Belastingdienst

Onderzoek Implementatie HBB

Eindrapport

Versie 1.0

Datum	18 september 2017
Status	definitief

Colofon

Projectnaam	Actie Implementatie HBB
Versienummer	versie 1.0
Opdrachtgever	DG Belastingdienst
Ged. Opdrachtgever	hoofd directeur IV
Opdrachtnemer	directeur Bedrijfsvoering IV
Projectleider	
Projectleden	

Inhoud

1 Management Samenvatting

Achtergrond
In het Kamerdebat van 9 februari 2017 zijn vragen gesteld naar aanleiding van een tv uitzending van 1 februari 2017. In deze uitzending is gesteld dat bij het koppelen van gegevens voor fraudebestrijding door de Belastingdienst belangrijke beveiligingsrisico's aan het licht zijn gekomen. De Staatssecretaris van Financiën heeft naar aanleiding van het Kamerdebat meerdere onderzoeken en acties toegezegd. Onder meer is toegezegd dat de Belastingdienst zou bezien op welke wijze het Handboek Beveiliging Belastingdienst (HBB) is geïmplementeerd in de organisatie, processen en systemen. Met als doel inzicht te krijgen in de vraag of de getroffen maatregelen adequaat zijn in relatie tot de aard van de gegevens en processen waarin zij worden gebruikt, en om waar nodig verbeteracties te formuleren.

In opdracht van de directeur generaal (DG) Belastingdienst (zie bijlage 1) is vervolgens onderzoek gedaan naar de besturing van de integrale beveiliging binnen de Belastingdienst zoals vastgelegd in het HBB, en de daarmee samenhangende beheersing van beveiligingsrisico's. Het doel hiervan is ten aanzien van deze twee thema's inzichtelijk te maken:
- hoe deze in de praktijk procedureel en inhoudelijk zijn ingericht en functioneren en of deze voldoen aan de hiervoor rijksbreed geldende normen en eisen;
- waar en hoe verbeteringen in de huidige werkwijze dienen te worden gerealiseerd.

In dit rapport worden de uitkomsten van het onderzoek beschreven, op basis waarvan verbetermaatregelen zijn geformuleerd. Het onderzoek richt zich op de situatie in de periode 2015-2016 en heeft in tegenstelling tot de *fact finding* onderzoeken naar de beveiliging bij het onderdeel Data & Analytics (D&A) en Broedkamers vooral een beschouwend beleidsmatig karakter.

Het was bij aanvang van dit onderzoek de bedoeling om de resultaten van het onderzoek van de Autoriteit Persoonsgegevens en de resultaten van het forensisch onderzoek naar een aanbesteding bij D&A, in het onderzoek te betrekken. Bij oplevering van deze rapportage waren deze onderzoeken echter nog niet gereed.

1.1 Uitkomsten onderzoek

De uitkomsten van het onderzoek zijn gestructureerd weergegeven op basis van de vier fasen van de PDCA (plan-do-check-act) cyclus.

<u>Het Handboek Beveiliging Belastingdienst (plan)</u>
- Beheersingsmechanismen voor integrale beveiliging zijn beschreven in het Handboek Beveiliging Belastingdienst. Daartoe behoren onder meer de P&C cyclus, besturing en besluitvorming in het MT Belastingdienst, de inzet van risicomanagement en het toedelen van rollen en verantwoordelijkheden.

- Het HBB volgt de rijksbrede beveiligingskaders en ISO standaarden uit de markt. Het HBB wijkt op een aantal punten af van de rijksbrede kaders op het gebied van informatiebeveiliging (i.c. BIR 2012). Behalve dat het HBB voor wat betreft informatiebeveiliging uitgaat van een meer recente ISO norm zijn er geen redenen of noodzakelijkheden gevonden voor het enigszins afwijkende informatiebeveiligingsbeleid dat de Belastingdienst met het HBB hanteert. Het hanteren van een eigen kader vereist onderhoud aan dat kader en beperkt eenheid van taal, uitvoering en verantwoording rijksbreed.
- Er is in het HBB geen verbinding gelegd tussen het HBB en het informatiebeveiligingsbeleid van het Kerndepartement. Er is sprake van grotendeels gescheiden PDCA-cycli rondom (informatie)beveilging.

<u>De beheersing van integrale beveiliging en borging in P&C (do)</u>

- Het HBB is een tactisch kader waarbij binnen de bedrijfsonderdelen een nadere uitwerking en operationalisering dient plaats te vinden. Op deze manier kan zo goed mogelijk worden aangesloten bij de beveiligingsvraagstukken van het betreffende onderdeel. De wijze waarop en mate waarin de onderdelen het HBB hebben uitgewerkt en geimplementeerd verschilt.
- Beveiliging maakt onderdeel uit van de P&C cyclus van de Belastingdienst. De beveiligingsdoelstellingen die opgenomen zijn in de P&C cyclus van de verschillende onderdelen, vormen een afgeleide van de beveiligingsdoelstellingen op concernniveau. Voor het merendeel van de gekozen concern beveilingdoelstellingen in de P&C is niet gebleken dat deze een directe relatie hebben met organisatiedoelen en de daarbij te onderkennen risico's.
- Uit het onderzoek is niet gebleken dat in de periode 2015-2016 in het concern MT/RvB is gesproken of besloten over integrale beveiliging. Er heeft wel onderdeel overstijgende coördinatie plaats gevonden op het niveau van beveiligingsadviseurs; voornamelijk via het Tactisch Beveiligingsoverleg (TBO). Middels dit adviserend overleg werden ook de jaarlijkse doelstellingen voor beveiliging afgestemd.
- De bedrijfsonderdelen hebben de afgelopen jaren jaarlijks een Zelfanalyse HBB opgeleverd waarin zij een beschrijving geven van de ontwikkelingen rondom integrale beveiliging en naleving van het HBB. Vanaf dit jaar is deze geïntegreerd in de Viermaandsrapportage.
- De Zelfanalyses verschillen tussen de onderdelen qua inhoud, structuur, detaillering en hebben met name een kwalitatief karakter. Dit maakt een centrale aggregatie op concern niveau en onderlinge vergelijkbaarheid lastig.
- Een centraal uitgangspunt van het HBB en rijksbrede kaders is dat integrale beveiliging beheerst wordt op basis van risicomanagement. Uit het onderzoek blijkt dat er enige vorm van risicomanagement rondom beveiligingsvraagstukken plaats vindt. De wijze waarop dit plaats vindt verschilt per dienstonderdeel. In algemene zin heeft het geen structureel of gestructureerd karakter.
- Er worden beveiligingsrisico's onderkend, voornamelijk op het niveau van de onderdelen. Uit het onderzoek is gebleken dat in enkele gevallen bijzondere risico gebieden zijn onderkend. De aandacht richt zich dan voornamelijk op bedreigingen van buiten (cybercrime). Beveiligingsrisico's die samenhangen met het (on)bewust onjuist handelen van medewerkers krijgen over het algemeen minder aandacht.
- Onderkende risico's worden niet gestructureerd of structureel gedeeld met andere onderdelen. Op concern niveau bestaat geen (dekkend

actueel) inzicht in de belangrijkste beveiligingsrisico's waar de organisatie mee te maken heeft.
- In algemene zin blijkt uit het onderzoek dat de beheersing van integrale beveiliging vooral is ingericht op het niveau van de onderdelen. Onderdeeloverstijgende beheersmechanismen, bijvoorbeeld voor de beheersing in ketens of op concern niveau, zijn beperkt.

Evaluatie, toezicht en externe onderzoeken (check)
- De onderdelen evalueren jaarlijks de naleving van enkele specifieke beveiligingsaspecten aan de hand van een intern controle programma. Over de uitkomsten daarvan wordt gerapporteerd in de Zelfanalyses. De wijze waarop dit gebeurt, verschilt tussen de onderdelen.
- De Zelfanalyses en halfjaarlijkse incidentrapportages verschaffen op concern niveau inzicht in de ontwikkelingen rondom integrale beveiliging en de naleving van het HBB. Dit inzicht is echter niet dekkend.
- Dienstonderdelen zijn in belangrijke mate afhankelijk van hoe beveiliging bij andere onderdelen is georganiseerd. Zij hebben echter geen inzicht in de naleving van kaders bij andere onderdelen. Zij vertrouwen erop dat de ander zijn beveiliging adequaat heeft ingeregeld.
- Een toezichthoudende rol (de *control*- en BVA functie) op het gebied van integrale beveiliging is voor zover het onderzoek heeft kunnen vaststellen, binnen de Belastingdienst de afgelopen jaren niet belegd geweest of ingevuld.
- De werking en effectiviteit van de integrale beveiliging (als samenstel van geimplementeerde maatregelen) is niet (periodiek) getoetst. Het inzicht hierover ontbreekt.
- Er worden met regelmaat onderzoeken uitgevoerd naar de beveiliging van de Belastingdienst door externe partijen; veelal door ADR en Algemene Rekenkamer (ARK). Zowel ADR als ARK constateren ten aanzien van de situatie in 2016 enkele tekortkomingen rondom *business continuity management* (BCM).
- Naast de onderzoeken die de ADR en ARK op basis van hun wettelijke taak uitvoeren, voert de ADR voor de Belastingdienst ook zogenoemde vraaggestuurde beveiligingsonderzoeken uit. Onder meer naar de tot stand koming en onderbouwing van de Zelfanalyses.
- Voor de meeste externe onderzoeken geldt dat deze rapporteren over een deelaspect van beveiliging en daarmee geen oordeel opleveren over het functioneren van de integrale beveiliging als geheel. Feitelijk is het onderhavige onderzoek de eerste evaluatie van de gehanteerde werkwijze ten aanzien van concernbrede control op het HBB.

Opvolging en bijstelling (act)
- Gebleken is dat het HBB jaarlijks wordt geactualiseerd.
- Wanneer uit de onderzoeken die de ADR en ARK vanuit hun wettelijke taak uitvoeren, tekortkomingen blijken, krijgen deze binnen de organisatie aandacht en opvolging. Het oplossen van geconstateerde tekortkomingen kan wel meerdere jaren in beslag nemen.
- In enkele gevallen is het oplossen van een geconstateerde tekortkoming opgenomen in de P&C doelstellingen van een onderdeel.

Conclusie
Het HBB is het integrale beveiligingskader voor de Belastingdienst, en het volgt als zodanig de rijksbrede kaders ten aanzien van integrale beveiliging. Het HBB deel voor informatiebeveiliging kent een zekere afwijking van de BIR. Het HBB kent een borging in de planning en control

cyclus van de Belastingdienst. Daarbij is er met name een afhankelijkheid van specialisten in de beveiligingsfunctie en de risico inschatting van de individuele dienstonderdelen. Het onderzoek bij D&A en met name de ondersteuning daarbij vanuit het Security Operations Center (SOC) laat zien dat er meer aandacht is voor de effectiviteit van de maatregelen tegen bedreigingen van buiten (cybercrime) dan voor de risico's in omgang met gegevens door eigen medewerkers. Verantwoording en monitoren op risico's en beveiligingsdoelstellingen is per dienstonderdeel georganiseerd en kent een beperkte aansluiting op de cyclus van het kerndepartement. Er is geen inzicht in de werking en effectiviteit van de integrale beveiliging Het onderhavige onderzoek is het eerste concernbrede evaluerende onderzoek naar de integrale beveiliging bij de Belastingdienst.

1.2 Verbetermaatregelen

De uitkomsten van dit onderzoek en de onderzoeken bij D&A en Broedkamers wijzen op een aantal verbeterpunten. Een aantal daarvan zijn inmiddels opgepakt, een aantal andere wordt gerealiseerd bij het implementeren van de nieuwe Topstructuur, en voor een derde categorie verbetermaatregelen geldt dat deze nog moeten worden uitgewerkt en gestart. De verdere coördinatie en uitwerking van deze maatregelen wordt belegd bij de CSO (Chief Security Officer).

- Al gestarte maatregelen hebben betrekking op het herijken en versterken van het pakket aan beveiligingsmaatregelen gericht op het tegengaan van (on)bewust onjuist handelen van medewerkers. Zo zijn striktere eisen gesteld aan het gebruik van de data analyse omgeving en wordt gewerkt aan een breder pakket aan technische maatregelen die onjuist handelen beter helpen te voorkomen en detecteren. Verder is de afgelopen maanden vanuit het concern Belastingdienst aandacht besteed aan verschillende beveiligingsvraagstukken en de verbetering daarvan. Daarmee wordt gewerkt aan een versterking van de tone-at-the-top.
- Daarnaast wordt met de implementatie van de Topstructuur een aantal belangrijke maatregelen gerealiseerd. Zo komen er een aparte CSO en BVA (Beveiligingsambtenaar) voor de Belastingdienst, ontstaat een nauwere verbinding met het Kerndepartement, worden rijksbrede normen leidend en komt er een nieuwe beheersingsstructuur gebaseerd op lijnsturing en functiescheiding.
- Enkele aanvullende maatregelen zijn nog niet expliciet genoemd in de Topstructuur maar vertonen daar wel een nauwe samenhang mee. Deze hebben te maken met 1) het als beveiliging beter aansluiten op de business en organisatiedoelstellingen 2) het versterken van risicomanagement op een zodanig wijze dat dit een gestructureerd en structureel karakter heeft en 3) het verbeteren van de onderdeel overstijgende beheersing van beveiligingsvraagstukken.

2 Uitkomsten van het onderzoek

2.1 Aanleiding en achtergrond

In de brief naar de Kamer naar aanleiding van het Zembla debat[1] is een beschrijving gegeven van een aantal onderzoeken en acties die de Belastingdienst zou uitvoeren naar aanleiding van het Kamerdebat van 9 februari 2017. Eén daarvan betrof de toegezegde actie dat "*de Belastingdienst zal bezien op welke wijze het Handboek Beveiliging Belastingdienst is geïmplementeerd in de organisatie, processen en systemen. Doel hiervan is inzicht te krijgen in de vraag of de getroffen maatregelen adequaat zijn in relatie tot de aard van de gegevens en processen waarin zij worden gebruikt, en om waar nodig verbeteracties te formuleren.*"

In lijn met deze toezegging is vervolgens op verzoek van de DG Belastingdienst onderzoek gedaan naar de besturing van de integrale beveiliging binnen de Belastingdienst zoals vastgelegd in het Handboek Beveiliging Belastingdienst (HBB), en de daarmee samenhangende beheersing van beveiligingsrisico's (risicomanagement). Het doel hiervan is ten aanzien van deze twee thema's inzichtelijk te maken:

- hoe deze in de praktijk zijn ingericht en functioneren en of deze voldoen aan de hiervoor rijksbreed geldende normen en eisen;
- waar en hoe verbeteringen in de huidige werkwijze dienen te worden gerealiseerd.

In bijlage 1 is de opdracht van de DG opgenomen en staat beschreven hoe het onderzoek is uitgevoerd.

In dit hoofdstuk zijn de uitkomsten van het onderzoek beschreven, dit aan de hand van de vier fasen van de PDCA (plan-do-check-act) cyclus.

2.2 Het Handboek Beveiliging Belastingdienst (*plan*)

Het beveiligingsbeleid van de Belastingdienst en de bijbehorende beheersmechanismen zijn beschreven in vier delen (A-D) van het Handboek Beveiliging Belastingdienst (HBB). Het HBB wordt jaarlijks geactualiseerd. Voor dit onderzoek is het HBB 2016 als referentiekader gehanteerd. Het HBB 2016 omvat de delen:

A. met de beleidsmatige uitgangspunten voor integrale beveiliging;
B. waarin de organisatie van beveiliging is beschreven, inclusief de benodigde rollen en functies, risicoanalyse, audit, rapportage etc.;
C. met de NEN-ISO 27002:2013 norm voor informatiebeveiliging;
D. waarin de *business continuity management* (BCM) richtlijn NEN-ISO 22313 is opgenomen.

2.2.1 Het HBB als werkbaar kader

Het HBB geldt binnen de Belastingdienst als *het* beleidskader voor integrale beveiliging en het HBB is als zodanig binnen de organisatie breed bekend.

Onderdelen – Het HBB gaat uit van de verantwoordelijkheid van (het lijnmanagement van) de individuele bedrijfsonderdelen en stelt net als

1 kenmerk 2017-0000026699

de Rijksbrede beveiligingskaders BVR[2], VIR[3] en BIR[4], dat het lijnmanagement primair verantwoordelijk is voor het organiseren, inrichten en borgen van de integrale beveiliging binnen het eigen organisatieonderdeel. Toepassen van het HBB is daarmee vooral een decentrale aangelegenheid. Het voordeel hiervan is dat de implementatie en uitwerking zo kan aansluiten op de dynamiek en uitdagingen van het betreffende onderdeel.

Basis beveiligingsniveau – Een aandachtspunt is dat dit kan leiden tot onderlinge verschillen in beveiliging. Individuele onderdelen staan niet op zichzelf; hun processen zijn nauw verbonden met die van anderen, en zij zijn daarom ook afhankelijk van hoe beveiliging daar is georganiseerd. Het HBB kent daarom een zogenoemd 'basis beveiligingsniveau' waaraan alle onderdelen dienen te voldoen. *Hoe* dat niveau in onderlinge samenwerking en samenhang in de dagelijkse praktijk tot stand moet komen en moet worden bestuurd tussen de onderdelen, is in het HBB niet uitgewerkt.

Overzicht van kaders en eisen – Een ander aandachtspunt is dat het HBB geen dekkend overzicht bevat van alle wettelijke- en rijksbrede beveiligingskaders en –eisen waaraan de organisatie dient te voldoen. Fysieke beveiligingsnormen, EU beveiligingsnormen en onderdelen van het Beveiligingsvoorschrift Rijksdienst staan er bijvoorbeeld niet in. Dit kan het voor gebruikers lastig maken om vast te stellen of en hoe er in specifieke gevallen, bovenop de in het HBB genoemde maatregelen, nog aanvullende maatregelen moeten worden getroffen die voortvloeien uit kaders die niet in het HBB zijn opgenomen.

Tactisch kader – Het HBB is, net als de BIR, een tactisch beveiligingskader, wat betekent dat de voorgeschreven maatregelen in de praktijk veelal nader moeten worden uitgewerkt en geoperationaliseerd. Het operationaliseren hiervan vereist specifieke kennis van (risicomanagement) en tijd, en kan in verder identieke situaties, leiden tot verschillende afwegingen en implementaties. De nadere operationalisering van tactische kaders vindt plaats op basis van een analyse van de betrokken Te Beschermen Belangen (TBB's) en bijbehorende risico's. Het vereist daarmee dus een goed inzicht in die TBB's en risico's. Gebleken is dat dat inzicht op dit moment niet dekkend is, wat een adequate (risicogestuurde) operationalisering in de praktijk belemmert.

2.2.2 *Het HBB en de samenhang met departement en Rijk*

Kerndepartement –Het Kerndepartement van Financiën en de Belastingdienst kennen ieder eigen (informatie)beveiligingsbeleid. Kaderstelling, *control* en rapportage rondom integrale beveiliging werd de afgelopen jaren in belangrijke mate door de Belastingdienst zelfstandig ingevuld. Dat is ook terug te zien in het feit dat het HBB, als het centrale kader voor integrale beveiliging van de Belastingdienst, geen relatie legt met het beveiligingsbeleid van het departement, bijvoorbeeld in termen van rapportage- en escalatielijnen, of ten aanzien van de rol en positie van de departementale beveiligingsambtenaar (BVA) of secretaris generaal (SG). In lijn daarmee constateerde de ADR eerder dit jaar dat er ten

2 Beveiligingsvoorschrift Rijksdienst 2013
3 Voorschrift Informatiebeveiliging Rijksdienst 2007
4 Baseline Informatiebeveiliging Rijksdienst 2012

aanzien van informatiebeveiliging "*sprake* [is] *van afzonderlijke PDCA cycli binnen het Kerndepartement en de Belastingdienst*".

BVA – Het voorgaande neemt niet weg dat er wel periodiek informatie-uitwisseling plaats vindt tussen Belastingdienst en Kerndepartement, hoofdzakelijk via de departementale BVA. De recent aangetreden nieuwe BVA van het ministerie heeft tevens als opdracht meegekregen om de samenwerking tussen Kerndepartement en Belastingdienst verder te versterken.

Rijkskaders – In de relatie met het Rijk is onderzocht in hoeverre het HBB aansluit op de rijksbrede beveiligingskaders. Het HBB sluit aan op deze rijksbrede kaders en op een tweetal ISO standaarden in de markt: HBB deel C omvat de NEN-ISO 27002:2013 norm voor informatiebeveiliging en deel D de NEN-ISO 22313 norm voor *business continuity management*.

BIR vs. HBB - Uit een inhoudelijke vergelijking blijkt dat het informatiebeveiligingsbeleid in het HBB 2016, net als de BIR 2012, is gebaseerd op ISO 2700x. Wel wijkt het HBB op een aantal punten af van de BIR.

Met het HBB deel C is gekozen voor een Belastingdienst-eigen invulling van de rijksbrede informatiebeveiligingskaders (VIR/BIR). Het HBB heeft niet de BIR 2012 integraal overgenomen, maar een nieuwere generieke (dus niet rijksspecifieke) versie van de ISO 2700x norm. De BIR 2012 is gebaseerd op een eerdere versie van deze norm. Deze werkwijze heeft mede tot gevolg dat enkele aanvullende rijksspecifieke beveiligingsnormen uit de BIR niet als zodanig terug vindbaar zijn in het HBB. Ook houdt het HBB rekening met andere bedreigingen en bedreigers dan de BIR[5]. Daarnaast hanteert het HBB niet het rijksbrede begrip Te Beschermen Belang en ontbreekt een baseline toets, zoals de BIR Quickscan, aan de hand waarvan beoordeeld kan worden of het basisbeveiligingsniveau volstaat in specifieke situaties.

De BIR 2012 heeft rijksbreed een verplicht karakter op basis van *comply or explain*, wat betekent dat organisaties hieraan moeten voldoen, dan wel aan dienen te geven op welke punten, en waarom, zij hiervan afwijken. Dit dient te worden toegelicht in de jaarlijkse In Control Verklaring BIR. In de ICV BIR 2016 geeft de Belastingdienst aan dat het een eigen informatiebeveiligingskader hanteert en dat het informatiebeveiligingsniveau van het HBB, 'minimaal gelijk' is aan dat van de BIR. In dit onderzoek is dit niet nader onderzocht.

Behalve dat het HBB is gebaseerd op een meer recente versie van de ISO2700x norm dan de BIR 2012, zijn er geen concrete aanwijzingen gevonden dat het eigen informatiebeveiligingsbeleid in het HBB tot een verbeterde beveiliging leidt of beter aansluit op (de dynamiek van) de Belastingdienst.

5 Het HBB 2016 (onderdeel B 2.2) heeft in tegenstelling tot de BIR 2012 (paragraaf 2.2) in het dreigingsprofiel geen 'contractors' (externe leveranciers/inhuur) opgenomen. Aan de andere kant geldt dat waar de BIR aangeeft geen bescherming te bieden tegen statelijke actoren en georganiseerde criminaliteit, het HBB stelt hier in het basis beveiligingsniveau wel rekening mee te houden..

Eigen kader – Het hanteren van een eigen kader kent twee aandachtspunten. Allereerst brengt dit onderhoud aan het kader met zich mee, waarvoor schaarse kennis ingezet moet worden. Daarnaast heeft het invloed op de samenwerking in de rijksbrede context. De Belastingdienst werkt nauw samen met andere rijkspartijen, waardoor onderlinge afhankelijkheden bestaan ten aanzien van het niveau van beveiliging en de daarbij gehanteerde werkwijze. Dit is ook de reden waarom de BIR is ontwikkeld. Het hanteren van een eigen norm draagt in die context niet bij aan een rijksbrede eenheid van taal, uitvoering en verantwoording.

2.3 De beheersing van integrale beveiliging en borging in P&C (do)

De in het HBB beschreven beheersingsmechanismen voor integrale beveiliging worden uitgevoerd op verschillende niveaus binnen de organisatie.

2.3.1 *Beheersing door het management op concernniveau*

De rollen, verantwoordelijkheden en beheersprocessen rond integrale beveiliging op concernniveau zijn op hoofdlijnen beschreven in het HBB. De drie centrale elementen in die beheersing op concernniveau zijn:

- de behandeling van beveiligingsvraagstukken en besluitvorming in het MT, onder verantwoordelijkheid van de Chief Security Officer;
- de inbedding van integrale beveiliging in de P&C cyclus;
- rapportage over beveiliging in de bedrijfsvoeringsparagraaf in het jaarverslag.

Behandeling in MT - Eindverantwoordelijk voor de integrale beveiliging binnen de Belastingdienst is volgens het HBB, de Chief Security Officer (CSO), wat in de periode 2015-2016 een rol was van de Chief Financial Officer (CFO). Concernbrede besluitvorming en besturing op het gebied van integrale beveiliging diende in deze periode plaats te vinden in het concern MT. Uit het onderzoek blijkt dat er vanaf februari 2015 geen stukken zijn terug te vinden waaruit blijkt dat in MT verband is gesproken of besloten over beveiligingsaspecten of risicoafwegingen, dan wel dat er besluitvorming heeft plaats gevonden over de doorontwikkeling/ verbetering van beveiliging. Een beveiligingsstrategie of –visie en daarvan afgeleide doelen of ambitie, is niet aangetroffen.

Beveiligingsadviseurs binnen de beveiligingsfunctie (rondom het Tactisch Beveiligingsoverleg) zijn blijven adviseren richting de CSO en het MT, maar omdat besluitvorming uitbleef zijn die adviezen in voorkomende gevallen als *de facto* besluit uitgevoerd (stafsturing).

P&C cyclus - De Belastingdienst hanteert een P&C cyclus en beveiliging komt hier jaarlijks in terug. Als onderdeel daarvan wordt jaarlijks over enkele prioritaire beveiligingsonderwerpen gerapporteerd in de bedrijfsvoeringsparagraaf van het jaarverslag van Financien.

Voor het merendeel van de concern beveilingdoelstellingen in de P&C is niet gebleken dat deze een directe relatie hebben met organisatiedoelen en bijbehorende risico's. Ze zijn weinig SMART omschreven en niet is gebleken dat bij het opstellen ervan rekening is gehouden met een mogelijke impact ervan op de bedrijfsonderdelen. Het risico is dat de P&C rondom beveiliging daardoor een administratief karakter krijgt.

2.3.2 *Beheersing op het niveau van bedrijfsonderdelen*

Het HBB is zoals aangegeven een tactisch kader waarbij binnen de bedrijfsonderdelen een nadere uitwerking en operationalisering dient plaats te vinden. De wijze waarop en mate waarin de onderdelen de beheersmechanismen uit het HBB hebben uitgewerkt en geimplementeerd verschilt. Een centraal gestuurde implementatie van het HBB heeft niet plaats gevonden.

MT - Beveiliging is een thema dat periodiek aan de orde komt in de MT's van de onderdelen. De onderdelen verschillen in de frequentie waarin zij beveiligingsvraagstukken bespreken in het MT. Evenzeer verschillen zij in de uitwerking van verantwoordelijkheden op het gebied van beveiliging en de wijze waarop zij hun beveiligingsfunctie invulling hebben gegeven. De verschillen in uitwerking en werkwijze vormen een aandachtspunt bij bedrijfsonderdeel overstijgende beveiligingsvraagstukken, zoals bij het onderling leveren van diensten of samenwerking in (deels externe) ketens.

P&C - Beveiliging is een onderwerp dat voorkomt in de jaarcontracten (P&C) van de bedrijfsonderdelen. De beveiligingsdoelstellingen die opgenomen zijn in jaarcontracten, vormen een afgeleide van de beveiligingsdoelstellingen op concernniveau.

Vertrouwen – Bedrijfsonderdelen hanteren naast de P&C ook andere beheersmechanismen voor beveiliging, waarbij onder meer gesteund wordt op zogenoemde *soft controls* (loyaliteit, integriteit, alertheid ed. van medewerkers). Dit past bij het gegeven dat menselijk gedrag van cruciaal belang is bij beveiliging. 'Vertrouwen' staat hierin centraal; vertrouwen in medewerkers, en vertrouwen in het adequaat handelen van andere bedrijfsonderdelen. Dit sluit ook aan bij de beveiligingsprincipes in het HBB.

Dit werken op basis van vertrouwen in medewerkers en collega's, is ook zichtbaar in het feit dat een groot deel van de beveiligingsmaatregelen gericht is op de bescherming tegen externe bedreigingen en bedreigers. Het Security Operations Center[6] (SOC) speelt een belangrijke rol in deze 'grensbewaking'. Tegelijkertijd laat het onderzoek naar de beveiliging bij D&A zien dat beveiligingsrisico's die voortkomen uit (on)bewust onjuist handelen van medewerkers, reëel zijn en om aandacht vragen.

Randvoorwaardelijk voor een beveiliging gebaseerd op vertrouwen is dat medewerkers en organisatie hiertoe inhoudelijk geequipeerd zijn. Medewerkers kunnen alleen alert reageren op wat zij zien en meemaken als zij weten waar zij op moeten letten (risico bewustzijn) en weten aan wie zij zaken moeten melden. Net zo vraagt integer en loyaal handelen om heldere normen[7], een regelmatige dialoog over normen en normbesef, en alert zichtbaar reageren wanneer grenzen worden overtreden. Dit vereist leiderschap (voorbeeldgedrag en *tone-at-the top*) en

6 Het SOC bewaakt de verkeersstromen binnen het datacentrum en tussen de interne systemen, de datastromen met externe partijen/netwerken en die van en naar de end points die B/CIE beheert. In dit verkeer probeert de SOC mogelijk-verdachte afwijkende patronen te detecteren. Daarnaast heeft het SOC onder meer ook een intelligence functie.

7 Dit kunnen geschreven of ongeschreven regels zijn. Niet alle facetten van loyaliteit en integriteit zijn te vatten in geschreven regels of kaders, ze vereisen een continue dialoog over wat wel en niet kan, mag of betamelijk is.

het *in place* zijn van een set met *hard controls*: voorlichtingsmateriaal, opleidingen, normen, procedures, (technische) maatregelen ter voorkoming en tijdige detectie van mogelijke *insider threats*[8], zoals monitoring. Sturen op basis van vertrouwen vereist zo een context van *hard controls*. De samenhang tussen al deze maatregelen bepaalt uiteindelijk de effectiviteit van de overall beheersing van integrale beveiliging. De bevindingen in het D&A onderzoeken maken duidelijk dat deze samenhang aandacht verdient.

Ook in de beheersing van onderdeel overstijgende beveiligingsvraagstukken wordt gesteund op het onderling vertrouwen; het vertrouwen dat de andere onderdelen de juiste zaken op het vlak van beveiliging goed hebben georganiseerd en dat zij eventuele risico's tijdig onderkennen, melden en oplossen. De onderdelen verwachten in die zin alertheid, transparantie en bewustzijn van de andere onderdelen.

2.3.3 *De beveiligingsfunctie*

De beveiligingsfunctie (beveiligingsadviseurs) op concern niveau en bij de bedrijfsonderdelen moet het lijnmanagement ondersteunen bij de beheersing van integrale beveiligingsvraagstukken. Vrijwel alle onderdelen hebben een dergelijke vorm van ondersteuning. Er is sprake van een diversiteit in omvang, uitwerking en inrichting. Dit heeft gevolgen voor de onderdeel overstijgende (keten)samenwerking en beveiliging.

<u>Rol</u> – De beveiligingsfunctie ondersteunt onder meer bij de uitwerking en operationalisatie van het HBB. In de praktijk kost dit uitwerken de nodige tijd. Het leidt tot dubbel werk en onduidelijk is of dit adequaat is gebeurd. Dit is met name relevant voor de besluitvorming en daarmee voor afstemming bij bedrijfsonderdeel overstijgende beheersaspecten (Heeft het ene onderdeel voldoende rekening gehouden met de risico's, kaders, maatregelen die nodig zijn voor de ander?). Onderdelen vertrouwen er, zoals hierboven reeds aangegeven, op dat de ander het goed doet, maar zeker weet men dat niet.

<u>Functiescheiding</u> – In algemene zin geldt dat rollen en taken op het gebied van integrale beveiliging op hoofdlijnen zijn beschreven en veelal een nadere uitwerking missen. Functiescheiding vormt in die zin een aandachtspunt. Kaderstellende, uitvoerende en control(erende) taken worden rondom integrale beveiliging soms gecombineerd.

2.3.4 *Risicomanagement*

Een centraal uitgangspunt van het HBB en rijksbrede kaders is dat integrale beveiliging beheerst wordt op basis van risicomanagement.

<u>Structureel en gestructureerd</u> - Uit het onderzoek blijkt dat voornamelijk op het niveau van de bedrijfsonderdelen beveiligingsrisico's worden onderkend. Op het moment dat risico's in beeld zijn, dienen deze gemonitord en beheerst te worden. De wijze waarop de onderkende risico's worden beheerst, en de mate waarin dit op een structurele en gestructureerde manier (volgens een vaste structuur en proces) gebeurt, verschilt tussen de onderdelen. In algemene zin geldt dat dit een niet-gestructureerd en niet-structureel karakter heeft.

8 Hieronder vallen technische maatregelen als pseudonimisering en anonimisering, datacompartimentering en dataclassificatie, logging & monitoring en data loss prevention (DLP) tooling.

Risicomanagement beleid – De verschillen in werkwijze tussen de onderdelen in de manier waarop zij met risicomanagement omgaan, zijn onder meer verklaarbaar uit het feit dat concernbrede kaders of handvatten voor beveiligingsrisicomanagement ontbreken. De Belastingdienst kent wel algemeen risicomanagement beleid. De beheersing van beveiligingsrisico's is hier een deelaspect van, en het HBB verwijst ook naar het algemene beleid. Uit het onderzoek is niet gebleken dat het algemene risicomanagement beleid in de praktijk wordt toegepast. Eerdere initiatieven die zijn ondernomen om dit beleid in de organisatie te implementeren, hebben niet het gewenste effect gehad. Op het moment dat algemeen risicomanagement nog niet is georganiseerd in het reguliere dagelijkse werk van de organisatie, belemmert dit de verdere doorontwikkeling en internalisatie van het risicomanagement dat specifiek gericht is op beveiliging.

Delen van risico's – Door onderdelen onderkende beveiligingsrisico's worden niet actief/structureel horizontaal (met andere onderdelen en ketenpartners) of verticaal gedeeld. Van een samenhangende onderdeel overstijgende beheersing van beveiligingsrisico's is nog geen sprake.

Inzicht – Op concern niveau bestaat geen actueel dekkend inzicht in de (prioritaire strategische) beveiligingrisico's waar de organisatie mee te maken heeft. De meest recente risicoanalyses dateren uit 2014. Voorts is niet gebleken dat in de periode 2015-2016 op concern niveau besluitvorming heeft plaats gevonden over (strategische) beveiligingsrisico's of over de opvolging/beheersing daarvan.

Risicotolerantie – Een belangrijk richtinggevend aspect in het risicomanagement proces vormt de risicobereidheid of risico tolerantie. Dit is de mate waarin de organisatie of een organisatieonderdeel risico's wil, mag en kan dragen. Een expliciet omschreven niveau van risicobereidheid/-tolerantie voor beveiligingsrisico's op concernniveau is niet aangetroffen.

Wel geldt dat de organisatie met het HBB heeft gekozen voor een basis beveiligingsniveau voor alle bedrijfsonderdelen. In het HBB staan ook de actoren en bedreigingen waarmee rekening is gehouden in dit basis beveiligingsniveau. Bedrijfsonderdelen dienen na te gaan op basis van risicomanagement, of dit basis beveiligingsniveau volstaat, of dat voor bepaalde aspecten/onderdelen/systemen etc. aanvullende maatregelen nodig zijn. Mede door het ontbreken van monitoring en evaluatie is het niet aantoonbaar of het basis beveiligingsniveau in de praktijk wordt gerealiseerd, waar het exact tegen beveiligt, en welke restrisico's daarmee nog blijven bestaan. Zichtbaar is dat onderdelen aandacht hebben voor bijzondere risico gebieden en dat enkele bedrijfsonderdelen risico analyses hebben uitgevoerd om in een aantal concrete situaties vast te stellen of het basis niveau volstaat.

2.4 Evaluatie, toezicht en externe onderzoeken (check)

Zelfanalyses – De onderdelen rapporteren jaarlijks (vanaf 2017, viermaandelijks) richting het concernniveau via de de zogenoemde Zelfanalyse HBB. De onderwerpen waarover de dienstonderdelen dienen te rapporteren worden vastgelegd in de jaarlijkse centraal door het Tactisch

Beveiligingsoverleg (TBO) bepaalde beveiligingsdoelstellingen. Inhoudelijk geldt dat in de Zelfanalyses wordt gerapporteerd over de uitkomsten van een intern controle programma (ICP) dat onderdelen jaarlijks opstellen en uitvoeren en dat gekoppeld is aan de beveiligingsdoelstellingen. De onderdelen rapporteren halfjaarlijks ook over de beveiligingsincidenten die zich in de voorgaande periode hebben voorgedaan.

De Zelfanalyses HBB hebben een kwalitatief karakter en verschillen onderling in structuur, detailering en inhoud. Ook blijkt uit eerder onderzoek van de ADR dat er sprake is van verschillen in kwaliteit bij de tot standkoming ervan. Deze verschillen maken dat de analyses op concern niveau lastig zijn te aggreren tot een dekkend beeld voor de Belastingdienst als geheel. Voor de naleving van het HBB betekent dit, dat er wel enig inzicht in de naleving bestaat op hoofdlijnen, maar dit is niet dekkend.

Toezicht – Het toezicht op de (werking van de) integrale beveiliging is volgens de rijksbrede kaders belegd bij de departementale beveiligingsambtenaar (BVA). Gebleken is dat deze toezichtstaak voor de Belastingdienst niet helder is belegd. Ook is niet gebleken dat deze taak in de periode 2015-2016 is ingevuld. Mede hierdoor ontbreekt op concern niveau een dekkend inzicht in de werking en effectiviteit van de integrale beveiliging en het (samenstel van maatregelen uit het) HBB.

2.4.1 *Externe beveiligingsonderzoeken en audits*

Er worden op alle organisatie niveaus diverse beveiligingsonderzoeken en –audits uitgevoerd die (het lijnmanagement) inzicht geven in het functioneren van deelaspecten van de integrale beveiliging van de Belastingdienst. Deze worden met name uitgevoerd door de Auditdienst Rijk (ADR) en door de Algemene Rekenkamer (ARK).

Onderzoeken wettelijke taak – Op basis van hun eigen wettelijke taak voeren de ADR en Algemene Rekenkamer (ARK) jaarlijks bij de rijksonderdelen onderzoek uit naar enkele (wisselende) beveiligingsaspecten. Uit de rapportages van ADR[9] en ARK[10] over 2016 blijkt dat bij de Belastingdienst ten aanzien van beveiliging, tekortkomingen zijn geconstateerd op het gebied van *business continuity management* (BCM)[11]. Het feit dat onderzoek wordt gedaan naar enkele (wisselende) beveiligingsaspecten betekent dat er niet wordt gerapporteerd over de werking of effectiviteit van de integrale beveiliging in brede zin. Wel constateert de ADR over 2016 ten aanzien van informatiebeveiliging: *"De PDCA cyclus voor de Belastingdienst is ingericht maar er is nog ruimte voor verbetering, bijvoorbeeld op het gebied van aansluiting tussen risico's, doelstellingen, verbeterplannen en rapportages."*

Vraaggestuurde onderzoeken – Verder voert de ADR ook zogenoemde vraaggestuurde onderzoeken uit naar beveiligingsaspecten binnen de organisatie. Jaarlijks wordt hiervoor vanuit het Tactisch Beveiligingsoverleg (TBO) een auditplanning opgesteld. De realisatie hiervan blijft de afgelopen jaren echter achter op planning. Een duidelijk aanwijsbare

9 Samenvattend auditrapport bij het jaarverslag 2016
10 Resultaten verantwoordingsonderzoek 2016, Rapport bij jaarverslag. Ministerie van Financien en Nationale Schuld (IX). Algemene Rekenkamer
11 De ADR noemt daarnaast een bevinding ten aanzien van het informatiebeveiligingsbeleid van de Belastingdienst Caribisch Nederland.

oorzaak hiervoor is niet gevonden. Een jaarlijks terugkerend onderzoek dat de ADR uitvoert is die naar de HBB Zelfanalyses.

ICV - De resultaten en uitkomsten van de zelfanalyses worden gebruikt voor de In Control Verklaring (ICV) BIR die jaarlijks wordt afgegeven door het departement. De ADR onderzoekt jaarlijks het tot stand komen van de Zelfanalyses bij enkele onderdelen.

Inzicht – In algemene zin geldt dat de extern uitgevoerde onderzoeken enig inzicht verschaffen over het functioneren van specifieke deelaspecten van integrale beveiliging. Een samenhangend beeld of oordeel over de werking of effectiviteit van de integrale beveiliging leverden deze niet.

2.5 Opvolging en bijstelling (act)

Opvolging – Wanneer uit de onderzoeken die de ADR en ARK vanuit hun wettelijke taak uitvoeren, tekortkomingen blijken, krijgen deze binnen de organisatie aandacht en opvolging. Dit is bijvoorbeeld zichtbaar bij de eerder geconstateerde onvolkomenheden rond vertrouwensfuncties en logisch toegangsbeheer (LTB), en bij het door de Rijksinspecties uitgevoerde onderzoek naar de Kwetsbaarheidsanalyse Spionage (KWAS). Ten gevolge van dit laatste onderzoek is in het HBB bijvoorbeeld meer aandacht gekomen voor spionage risico's.

Wel is zichtbaar dat het oplossen van geconstateerde tekortkomingen meerdere jaren in beslag kan nemen. Het wegwerken van de onvolkomenheid op het gebied van LTB heeft meerdere jaren in beslag genomen. En de tekortkomingen rondom BCM die nu een onvolkomenheid vormen, werden door de ARK al in 2014 voor het eerst als aandachtspunt benoemd, en door de ADR reeds geadresseerd in 2011.

In enkele gevallen is het oplossen van een in extern onderzoek geconstateerde tekortkoming opgenomen in de P&C doelstellingen van een onderdeel.

Bijstellen HBB – Het HBB wordt jaarlijks geactualiseerd. Aanpassingen aan het HBB vloeien voornamelijk voort uit aanpassingen in externe normen. De jaarlijkse zelfevaluaties, politiek-bestuurlijke ontwikkelingen, of vraagstukken die spelen bij de business leiden niet direct tot aanpassingen in het HBB.

3 Te treffen verbetermaatregelen

De in het voorgaande hoofdstuk beschreven bevindingen nopen tot het doorvoeren van een aantal verbetermaatregelen. Dit wordt onderstreept door de uitkomsten van het onderzoek naar de beveiliging bij D&A en Broedkamers.

In dit hoofdstuk worden de maatregelen beschreven die de Belastingdienst zal treffen om de integrale beveiliging en de beheersing daarvan te versterken. De realisatie van enkele maatregelen is de afgelopen maanden al in gang gezet, een aantal andere wordt gerealiseerd als direct gevolg van de implementatie van de Topstructuur. Een derde categorie maatregelen is nog niet als zodanig eerder benoemd of uitgewerkt. Een groot deel daarvan heeft wel een directe relatie met de uitgangspunten van de nieuwe Topstructuur.

Deze drie groepen maatregelen zijn in de volgende paragrafen nader uitgewerkt.

3.1 Al in gang gezette maatregelen

Naar aanleidingen van de ontwikkelingen eerder dit jaar en de bevindingen van het onderzoek naar de beveiliging bij D&A zijn de afgelopen maanden al verschillende maatregelen getroffen ter versterking van de integrale beveiliging. Deze zijn in te delen in:

- versterken van maatregelen tegen (on)bewust onjuist handelen van medewerkers;
- versterken van tone-at-the-top.

Versterken maatregelen tegen (on)bewust handelen van medewerkers – Ontwikkelingen rondom digitalisering, automatisering en *big data* analyse capaciteiten zorgen ervoor dat steeds grotere en 'rijkere' gegevensbestanden bijeengebracht en verwerkt worden binnen de organisatie. De maatregelen die de beveiliging van die gegevens moeten borgen, moeten meegroeien. Enerzijds dienen deze te beschermen tegen bedreigingen van buiten, en anderzijds tegen (on)bewust onjuist handelen van medewerkers intern.

Ten aanzien van dit laatste geldt dat beveiliging in belangrijke mate steunt op het vertrouwen in het risicobewustzijn van medewerkers. Uit de bevindingen van het onderzoek bij D&A blijkt dat dit niet altijd voldoende zekerheid geeft dat incidenten adequaat voorkomen en gedetecteerd kunnen worden.

Het samenhangend pakket aan maatregelen dat dient ter bescherming tegen (on)bewust onjuist handelen van medewerkers zal daarom herijkt worden, en de effectiviteit ervan verbeterd. De afgelopen maanden zijn hier al diverse stappen in gezet. Zo is het gebruik van de data analyse omgeving aan striktere regels gebonden. Ook zijn technische maatregelen getroffen om het verspreiden van gegevens uit die omgeving tegen te gaan, en aan aanvullende maatregelen wordt gewerkt. De ervaringen daarmee zullen de komende periode gebruikt worden om te bezien of er in bredere zin aanvullende maatregelen nodig zijn.

Versterken *tone at the top* – Een juiste *tone at the top* ten aanzien van beveiliging is van groot belang. Daarom wordt de komende periode aandacht besteed aan aspecten als voorbeeldgedrag, alertheid, daadkracht, commitment, eigenaarschap, aanspreken en beveiligingsbewustzijn. De wijze waarop dit op concern niveau in de MT's, en in de onderdelen en regiodirecties wordt opgepakt straalt uit naar de onderliggende management lagen en de gehele organisatie.

Sinds begin dit jaar zijn hier al stappen in gezet. Zo is met regelmaat op verschillende manieren gecommuniceerd over verschillende beveiligingsgerelateerde zaken en het belang van een adequate beveiliging. De hierna genoemde maatregelen die de organisatie wil treffen onderstrepen in die zin ook de gevoelde urgentie om ten aanzien van integrale beveiliging een aantal forse stappen te zetten.

3.2 Verbetermaatregelen die onderdeel vormen van Topstructuur

De Belastingdienst zal de komende periode de nieuwe Topstructuur verder uitwerken en implementeren. Hiermee wordt ook direct een aantal noodzakelijke verbetermaatregelen rondom integrale beveiliging gerealiseerd:

Versterking van de relatie met het Kerndepartement – De Topstructuur voorziet in een andere, meer reguliere, verankering van de Belastingdienst binnen het departement en intensievere verbinding met het Kerndepartement, ook op het vlak van de beleidscyclus. In lijn hiermee zullen ten aanzien van beveiliging de grotendeels gescheiden PDCA cycli verdwijnen en die van Belastingdienst en Kerndepartement met elkaar worden verbonden. Met het Kerndepartement zal worden toe gewerkt naar een gezamenlijk departement breed integraal beveiligingsbeleid, waarbij er ruimte blijft om zo nodig aanvullend beleid te formuleren daar waar dit nodig mocht zijn.

Vervanging van de CSO rol door een CSO functie – De uitkomsten van het onderzoek laten zien dat bestuurlijke tijd en aandacht op concernniveau randvoorwaardelijk is voor een adequate beheersing van integrale beveiliging. De nieuwe Topstructuur helpt bij de aanpak hiervan doordat het een CSO functie introduceert, als alternatief voor de rol van CSO nu. De CSO kan fulltime aandacht besteden aan de integrale beveiliging, en de verdere verbetering daarvan, en is ondergebracht bij de concerndirectie IV en databeheersing. Ter versterking van de verticale samenhang zal de CSO ook de beveiligingsadviseurs bij de onderdelen functioneel aansturen.

Inrichting van een heldere beheersingsstructuur – De Topstructuur brengt voor de Belastingdienst een ander besturingsmodel, waarmee de beheersbaarheid van de organisatie wordt vergroot, onder meer in de relatie tussen concern en bedrijfsonderdelen en tussen lijn en staf. Zoals uit de bevindingen blijkt behoeft dit ten aanzien van integrale beveiliging ook aandacht en verbetering. De CSO zal daartoe, samen met de onderdelen een beheersingsstructuur voor integrale beveiliging ontwikkelen die de verschillende lagen van de organisatie aan elkaar verbindt. Deze beheersingsstructuur omvat een eenduidige omschrijving van verantwoordelijkheden (RASCI), taken en bevoegdheden en

beschrijft gremia voor afstemming en besluitvorming, eenduidige escalatie- en rapportagelijnen, alsmede een beschrijving van de relatie tussen lijn en beveiligingsfunctie en de bijbehorende hiërarchische/functionele verhoudingen. Met deze nieuwe structuur wordt de verticale alignment en beheersing van de integrale beveiliging versterkt en kunnen de verantwoordelijkheden op concernniveau adequater worden ingevuld.

Een eenduidige functiescheiding – Met de implementatie van de Topstructuur wordt ook toegewerkt naar een betere functiescheiding. Voor integrale beveiliging ziet die functiescheiding er als volgt uit:

- Beleidsvorming en kaderstelling[12] – De CSO is verantwoordelijk voor de beveiligingsvisie en –strategie, het (doen laten) ontwikkelen van het concernbrede beveiligingsbeleid, en de borging daarvan. In dat kader zorgt hij voor de samenhang en relatie met het departementale en rijksbrede beveiligingsbeleid en bijbehorende beleidscycli. De CSO zoekt beleidsmatig de samenwerking en afstemming met onder andere de CIO, CDO en directeur F&C. Laatst genoemde is kaderstellend op het gebied van risicomanagement. De CIO en CDO hebben een kaderstellende taak rondom IV en datahuishouding; informatiebeveiliging vormt hier een onderdeel van. Beleidsvorming rondom de personele aspecten vindt plaats bij de concerndirectie O&P.
- Uitvoering – Uitvoering en implementatie van beveiligingsmaatregelen is belegd in de reguliere bedrijfsprocessen in de lijn (bedrijfsonderdelen, CD's en SSO's). De lijnmanager is verantwoordelijk voor de (inrichting en het functioneren van de) integrale beveiliging van zijn onderdeel. De beveiligingsadviseurs ondersteunen hierbij.
- Control – Het lijnmanagement is verantwoordelijk voor de inzet van juiste beheers- en borgingsmechanismen rondom integrale beveiliging in de dagelijkse management praktijk. De controlfunctie houdt toezicht op de juiste inrichting en werking hiervan en naleving van kaders. Bij control is daarom ook de BVA taak voor de Belastingdienst belegd. De functionaris die hiermee belast is houdt toezicht op het functioneren, werking en effectiviteit van de integrale beveiliging en wordt daartoe functioneel aangestuurd door de BVA Financiën.

Versterken toezicht en inzicht in werking – De introductie van een BVA voor de Belastingdienst, zoals voorzien in de Topstructuur, vormt een belangrijke verbetermaatregel. In het onderzoek blijkt dat deze rol de afgelopen jaren binnen de organisatie feitelijk niet is ingevuld en dat er (mede daardoor) geen inzicht bestaat in de werking en effectiviteit van de integrale beveiliging. Op het moment dat dit inzicht ontbreekt kan ook niet gericht gestuurd worden op de verbetering daarvan.

Rijksbrede normen zijn leidend – Een laatste maatregel die concreet voortvloeit uit de nieuwe topstructuur vormt het overnemen van rijksbrede beveiligingskaders. De Topstructuur stelt dat de rijksbrede bedrijfsvoering(safspraken) leidend zijn en de rijksbrede trapsgewijze vormgeving van kaderstelling wordt gevolgd. Dit betekent dat alle rijksbrede kaders integraal in het HBB worden overgenomen, waaronder het huidige BIR. Ook wordt het basisniveau van beveiliging gelijk getrokken met die in de BIR.

12 Het betreft hier uitsluitend kaderstelling in aanvulling op, dan wel nadere precisering van, de rijksbrede en departementale beveiligingskaders.

3.3 Nog in gang te zetten verbetermaatregelen

De onderzoeksresultaten wijzen verder op de noodzaak om een aantal centrale beheersaspecten verder te versterken, die nog niet al zodanig zijn geadresseerd binnen de Topstructuur, maar hier wel nauw op aansluiten, dan wel hier logisch uit voortvloeien. Die aanvullende maatregelen zijn niet alleen nodig om aan rijksbrede en wettelijke eisen te kunnen blijven voldoen, maar ook om in de toekomst adequaat te kunnen reageren op steeds complexere beveiligingsvraagstukken.

De in de vorige paragraaf beschreven, en op korte termijn aan te stellen CSO, zal de opdracht krijgen deze aanvullende maatregelen, binnen de kaders van de Topstructuur, nader uit te werken. De implementatie van de daaruit voortvloeiende veranderingen vormt de verantwoordelijkheid van het lijnmanagement. Het gaat om de volgende veranderopgaven:

- Sluit integrale beveiliging aan op de business en organisatiedoelen.
- Zorg voor structureel en gestructureerd risicomanagement.
- Versterk de beheersmechanismen tussen onderdelen.

Deze drie worden hieronder nader uitgewerkt.

3.3.1 *Sluit aan bij de business en organisatiedoelen*

Het onderzoek laat zien dat de concern beveiligingsdoelstellingen voornamelijk tactisch van aard zijn en nog niet goed aansluiten bij de doelstellingen van de organisatie en ontwikkelingen waar deze mee te maken heeft. De beveiligingsfunctie, onder aansturing van de CSO, zal in dat kader de volgende maatregelen uitvoeren of uitwerken:

ontwikkelen van een beveiligingsvisie en -strategie – Een beveiligingsvisie, -strategie en –ambitie mist op dit moment. Deze zullen worden uitgewerkt waarbij de inhoud nauw aansluit op de strategische doelstellingen en taakopdracht van de organisatie, verwachtingen van stakeholders en ontwikkelingen in wetgeving, techniek en maatschappij.

beveiliging levert een bijdrage aan organisatiedoelen – Behalve in de visie en strategie dient de relatie met de bedrijfsdoelstellingen, en de relatie met de business, tot uitdrukking te komen in de P&C cyclus, het reguliere risicomanagement proces en dagelijkse taakuitvoering van de beveiligingsfunctie. Deze zal moeten laten zien hoe het een zichtbare bijdrage levert aan het zekerstellen van de bedrijfscontinuiteit en het realiseren van strategische doelstellingen.

verbinden van beveiligingskaders aan bedrijfsarchitectuur – Ook op het niveau van processen en beleid zal de relatie met de business worden versterkt. Beveiligingskaders en daarmee samenhangende architectuurprincipes dienen daarvoor verbonden en geintegreerd te worden met de bedrijfsarchitectuur. Zo wordt geborgd dat beveiligingseisen structureel verweven worden in de reguliere bedrijfsprocessen van de organisatie. Tegelijk borgt dit dat de taakuitvoering van de organisatie voldoet aan alle relevante wettelijke en rijksbrede bepalingen.

3.3.2 *Groei naar structureel en gestructureerd risicomanagement*

Een volwassen integrale beveiliging richt zich op het tijdig en vooraf onderkennen van beveiligingsrisico's en continue beheersing ervan, in plaats van op het oplossen van incidenten. Dit vraagt om een structurele (d.w.z. regelmatig terugkerende) en gestructureerde vorm (d.w.z.

volgens een vast proces) van risicomanagement, aan de hand van een concernbreed geharmoniseerde werkwijze. De CSO zal de nadere uitwerking van de volgende verbetermaatregelen coördineren, in afstemming met Control, die verantwoordelijk is voor het algemene risicomanagement.

verantwoordelijkheden beleggen – Het gestructureerd uitvoeren van risicomanagement, zoals omschreven in rijksbrede beveiligingskaders[13], vereist dat verantwoordelijkheden en eigenaarschap helder zijn. Daarom dient voor alle IT diensten, informatiesystemen, informatieketens en ketenprocessen deze verantwoordelijkheid te zijn belegd. De betreffende functionaris is dan ook verantwoordelijk voor de beheersing van (beveiligings-)risico's.

beveiliging structureel in MT beleggen – Er worden stappen ondernomen die er toe leiden dat de behandeling van beveiligingsrisico's, -analyses, beheersmaatregelen en restrisico's een structureel en gestructureerd karakter heeft in de MT overleggen op concern, onderdeel- en afdelingsniveau. Dit betekent dat ten minste éénmaal per kwartaal beveiligingsaspecten op die MT tafels tot besluitvorming leiden, evenals de voortgang in de opvolging daarvan.

inzicht creëren – Op dit moment bestaat er binnen de organisatie geen goed actueel inzicht in het zich veranderende risicolandschap, in alle beveiligingseisen waar we aan moeten voldoen, de maatregelen die we dientengevolge dienen te implementeren, de mate waarin die zijn geïmplementeerd (*compliance*), en in de mate waarin die daadwerkelijk ook effectief en efficiënt zijn. Het ontbreken van dit inzicht maakt het voor lijnmanagers lastig om adequaat beveiligingsvraagstukken te besturen. De beveiligingsfunctie zal daarom samen met de lijnonderdelen en control op de genoemde punten het inzicht versterken en die inzichten vervolgens periodiek inbrengen op de MT tafels.

3.3.3 *Versterk beheersingsmechanismen tussen onderdelen*

Uit het onderzoek blijkt dat de onderdeel-overstijgende beheersing van integrale beveiliging verbetering behoeft. Dit omdat de beveiliging van het ene onderdeel afhankelijk is van de beveiliging bij andere, en besturingsmechanismen (reguliere afstemming, besluitvorming, inzichten e.d.) hiervoor nu grotendeels ontbreken. Deze besturing van interne ketenprocessen vormt ook een centraal thema in de Topstructuur. In de nadere uitwerking daarvan zal daarom met de ketenverantwoordelijken naar een effectieve vorm van afstemming en besluitvorming worden gezocht. De volgende aspecten krijgen hierin in ieder geval een plek.

Beter hanteerbaar maken van beveiligingsniveau – Het HBB kent een basis beveiligingsniveau dat generiek geldt voor alle onderdelen. Niet helder is nu 1) tegen welke risico's het wel en niet beschermt, 2) welke maatregelen precies geïmplementeerd moeten worden, 3) of onderdelen en diensten hier ook daadwerkelijk aan voldoen, 4) of en wanneer aanvullende maatregelen nodig zijn en 5) of/hoe het basis niveau afwijkt van het niveau dat externe ketenpartners hanteren. Het HBB zal zodanig worden aangepast dat op al deze punten helderheid

13 VIR 2007 en BVR 2013

bestaat. Ook zullen de onderdelen periodiek inzichtelijk maken dat zij en hun diensten aan dit basis niveau voldoen.

'generieke' diensten/componenten beveiligd op basis van centraal vastgestelde maatregelen – De organisatie kent verschillende diensten, processtappen of gegevensbestanden die door meerdere onderdelen worden gebruikt. Onderdelen weten nu onvoldoende of die diensten/componenten een beveiligingsniveau hebben welke past bij de risico's die zij in hun proces ervaren. Daarom wordt centraal vastgesteld aan welke eisen die componenten/diensten exact moeten voldoen. De leverancier/ eigenaar toont vervolgens aan de gebruikers aan dat alle maatregelen zijn geïmplementeerd, zodat zij kunnen bepalen of zij zelf nog aanvullende maatregelen moeten treffen.

het HBB toepasbaar en dienend – Het HBB, als verzamelwerk voor alle verplichte beveiligingskaders dient toegankelijker en laagdrempeliger te worden gemaakt, vooral ook voor partijen buiten de beveiligingsfunctie. Dit betekent dat meer aandacht wordt besteed aan communicatie (bijvoorbeeld in video's en wiki's) en specifiek op afnemersgroepen gericht voorlichtingsmateriaal. Waar nodig wordt de bestaande set MTHV's en uitvoeringsrichtlijnen uitgebreid.

Bijlage 1 Opdracht en uitvoering onderzoek

Opdracht van de directeur generaal Belastingdienst
De opdracht zoals geformuleerd in '20170309 Beveiligingsonderzoek opdracht def 1.0' luidt als volgt: *"De kern van de uit te voeren actie is een evaluatie van de huidige door Belastingdienst gehanteerde werkwijze ten aanzien van de concern brede control op de implementatie van het HBB, inbegrepen de door externen uitgevoerde onderzoeken. Het gaat hierbij om zowel de procedurele werkwijze als de inhoudelijke effectiviteit van beleidskaders. In deze evaluatie komen in ieder geval aan bod:*

A Procedureel
A1: Borging van HBB bij alle organisatie onderdelen en op management niveau de borging in P&C (plan do act check) en samenhang tussen de beheersmaatregelen en risicomanagement processen.
A2: Bestaat —vanuit de baselinebenadering door het HBB- voldoende aandacht voor bijzondere risicogebieden waarbij op grond van additionele risicoanalyses op basis van geïnventariseerde risico's geëigende maatregelen dienen te worden getroffen
- *Mate van onafhankelijkheid in de tot stand koming van HBB self assessments*
- *Wordt HBB procedureel of risk based gehanteerd?*

A3: Zijn de door externen uitgevoerde onderzoeken voldoende effectief qua maatregel in het licht van het systeem van zelfevaluaties en wordt voldoende follow-up gegeven aan de in de rapportages opgenomen aanbevelingen.
A4: Is het HBB compliant met externe beveiligingsmodellen?

B Inhoudelijk
B1: Mate van beleidsmatige onderbouwing van HBB, verankering in werkprocessen en MTHV's voor de IV-ketens. Zijn de kaders en normen passend, voldoende en werkbaar in een uitvoeringsinstantie?
B2: Zijn de adviezen van de door externen uitgevoerde onderzoeken voldoende effectief vertaald in beleid, kaders en richtlijnen.
B3: Zijn de beveiligingsdoelstellingen van de dienstonderdelen inhoudelijk in lijn met
de prioriteiten in de jaarcyclus.
B4: Impact van aanbevelingen AP en forensisch onderzoek.
B5: Impact van AGV, meldpunt data lekken, vertrouwenspersonen, integriteitscoördinatoren.

Uitvoering onderzoek
Het onderzoek is uitgevoerd in de periode maart-juli 2017, op basis van een daartoe uitgewerkt Plan van Aanpak. In deze periode is documentstudie uitgevoerd, een schriftelijke vragenlijst uitgezet bij de verschillende bedrijfsonderdelen en zijn interviews gehouden, waaronder met de directeuren van de bedrijfsonderdelen. De verslagen en uitkomsten hiervan zijn ter review voorgelegd aan de verschillende betrokken partijen, om zo de inhoudelijke juistheid van de bevindingen te borgen.

Voorts zijn de (concept) bevindingen en eindrapportage voorgelegd aan een daartoe ingestelde Review Committee, bestaande uit 1) de Rijksbeveiligingsambtenaar (RijksBVA), de 2) Beveiligingsambtenaar van het ministerie van Financiën, de 3) de CISO van he ministerie van BZK en 4) de functionaris gegevensbescherming (FG) van het ministerie van Financiën. Doel hiervan was om de:

- kwaliteit en juistheid van de analyse;
- samenhang met overige ontwikkelingen binnen het ministerie van Financiën, en
- samenhang met Rijksbrede ontwikkelingen op het gebied van integrale beveiliging, te borgen.

De Auditdienst Rijk (ADR) heeft daarnaast het verloop van het onderzoekstraject gevolgd, alsmede de gekozen onderzoeksaanpak en uitvoering daarvan. De ADR rapporteert hierover separaat.