraad werd het MLTP 2011-2015 genomen, de speerpunten in dit MLTP waren:

Verbetering van:

1. Aangiftegedrag
2. Betalingsgedrag
3. Juistheid en volledigheid
4. Registratie van de onbekende ondernemer.

De genoemde onderwerpen hadden het in zich dat er onderzocht moest worden op welke wijze en met welke "tools" de vragen konden worden beantwoordt.

Voor de hand liggend waren IKB en het toenmalige RAM daarnaast waren er nog tal van LOA's en andere afgeleiden van bronbestanden.

Al deze "bronnen" bevatten informatie die, op zich, wel bruikbaar zouden zijn echter geen van deze bronnen gaf de mogelijkheid op eenduidige relatief eenvoudige wijze een selectie te maken op doelgroepen/branchecodes enz.

Basis

De basis voor het RDM werd gevormd door een aantal basisprincipes:

- Selectie mogelijkheden.
- Flexibiliteit.
- Uniformiteit.
- Te bevatten voor gebruikers.

Verder was gewenst dat, wil men uitspraken over gedrag doen, dat de te gebruiken data:

- Steeds op dezelfde wijze kon worden verkregen.
- Dat deze data steeds uit dezelfde bronnen afkomstig zijn.
- Dat de te gebruiken data regelmatig kan worden verkregen.

Als basis bronnen werd gekozen voor IKB, RAM en enige BI bestanden.

Met behulp van deze bestanden werden met ACL (EDP_Audit) 2 "platte" bestanden op respectievelijk Entiteitnummer en Fiscaalnummer gemaakt die informatie bevatten over de volgende onderwerpen:

- Verzuimen, aangifte en/of betaalverzuimen.
- Naheffingen.
- Navorderingen.
- Invordering.
- Controles en andere externe, in IKB geregistreerde, bezoeken.
- Omzetten en omzetbelasting.
- Lonen en loonheffing.
- Convenanten.

Gedrag:

MLTP 2011-2015:

Om nu het MLTP 2011-2015 vorm te geven en inzichtelijk te maken wat:

- A. Het gedrag is.
- B. Het gedrag is na interventie.
- C. Het effect is van de interventie.
- D. Het gedrag van groepen van ondernemers/ondernemingen
- E. Het gedrag van groepen van na interventie op een (deel) van deze groepen
- F. Het gedrag van de fiscaal intermediair is

Hebben wij gekozen voor het inzichtelijk maken op basis van "verstoringen" die door onze *systemen steeds op dezelfde wijze worden geregistreerd en die (kunnen) leiden tot een interventie vanuit een systeem of door een menselijke interventie.

Zachte info:

De wijze van administreren en vastleggen van allerlei informatie in systemen/ loa's enz. heeft als nadeel dat we alleen gebruik kunnen maken van subjectieve in en door het systeem vastgelegde informatie daar, als er al "zachte" informatie vastligt, deze veelal "gekleurd" is door ervaringen van de vastlegger.

Wij hebben geen gestructureerd (ontdaan van subjectieve gevoelens) vastgelegde "zachte" informatie over ondernemers/ondernemingen/belastingconsulenten kunnen vinden.

Verstoringen:

Als wij het hebben over verstoringen bedoelen wij daar het volgende mee:

AANGIFTEGEDRAG

- aangifte verzuimen Omzetbelasting
- ambtshalve Vennootschapsbelasting
- ambtshalve Inkomensheffing
- aangifte verzuimen Loonheffing
- contactmomenten project Tijdige aangifte (ATA)

BETALINGSGEDRAG

- betaalverzuimen Omzetbelasting
- betaalverzuimen Loonheffing
- INL stand per 01-01-2010 of INL stand per 01-07-2010 idem voor 2011, 2012 en 2013 en 2014 en het actueel openstaand bedrag 2015 (brutobedragen dus alles wat openstaat)
- oninbaar geleden

JUISTHEID VOLLEDIGHEID

- correcties uit controle
- navorderingen Inkomstenbelasting
- navorderingen Vennootschapsbelasting
- naheffingen Omzetbelasting
- naheffingen Loonheffing
- systeemaanslagen OB

*wij hebben er voor gekozen niet allerlei bestanden van "handige Harrie's enz" zomaar aan mekaar te knopen.

Compliance

Kleuren:

Wit:

Deze kleur geeft aan dat wij het betreffende BSN of de Entiteit de laatste 6 jaar niet hebben bezocht, dit is middels een behandelopdracht in IKB, en dat we geen van de genoemde verstoringen bij dit BSN of Entiteitsnummer hebben geconstateerd.

Groen:

Deze kleur geeft aan dat we het betreffende BSN of de Entiteit hebben bezocht in de afgelopen 6 jaar en dat we geen van de genoemde verstoringen bij dit BSN of Entiteitsnummer hebben geconstateerd.

Geel:

Deze kleur geeft aan dat in het betreffende jaar er één verstoring is geweest in één van de drie genoemde categorieën.

Oranje:

Deze kleur geeft aan dat in het betreffende jaar er twee verstoringen zijn geweest in een combinatie van 2 van de 3 genoemde categorieën.

Rood:

Deze kleur betekent dat alle 3 de categorieën in het betreffende jaar zijn geraakt.

SCORE:

Inmiddels wordt RDM ook, mede, gebruikt voor de indeling van entiteiten in het Landelijk Klantbeeld.

Er wordt een score (ranking) bepaald aan de hand van de volgende criteria:

Aantal Systeemaanslagen OB 2010 t/m 2014 +
Aantal Aangifte verzuimen OB/LH/IH/VPB 2010 t/m 2014 +
Aantal betaalverzuimen OB/LH 2010 t/m 2014 +
Aantal keren een INL stand per 01-01-jaar van 2010 t/m 2014 +
Aantal jaren met correcties uit controle van 2010 t/m 2014 +

Het getal wat hieruit ontstaat is het veld Score, hoe hoger de score in absolute aantallen hoe meer een fiscaalnummer en/of entiteit in beeld komt voor "integrale aanpak".

Werking Kleuren in het RDM:

De kleuren in het RDM geven aan wat er bij het betreffende nummer (entiteit of BSN) in de systemen aan de hand is(geweest) in een jaar.

Daar het MLTP 2011-2015 was gericht op het verbeteren van het aangifte- en betalingsgedrag en het verbeteren van de juistheid en volledigheid van de aangifte is het mogelijk te meten of er inderdaad een verbetering/verslechtering van dit gedrag door de jaren heen ontstaat.

Voorbeeld verzuimen Omzetbelasting:

Table: A_Basis_Fiscnrs

Aangifte verzuimen OB 2014	193.727
Aangifte verzuimen OB 2013	335.455
Aangifte verzuimen OB 2012	361.530
Aangifte verzuimen OB 2011	366.836
Aangifte verzuimen OB 2010	389.177

Table: A_Basis_Fiscnrs

Betaalverzuimen OB 2014	357.340
Betaalverzuimen OB 2013	700.075
Betaalverzuimen OB 2012	691.724
Betaalverzuimen OB 2011	715.115
Betaalverzuimen OB 2010	700.270

Deze verstoringen hebben invloed op de kleuren zoals deze worden weergegeven in het RDM, komt één van beide voor is het betreffende nummer tenminste geel komen beiden bij hetzelfde nummer voor is het betreffende nummer tenminste oranje (want het is 1 aangifte verzuim en 1 betaalverzuim dus 2 categorieën).

De Omzetbelasting en de Loonheffing zijn de middelen met de hoogste scoringskans daar deze meerdere aangifte- en/of betalingsmomenten binnen het (lopende) jaar hebben. De Vennootschapsbelasting en Inkomensheffing hebben echter slechts één aangiftemoment en dit is vaak gelegen aan het einde van het volgende jaar (uitstelregeling).

Ook is het gebruik van de cijfers uit de diverse rubrieken van deze laatste middelen op zijn minst discutabel daar de jaren die ter beschikking zijn, zo deze er al zijn, verouderd zijn en een beeld geven van tenminste één jaar terug.

De combinatie van INL en de middelen Omzetbelasting en Loonheffing met daaraan toegevoegd de controle informatie geeft voor detectie van risico's c.q. "verstoringsgedrag" dan ook voldoende informatie.

Om nu te kunnen "inzoomen" op de massa zijn er een aantal schermen in het RDM die hiervoor gebruikt kunnen worden.

WERKING KWADRANTEN IN RDM:

KWADRANTEN:

In RDM wordt de mogelijkheid geboden om met "kwadranten" selecties te maken op groepen van ondernemers/ondernemingen in, achtereenvolgens, dezelfde;

- Regio
- Thema/aandachtsgebied
- Branchecode

Ten behoeve van deze selectie worden de aangegeven Omzetbelasting omzetten van alle ondernemers/ondernemingen die door de combinatie hierboven worden geraakt bij elkaar opgeteld.

Deze optelling wordt vervolgens gedeeld door het aantal ondernemers/ondernemingen die voldoen aan de volgende criteria:

- Aangegeven omzet jaar ongelijk aan 0 en ondernemerscode ongelijk aan code 7= vrijgestelde ondernemer.
- Startdatum ondernemer/onderneming niet groter dan het berekeningsjaar.

De tabel die ontstaat ziet er als volgt uit:

Kwadrant	Betekenis
A	OMZET >150% VAN HET GEMIDDELDE
B	OMZET VAN 125 TOT EN MET 150% VAN HET GEMIDDELDE
C	OMZET VAN 100 TOT EN MET 125% VAN HET GEMIDDELDE
D	OMZET 75% TOT EN MET 100% VAN HET GEMIDDELDE
E	Omzet 50% tot en met 75% van het gemiddelde
F	Omzet 25% tot en met 50% van het gemiddelde
G	Omzet minder dan 25% van het gemiddelde
X	Geen OB activiteiten

Werking schermen in het RDM:

Schermen:

Het RDM bestaat uit 3 delen te weten:

- A. Het query en selectiescherm
- B. Het informatiescherm op entiteit of fiscaalnummerniveau.
- C. Het selectiescherm Belastingconsulent.

Query- en selectieschermen:

In het query en selectiescherm bestaat de mogelijkheid om middels voor gedefinieerde ja/nee vragen selecties te maken op het betreffende voorkomen.

Fiscaalnummer:

Algemeen	Comfort info	OB
Actief	Project	Alleen voorbelasting 2012
Regio	Aantal projecten	Alleen voorbelasting 2013
Kantoorcode	Controle	Alleen voorbelasting 2014
Thema	Ambtshalve	Verschuldige OB (0 tot 100 euro) 2012
Subsegment	Verzuimen	Verschuldige OB (0 tot 100 euro) 2013
Branche	Convenant	Verschuldige OB (0 tot 100 euro) 2014
Doelgroep	Controle correcties	OB 2012 nihil
Beconnummer	Doelgroepsegment	OB 2013 nihil
Beconnaam	Beroepsgroep	OB 2014 nihil
FICOMPL10	Navordering, naheffing en vermindering 2010/2014	Saldo OB negatief 2010 t/m 2014
FICOMPL11	Planning15	Negatieve norm 2013
FICOMPL12		Negatieve norm 2014
FICOMPL13		OB suppleties 2012
FICOMPL14		OB suppleties 2013
Kwadrant 2011	Inning	OB suppleties 2014
Kwadrant 2012	INL open bedrag	Omzet OB negatief 2010 t/m 2014
Kwadrant 2013	Oninbare Post 2010/2014	Systeemaanslagen OB 2010 t/m 2014
Kwadrant 2014	Failissement	

Algemeen:

In de kolom Algemeen is informatie voorhanden om een onderscheid naar Regio, kantoor, Subsegment en Thema (nieuw Landelijk) enz. te maken.

Ook kunnen in deze kolom de compliance-kleuren worden gekozen.
Tevens kunnen de Belastingconsulenten (laatst bekende) worden geselecteerd.

Beconnummer	
Beconnaam	
Actief	

De keuze Actief is aanwezig omdat er in het RDM ook BSNRS staan die invloed hebben gehad op de compliance categorie van een entiteit of geraakt zijn door een project wat nog in beeld moet blijven die niet meer actief zijn als ondernemer.

Voorbeeld selectie Algemeen:

Aantal: 34	
Algemeen	
Actief	
Regio	906
Kantoorcode	
Thema	
Subsegment	
Branche	
Doelgroep	
Beconnummer	
Beconnaam	
FICOMPL10	ROOD
FICOMPL11	ROOD
FICOMPL12	ROOD
FICOMPL13	ROOD
FICOMPL14	ROOD
Kwadrant 2011	A
Kwadrant 2012	A
Kwadrant 2013	A
Kwadrant 2014	A

Geselecteerd achtereenvolgens:

Regio 906>Compliance categorie Rood 2010, 2011, 2012, 2013 en 2014 >Kwadrant A 2011, 2012, 2013 en 2014= 5 jaar150% van de gemiddelde omzet op Regio>Thema> Doelgroep>Branchecode.

Dit betekent dat er gelijksoortige bedrijven met elkaar worden vergeleken de H&TR branchecode 6822 wordt met een andere H&TR uit dezelfde regio dezelfde doelgroep en branchecode vergeleken (het betreft een indicatie)

Treffers: 34 fiscaalnummers die hier aan voldoen.

Op de volgende pagina ziet u een geselecteerde ondernemer in de weergave op fiscaalnummer.