Ministerie van Financiën

# Handboek Beveiliging Belastingdienst

## Deel B
## Algemene Uitvoeringsrichtlijnen

Mei 2011

## Inhoudsopgave

## Algemene uitvoeringsrichtlijnen

Leeswijzer

In deel B van het Handboek Beveiliging Belastingdienst worden uitvoeringsrichtlijnen voor beveiliging uitgewerkt op basis van deel A, het strategisch kader. Het betreft tactische beleidsuitgangspunten en beveiligingsrichtlijnen, die voor de hele organisatie van de Belastingdienst gelden. De organisatie van beveiliging wordt op basis van het strategisch kader uitgewerkt.
Daarnaast staan zogenaamde views op de normen beschreven, die zicht geven op Deel C vanuit verschillende invalshoeken. Hiermee kunnen de normen naar toepasselijkheid worden gefilterd. Verder wordt toelichting gegeven op de structuur en het gebruik van de normen. De *Verklaring van toepasselijkheid*, zoals vereist vanuit de standaarden, is in hoofdstuk B.8 opgenomen.

Beheer HBB

Het inhoudelijk beheer van het HBB wordt gevoerd door de aspectclusters en goedgekeurd door het Tactisch Beveiligingsoverleg. Hieronder valt ook de verwerking van eventuele wijzigingen in de gebruikte standaarden en best practices.

Updatefrequentie

Minimaal één maal per kalenderjaar worden wijzigingen in het HBB formeel doorgevoerd. Dit betreft bijvoorbeeld updates, verwerking van wijzigingen in de standaarden of rijksoverheidskaders, input uit implementatieresultaten en voortschrijdend inzicht.

Brondocument

In het eerste TBO van een kalenderjaar wordt de nieuwste versie vastgesteld. De meest actuele en leidende versie van het HBB is de digitale (web)versie op Belastingnet. De redactie en het technisch beheer is belegd bij de strategisch beveiligingsadviseurs van DGBel.

## B.1. Tactisch kader beveiliging

Het strategisch kader beveiliging geeft de belangrijkste beleidsmatige uitgangspunten voor beveiliging. Ze zijn ingegeven door de beveiligingsprincipes en liggen in het verlengde van de kwaliteit van de gehele bedrijfsvoering van de Belastingdienst. Ze worden benaderd vanuit de aspecten *personele veiligheid en integriteit*, *fysieke beveiliging*, *informatiebeveiliging* en *bedrijfscontinuïteit*.

Positie tactisch kader beveiliging

Het tactisch kader beveiliging geeft de algemene uitvoeringsrichtlijnen en beleidsuitgangspunten voor de inrichting van beveiliging, waarbij rekening wordt gehouden met de gescheiden verantwoordelijkheid ten opzichte van de uitvoering: ze hebben namelijk voor het merendeel betrekking op verschillende aspecten tegelijk, waarbij de samenhang geborgd moet zijn. Zodoende kan de verantwoordelijkheid voor een enkele maatregel uit het samenhangende stelsel op hoger lijnniveau worden gepositioneerd.

Code voor Informatiebeveiliging

De beleidsuitgangspunten en uitvoeringsrichtlijnen in dit tactisch kader zijn in eerste instantie geordend naar de beleidsthema's die volgen uit de Code voor Informatiebeveiliging ISO-NEN 27002. Het volgen van de thema's uit deze standaard zorgt voor een universele, organisatieonafhankelijke en uitwisselbare opzet.
Daar waar het van toepassing is, wordt de samenhang over de aspecten heen aangegeven.

### B.1.1. Beleid voor het classificeren van informatie

De Belastingdienst hanteert een niveau van beveiliging dat gericht is op de beveiliging van massale verwerking van persoons- en financieel-economische gegevens, overeenkomend met de door het College Bescherming Persoonsgegevens beschreven risicoklasse II, verhoogd risico. Hiermee is dit niveau van beveiliging gemiddeld genomen voor alle informatiesystemen tevens het basisniveau omdat voor wat betreft beveiliging de processen en gegevens voor een groot deel gelijkwaardig zijn. Een voordeel hiervan is dat het basisniveau beveiliging met generieke normen kan worden ingevuld. Dit vereenvoudigt het beheer en beperkt de kosten.
Binnen het basis beveiligingsniveau is op onderdelen wel sprake van differentiatie in beveiligingsniveau, zoals bij de fysieke, logische en netwerkzonering. Bij netwerkzonering hanteren we modellen die in de normering zijn uitgewerkt. Zie daarvoor ook bijlage B.I., patronen.
Daarnaast is ook sprake van differentiatie bij papieren en elektronische gegevens met een verhoogd risico, bijvoorbeeld bij gegevens van bedrijven waarvan de Belastingdienst koersgevoelige informatie bezit. In die gevallen worden per dienstonderdeel onder verantwoordelijkheid van het desbetreffende management aanvullende maatregelen getroffen m.b.t. procedures en personeel.
Bij de Belastingdienst wordt in de regel geen bijzondere informatie volgens het VIR-GI[1] gegenereerd, met uitzondering van de recherchegegevens van de FIOD. Met betrekking tot die gegevens worden op basis van ketenafspraken met andere inspectiediensten afzonderlijke maatregelen getroffen ter voldoening aan het VIR-GI.

. . . . . .
[1] Voorschrift Informatiebeveiliging Rijksdienst - Gerubriceerde Informatie, voorheen VIR - BI (i.c. Bijzondere Informatie).

Voor zover de Belastingdienst verder bijzondere informatie onder zich heeft, bestaat deze uit als zodanig geclassificeerde bijzondere informatie, welke is aangeleverd door andere handhavingspartners.
Informatie die de Belastingdienst aan bijzondere informatie van derden toevoegt, valt daarmee onder die rubricering. In principe wordt geen bijzondere informatie in digitale vorm door de Belastingdienst ontvangen of verzonden.

Vertrouwensfuncties

In de Belastingdienst zijn vertrouwensfuncties aan te wijzen. Over het algemeen is een vertrouwensfunctie een functie waarin wordt gewerkt met gevoelige informatie die, indien deze in verkeerde handen valt, de nationale veiligheid kan schaden.
Een functie wordt aangewezen als vertrouwensfunctie indien sprake is van tenminste één van de volgende drie criteria volgens de *Leidraad aanwijzing vertrouwensfuncties 2011* van de AIVD:
- Functies waarin het noodzakelijk is te werken met staatsgeheimen;
- Functies waarin door integriteitsaantastingen de nationale veiligheid in het geding kan zijn;
- Functies die van vitaal belang zijn voor de instandhouding van het maatschappelijk leven.

De Belastingdienst sluit zich bij deze richtlijn aan. Daarnaast worden veiligheidsonderzoeken ingesteld indien de samenwerking met externe partners dit vereist.

Vips

Tenslotte geldt voor de Belastingdienst een aparte classificatie voor *very important persons* (vips)[2]. De beveiligingsmaatregelen behorend bij die gegevensklasse worden afzonderlijk in de normatiek uitgewerkt.

### B.1.2. Beleid voor bedrijfscontinuïteit

De Belastingdienst heeft kritische bedrijfsfuncties benoemd op basis van de aan hem opgedragen wettelijke uitvoeringstaken, maar ook bijvoorbeeld op basis van impact en risico's op imagoschade, maatschappelijke onrust of politieke invloed uit binnen- of buitenland. De keuze voor kritische functies die de Belastingdienst aan de hand van deze criteria heeft gemaakt is de volgende:
- Alle teruggaafprocessen naar burgers en/of bedrijven;
- Communicatiemiddelen naar burgers, bedrijven en eigen personeel;
- De stopfunctie van Douane;
- Fysiek toezicht Douane;
- Transit Douane;
- Toeslagen.

Calamiteitenplannen

De bij BCM gehanteerde calamiteitenplannen richten zich op landelijke en regionale doelgroepen. De actuele versie van een calamiteitenplan wordt over meerdere personen verspreid. Dit betreft in ieder geval portiers, het hoofd BHV en plaatsvervanger, de voorzitter van het crisisteam en de beveiligingsmedewerkers.
De calamiteitenplannen worden periodiek getest:
- Complete crisismanagementplan tenminste één keer per jaar;
- Beschikbaarheid leden crisisteam tenminste één keer per kwartaal;
- Continuïteitsplan tenminste één keer per jaar;
- Evaluatie van de kritische bedrijfsactiviteiten één keer per jaar;
- Crisisteam tenminste één keer per jaar.

[2] Het beleid voor vips en ambtenarenposten wordt in 2011 geactualiseerd.

### B.1.3. Beleid voor functiescheiding

Het scheiden van functies als onvervangbare basismaatregel voor een betrouwbare informatievoorziening volgt in principe de arbeidsverdeling van de organisatie. In het normenkader voor het basis beveiligingsniveau zijn daartoe overal in de verschillende processen gedetailleerde uitgangspunten opgenomen. Globaal gelden de volgende functiescheidingen:

- tussen bewarende, registrerende, beslissende, uitvoerende en controlerende taken;
- tussen beleid en uitvoering;
- tussen gebruikersorganisatie en facilitaire organisatie: huisvesting (i.v.m. fysieke beveiliging) en levering van ICT;
- tussen ontwikkeling en productie in leveren ICT;
- met betrekking tot processen en ICT tussen functioneel, technisch en operationeel beheer.

Binnen de bedrijfsvoering ofwel primaire processen van de Belastingdienst is het in veel gevallen noodzakelijk functiescheidingen door te voeren, die niet generiek kunnen worden aangeduid. Kerngedachte is hierbij, dat niemand een gehele procescyclus mag beheersen voor zover die gebruikt zou kunnen worden voor het beïnvloeden van de geldstroom. In de situatie dat medewerkers flexibel op alle voorkomende taken binnen een dienstonderdeel worden ingezet, is een kernuitgangspunt, dat conflicterende taken niet voor één zaak/dossier mogen worden uitgevoerd. De maatregelen voor logische toegangsbeveiliging moeten dit dan verhinderen, door de vervulling van taken per zaak/dossier per medewerker te registreren en te controleren.

### B.1.4. Toegangsbeleid

Toegangs*beleid* is essentieel voor de veiligheid van medewerkers en bezoekers en voor de beveiliging van gegevens en goederen. Het begrip *toegang* omvat niet alleen de toegang van medewerkers tot kantoren en systemen maar ook de manieren van toegang van burgers, ondernemers, intermediairs en ketenpartners tot informatie en processen van onze organisatie.

Toegang tot informatie

Maatregelen op dit vlak zijn zowel fysiek als logisch van aard en worden als een geheel beschouwd en benaderd. Het principe hierbij is *vertrouwen voorop*, niet alleen in de eigen medewerker maar ook in burgers en bedrijven, samenwerkingsverbanden en ketenpartners. Tenslotte sluiten we met toegangsbeleid zoveel mogelijk aan bij ontwikkelingen zoals de Rijkspas, rijkswerkplek, DigiD en het rijksoverheidsbreed identity management.

Beheer van identiteiten

Beveiliging is in sterke mate afhankelijk van het op orde zijn van identiteiten en autorisaties. Het beheren van (digitale) identiteiten en toekennen van autorisaties gebeurt daarom zoveel mogelijk geautomatiseerd en generiek voor alle systemen, waarbij overbodige autorisaties worden verwijderd en conflicterende autorisaties direct worden gesignaleerd zodat adequate maatregelen getroffen kunnen worden.

Toegangs*beheer* richt zich op het verlenen van toegang aan personen tot de gebouwen, de informatieverwerkende systemen, de gegevens die daarin worden verwerkt en opgeslagen en andere bedrijfsmiddelen. Het beheerproces beschermt deze gebouwen, systemen, gegevens en bedrijfsmiddelen tegen onbevoegde toegang, raadpleging, mutatie of oneigenlijk gebruik en houdt rekening met de verschillende toegangsbeveiligingsrollen (toegangsverzoek, -autorisatie en -administratie).

### B.1.4.1. Beleid voor fysieke toegang

Het fysieke toegangsbeleid is er op gericht om gebouwen en informatie te beschermen door ongeautoriseerde toegang te voorkomen. Het voorziet mogelijkheden voor het leveren van beveiligde ruimten, gecontroleerde omgevingen en beveiliging van bedrijfsmiddelen. Eén en ander wordt beschouwd vanuit de samenhang tussen risicoprofielen, zonering, werkbaarheid en gedrag.

Brede toegang

Belastingdienstmedewerkers hebben in principe toegang tot alle gebouwen van de Belastingdienst. Gebouwen zijn ingericht volgens de rijksbrede normen voor zonering op basis van te beschermen belangen. Er zijn specifieke zones waar alleen geautoriseerd personeel mag komen. Zonering vervangt compartimentering, die niet meer wordt toegepast. Het management kan bewust van dit principe afwijken als daar gegronde redenen voor zijn.

Medewerker is geen bezoeker

Eigen medewerkers worden niet als bezoeker aangemerkt. Alleen aan niet-belastingdienstmedewerkers worden bezoekerspassen verstrekt. Aanmeldingen voor het "bezoek" van eigen medewerkers kunnen achterwege blijven, ze zijn ook onaangekondigd welkom in een gebouw. Hiermee lopen we gelijk op met de ontwikkeling van de Rijkspas.

Brandveiligheid

Een bijzonder aspect is brandveiligheid, aanvullend gericht op de bescherming van personeel, bezoekers en de omgeving van gebouwen. Hier is de wet- en regelgeving leidend, waaraan we dienen te voldoen.

### B.1.4.2. Beleid voor logische toegang

Het toekennen en intrekken van autorisaties gebeurt op basis van de werkprocessen binnen en buiten de organisatie.

**In het organisatiedomein**
- Volgend uit de eisen uit de bedrijfsvoering en het personeelsbeleid: het dienstverband, de plaats in de organisatie en de functie van medewerkers zoals die is geregistreerd in SAP-HR;
- Gekoppeld aan de werkzaamheden die de manager toewijst aan een medewerker in de vorm van bedrijfsrollen en bijzondere taken (Role Based Access). De manager is verantwoordelijk voor de toegang van de eigen medewerker tot bedrijfsmiddelen.

**In het rijksoverheidsdomein**
- Volgend uit de eisen gesteld aan al dan niet formele samenwerkingsverbanden, waaronder de generieke rijkswerkplek;
- Volgend uit de eisen gesteld in wet- en regelgeving.

**In het externe domein**
- Volgend uit de eisen gesteld aan uitvoeringstaken met ketenpartners (anders dan rijksoverheid);
- Volgend uit de eisen gesteld aan externe communicatie-, gegevensuitwisselings- en dienstverleningskanalen;
- Volgend uit de eisen gesteld in wet- en regelgeving.

Autorisatieprofielen

Hierbij wordt op basis van *need-to-do* en *need-to-know* gewerkt (zie A.2, Beveiligingsprincipes). Eén en ander is vastgelegd in organisatiebrede en formeel vastgestelde autorisatieprofielen, aan de hand waarvan autorisaties worden toegekend. Hierbij geldt dat welke autorisaties een medewerker mag hebben een gezonde balans is tussen niet teveel diversiteit aan

mutatierechten (beperken van kans op misbruik) en het zoveel mogelijk toepassen van organisatiebrede profielen (eenvoud van beheer).
De autorisatieprofielen differentiëren naar bedrijfstoepassing, privacybescherming, doelbinding en classificatie van gegevens.

### B.1.4.3. Beleid voor controle op gebruik van autorisaties

Autorisaties geven toegang tot (geautomatiseerde) bedrijfsmiddelen. Bedoeld of onbedoeld misbruik hiervan moet kunnen worden gesignaleerd zoals bij het onbevoegd raadplegen (need-to-know) of onbevoegd muteren (need-to-do) van gegevens. Dat geldt ook buiten de grenzen van de organisatie zoals op internet. Hiertoe zijn procedures vastgesteld, waarbij het resultaat ervan regelmatig wordt beoordeeld.

Privileges

Autorisaties die hierbij bijzondere aandacht behoeven zijn de privileges, autorisaties waarmee het mogelijk is interne elektronische informatie buiten het (beveiligings)domein van de Belastingdienst te brengen en vice versa.

### B.1.5. Beleid voor informatieuitwisseling

Vanuit informatie gezien

Informatieuitwisseling omvat zowel in- en uitgaande informatie, langs alle kanalen zoals post, telefoon of elektronisch, formeel of informeel.
Enerzijds geldt voor de Belastingdienst als organisatie dat hij gehouden is aan de relevante wet- en regelgeving over de bescherming van vertrouwelijke gegevens en (elektronische) informatieuitwisseling.
Anderzijds gelden er voorschriften voor de medewerkers, gericht op plichten als geheimhouding en gewenst gedrag. Met name in de contacten met burgers en bedrijven wordt hier aandacht aan besteed binnen de dienstverleningsstrategie. We hanteren de volgende uitgangspunten:

- Uitwisseling van informatie met een wettelijke grond, met ketenpartners, gebeurt op basis van de bestaande wet- en regelgeving. We voldoen hieraan en stellen geen aanvullende eisen.
- Andere uitwisseling van zakelijke informatie gebeurt onder het treffen van adequate generieke maatregelen ten aanzien van vertrouwelijkheid of rechtsgeldigheid, om bijvoorbeeld de privacy, authenticiteit of onweerlegbaarheid te borgen.
- Voor alle andere uitwisseling van informatie gelden voorwaarden en gedragsregels.

We presenteren veel gegevens aan burgers, bedrijven en overheden. Maar alleen de benodigde gegevens en alleen aan personen en organisaties waarvan we een bepaalde zekerheid hebben omtrent de identiteit en bevoegdheid. Ook letten we op welke gegevens fraudegevoelig kunnen zijn omdat we de drempel voor mis- en oneigenlijk gebruik van elektronisch berichtenverkeer niet willen verlagen. We sluiten aan op de overheidsbreed ontwikkelde voorzieningen als DigiD en eHerkenning.
We vertrouwen onze medewerkers bij het muteren en vastleggen van gegevens. Onze gegevens zijn altijd vertrouwelijk. Het is in ons eigen belang dat we de aan ons toevertrouwde gegevens beschermen tegen ongeautoriseerde inzage of mutatie en dat de in- en uitgaande gegevens betrouwbaar zijn. We kiezen hierbij voor algemene authenticatiemiddelen met een beperkt aantal niveaus. Afhankelijk van de doelgroep maken we ruimte voor extra maatregelen.

Aanvullend gelden, voor alle uitwisseling, voorschriften als het ARAR en het RPVB. Specifieke voorwaarden, bijvoorbeeld voor het gebruik van e-mail of

informatie van internet, houden rekening met deze invalshoeken met aandacht voor samenhang en werkbaarheid (zie ook B.1.7).
Deze aspecten dienen breed in de bedrijfsvoering te worden verankerd.

Vanuit domein gezien

Naast de bovenstaande inhoudelijke indeling, kan ook een logische indeling worden gemaakt. De invalshoek is er dan één vanuit het organisatiedomein, waarbij domein vertaald kan worden in *invloedssfeer* in de zin van fysieke bescherming en beheer:

- Uitwisseling van informatie met partijen *buiten* het domein van de Belastingdienst. Deze uitwisseling gebeurt met burgers, ondernemers en andere (overheids)partijen en betreft informatie uit het primaire proces. Zodra de informatie buiten het domein van de Belastingdienst is, hebben we minder invloed op risicomitigerende maatregelen. We hanteren afspraken voor transport, opslag en verwerking.
- Uitwisseling van informatie *binnen* het domein van de Belastingdienst. Hiervoor geldt het basisniveau beveiliging.

Binnen domein, buiten basis beveiligingsstelsel

We transporteren gegevens in eerste instantie over lijnverbindingen. Alleen als dit niet mogelijk is maken we gebruik van andere (fysieke) middelen.
Op momenten dat gegevens *buiten* de invloedssfeer van onze medewerkers zijn, treffen we extra beveiligingsmaatregelen. Dat geldt niet alleen bij gestructureerde gegevensuitwisseling maar ook bij een laptop, CD/DVD, USB-stick, papier of met externe e-mail.
We transporteren niet onnodig gegevens, verstrekken geen onnodige autorisaties en we bieden hard- en softwarematige voorzieningen aan zoals versleuteling, de BioSlimdisk als USB-stick en hanteren heldere voorwaarden en gedragscodes voor het gebruik er van.

Bij alle elektronische informatieuitwisseling van en naar *buiten* het belastingdienstdomein wordt op schadelijke programmatuur gecontroleerd en gescand (virussen, malware etc, ook op versleutelde stromen) en wordt de grens van het domein beschermd en gecontroleerd tegen aanvallen van binnen en buiten. Hierbij worden de richtlijnen die binnen de rijksoverheid gelden (o.a. GOVCERT.NL) gevolgd en worden adequate middelen ingezet.
We slaan zelf geen gegevens op buiten onze invloedssfeer.

Mobiele apparatuur

Een bijzondere vorm informatieuitwisseling *binnen* het domein zie je bij draagbare apparatuur (PDA's, Smartphones, USB-sticks en draagbare computers (PPC's)). Deze apparatuur kan fungeren als informatiedrager, die weliswaar binnen het domein van de Belastingdienst valt, maar buiten de beschermende invloedssfeer ervan kan verkeren. Hiervoor treffen we extra beveiligingsmaatregelen: We transporteren ook hier niet onnodig gegevens, verstrekken geen onnodige autorisaties en we bieden hard- en softwarematige voorzieningen aan zoals *externe media encryptie*. Daarbij zijn we kritisch op de noodzaak van het gebruik van een bedrijfsmiddel, koppelen dat bij voorkeur aan een functie en zien er op toe dat de extra maatregelen ook daadwerkelijk worden gebruikt.

Een andere bijzondere verschijningsvorm *binnen* het domein betreft telewerken/thuiswerken. De apparatuur die hiervoor gebruikt wordt valt buiten de invloedssfeer van de Belastingdienst, terwijl de functionaliteit er binnen valt. Hier treffen we eveneens adequate aanvullende maatregelen voor bijvoorbeeld de verbinding en het desbetreffende apparaat (eisen aan de browserversie, versleuteling, wissen van elektronische sporen etc, gedragsvoorschriften).

Label, logo of merk

Voor al de *bedrijfsmiddelen* die in dit kader worden gebruikt, geldt dat de herkenbaarheid als belastingdiensteigendom minimaal moet zijn.

Uitwisseling en verwerking van informatie in het primair proces, ook binnen de eigen organisatie, is gebonden aan de wet- en regelgeving voor wat betreft privacy en doelbinding. Koppeling van geautomatiseerde systemen gebeurt met inachtneming hiervan.

Koppeling van systemen

Bij de koppeling van kantoorautomatiseringssystemen ontstaan risico's voor bijvoorbeeld controlemedewerkers, rechercheurs, vertrouwenspersonen, bedrijfsartsen en OR-leden (toegankelijkheid tot e-mail, agenda). Deze worden opgevangen door huisregels, houding en gedrag. Dit hoort thuis in de regionale risicoanalyse en valt onder het desbetreffende management van een dienstonderdeel.

### B.1.6. Beleid voor telewerken/thuiswerken

Telewerken in de zin van plaats- en tijdsonafhankelijk werken zal in onze organisatie een prominentere rol krijgen. Hierin sluiten we aan bij de tendens in de rijksdienst, waarin actief wordt ingespeeld op de mogelijkheden die de ICT biedt. De Raamregeling Telewerken[3] is ook voor onze organisatie van toepassing.

Vrijwilligheid

Deze regeling staat echter los van de beleidsmatige wenselijkheid van telewerken, waarbij de medewerker werkzaamheden verricht in of vanuit zijn of haar woning. Zo gauw deze werkvorm niet is vereist vanuit de functie van een medewerker, wordt deze per definitie op basis van vrijwilligheid toegepast. De raamregeling geeft wel meer duidelijkheid over de rechtspositionele aspecten van telewerken zodat toepassing ervan op dat vlak zorgvuldig kan gebeuren.

Telewerken wordt in onze organisatie uitsluitend op basis van vrijwilligheid toegepast: het is geen recht. Maar het is ook geen plicht: er zijn bijvoorbeeld geen functies waarbij de plaats van tewerkstelling de woning van de medewerker is. De organisatie is niet verplicht om telewerkvoorzieningen te verschaffen.

Keuze aan dienstonderdeel

Zoals de raamregeling ook voorstaat, worden afspraken over de invoering van telewerken het best op decentraal, dat wil zeggen op dienstonderdeelniveau, gemaakt. Uiteindelijk wordt de afweging tot telewerken door leidinggevende en medewerker samen gedaan.

Telewerken sluit aan bij de mogelijkheden die de Digitale Werkplek Belastingdienst[4] (DWB) biedt. DWB is gericht op plaats-, tijd- en apparaatonafhankelijk werken en houdt eveneens rekening met de eisen die aan de mobiliteit van de medewerkers worden gesteld vanuit de organisatiegerichte huisvesting.

De functionaliteit van DWB wordt uiteindelijk gekoppeld aan *digitale profielen* van onze medewerkers, waarbij beheer en beheersing van risico's is ingeregeld. In principe is de functionaliteit ontkoppeld van het gebruikte soort apparaat.

Telewerken is in eerste instantie gericht op toegang vanaf niet-Belastingdienst apparaten tot de interne algemene informatiebronnen (intranetten), e-mail en agenda. Voorts kan telewerken worden ingericht met behulp van Belastingdienst apparaten (managed devices) of eigen

. . . . . .

[3] Raamregeling Telewerken 1 juni 2001, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

[4] De Digitale Werkomgeving Belastingdienst volgt de Digitale Werkomgeving Rijksdienst.

(Un)managed devices

apparaten (bring your own device), waarbij toegang tot bedrijfsapplicaties tot de mogelijkheden behoort.

Extra bescherming

Er dienen afdoende en zoveel mogelijk generiek aanvullende maatregelen te worden getroffen. Denk in de techniek aan *browsercache-cleaners* waarmee informatie die ongemerkt is achtergebleven wordt verwijderd en *host-checkers* die vooraf controleren of een platform op een afdoende onderhouden niveau zit of dat vereiste antivirusmaatregelen zijn getroffen. Dienstonderdelen kunnen bepaalde vormen van telewerken verbijzonderen en daarbij aanvullende maatregelen treffen.

Randvoorwaarden telewerken

Telewerken stelt het vertrouwen in de medewerker centraal, zowel wat betreft integriteit, houding en gedrag, als op het gebied van beveiliging. Aanvullend vindt de toegang tot het bedrijfsnetwerk minimaal plaats op basis van twee-factor authenticatie en versleuteling en worden er minimumeisen gesteld aan de apparaten waarmee toegang wordt verkregen, waarbij verplichte installatie van Belastingdienst-controleprogrammatuur tot de mogelijkheden behoort. Daarnaast gelden er (gedrags)voorwaarden aan het gebruik van voorzieningen voor telewerken.

Taak- of kenniswerker, mobiel of op kantoor

De digitale profielen sluiten in de basis aan bij de vier typologieën die voor de medewerkers worden gehanteerd in de Meerjarenvisie Huisvesting: de taakwerker en kenniswerker op kantoor en de mobiele taakwerker en kenniswerker. Elke groep heeft specifieke eisen voor wat betreft functionaliteit en eisen die vanuit de organisatie worden gesteld. De invulling van de eisen moet met behulp van profielen en privileges worden beheerd.

### B.1.7. Beleid op het gebruik van sociale media, internet en e-mail

Geheimhoudingsplicht

Het gebruik van internet is niet zonder risico's. E-mailberichten kunnen door veel partijen worden gelezen of gewijzigd. Het vinden van informatie is eenvoudig, maar we weten vaak niet of die informatie ook betrouwbaar is. Een bijdrage aan een discussie kan jaren blijven bestaan. Als je informatie naar buiten brengt, kan dat leiden tot het niet nakomen van de geheimhoudingsplicht. Ook mag je geen standpunt innemen dat het goed functioneren van jezelf in je functie of de overheid belemmert.

E-mail wordt in de basis niet gebruikt voor de uitwisseling van vertrouwelijke informatie of formele berichten. De vertrouwelijkheid en authenticiteit van het bericht kan niet voldoende gewaarborgd worden, waarmee de geheimhoudingsplicht in het geding komt. Zulke berichten dienen op de gebruikelijk manier, zoals per post, te worden verzonden.
Als we vooraf aanvullende maatregelen hebben getroffen en afspraken hebben gemaakt ten aanzien van het borgen van vertrouwelijkheid en authenticiteit van een bericht, kunnen we e-mail wél hiervoor gebruiken.

Goed ambtenaarschap

In het gebruik van internet, e-mail en online communicatie wordt van de medewerkers *goed ambtenaarschap* verwacht. Daarom stelt de Belastingdienst voorwaarden aan het gebruik van internet. Ze zijn gebaseerd op het Reglement Personeelsvoorschriften Belastingdienst en geven een nadere invulling aan het begrip *goed ambtenaar* zoals bedoeld in artikel 50 van het Algemeen Rijksambtenarenreglement.

Daarnaast heeft het Ministerie van Algemene Zaken in juni 2010 de *Uitgangspunten online communicatie rijksambtenaren* gepubliceerd. Deze uitgangspunten volgen we en zijn samen met het bovengenoemde

opgenomen in de in mei 2011 vastgestelde *Voorwaarden aan het gebruik van e-mail, internet en online communicatie*.

### B.1.8. Beleid op de bestrijding van computercriminaliteit

Cybercrime

Onder computercriminaliteit of cybercrime verstaan we alle vormen van criminaliteit die betrekking hebben op computersystemen of die met computersystemen (inclusief netwerken) worden gepleegd, zowel van binnen als van buiten de organisatie. Het gaat om (georganiseerde) criminele activiteiten waarbij gebruik wordt gemaakt van ICT.
Ze zijn gericht tegen personen, eigendommen of organisaties, of tegen elektronische communicatienetwerken en informatiesystemen.

We bestrijden computercriminaliteit door:
- Het versterken van detectie van interne en externe computercriminaliteit via monitoring van informatiesystemen, het alert maken van de medewerkers en de melding van mogelijk strafbare feiten;
- De afhandeling van meldingen, verstoringen en incidenten niet alleen gericht te laten zijn op continuïteit van de bedrijfsvoering, maar ook op het verzamelen van bewijsmateriaal en het veiligstellen van gegevens die kunnen helpen bij opsporing, vervolging en het eventueel verhalen van schade;
- Aansluiting te hebben met GOVCERT.NL en het doen van aangifte van computercriminaliteit bij de politie.

### B.1.9. Managementverantwoordelijkheid voor gedrag personeel

Het management bevordert dat werknemers, ingehuurd personeel en externe gebruikers van interne systemen beveiliging toepassen overeenkomstig het vastgestelde beleid en de vastgestelde procedures.
Het aanvaardbaar gebruik van bedrijfsmiddelen wordt daarbij uitgelegd, samen met het *clear desk* beleid voor fysieke middelen en *clear screen* beleid dat we voor IT-voorzieningen voeren.

### B.1.10. Arbeidsvoorwaarden

De algemene voorwaarden van het arbeidscontract van werknemers en ingehuurd personeel bevatten de wederzijdse verantwoordelijkheden ten aanzien van beveiliging.
Het beveiligingsbeleid wordt verduidelijkt aan de hand van de samenhang in beveiliging, waarbij in ieder geval onderwerpen als de geheimhoudingsovereenkomst en disciplinaire maatregelen aan bod komen.

### B.1.11. Identificatie van toepasselijke kaders

De relevante wettelijke en regelgevende eisen worden vastgesteld en actueel gehouden in het strategisch kader beveiliging (Deel A).

## B.2. Betekenis van het basis beveiligingsniveau

### B.2.1. Risicobeoordeling

Subsidiariteit

Voor het merendeel van de “normale” processen en ondersteunende informatiesystemen (VIR 2007) kunnen maatregelen worden getroffen volgens het basis beveiligingsniveau. Specifieke maatregelen worden getroffen op basis van een risicoafweging. Specifieke maatregelen zijn nodig als de kenmerken van de processen en ondersteunende informatiesystemen afwijken van de “normale”, op grond waarvan het basisniveau is samengesteld. Afwijkende situaties hebben betrekking op een ander dan het hier geformuleerde dreigingenprofiel, maar kunnen ook betrekking hebben op hogere beschikbaarheidseisen, anders dan standaard gebruik van de technologie, toepassing van nieuwe technologie, gegevens met een bijzonder belang, etc.

Proportionaliteit

Randvoorwaarden

Stelsel van maatregelen

Er zijn meer factoren op grond waarvan er in specifieke situaties afgeweken kan worden van de basismaatregelen: te hoge kosten, onvoldoende haalbaarheid, de mate van effectiviteit in de specifieke situatie, de ouderdom van het gebouw of van het informatiesysteem, etc. Die factoren worden hier samengevat onder het begrip *randvoorwaarden*. Bij het niet-implementeren van maatregelen op het basisniveau zal eveneens een risicoafweging moeten plaatsvinden: weegt de besparing van de maatregel op tegen de kans van het optreden van de dreiging, waartegen de maatregel een bijdrage levert. Hierbij speelt mee dat er meestal ook andere maatregelen zijn, die een bijdrage leveren aan het beperken van het risico.

Restrisico’s

Bij een risicoafweging worden de speciale bedreigingen benoemd en in kaart gebracht. Per bedreiging wordt de kans van het optreden ervan bepaald. Vervolgens wordt nagegaan wat de schade is die zou kunnen optreden als een bedreiging zich daadwerkelijk voordoet. Daarna worden analyses gemaakt van de kosten van te treffen maatregelen versus de baten van de hiermee te vermijden schaden of wordt bezien of de risico’s kunnen worden vermeden, bijvoorbeeld door een andere procesimplementatie of het gebruik van beter beveiligbare ICT-middelen.
Tenslotte worden de restrisico's door het management geaccepteerd. Op basis van de onderkende risico's van de specifieke situatie die bij een proces en ondersteunend informatiesysteem aan de orde kan zijn, worden compenserende maatregelen (extra maatregelen, bovenop het basisniveau en in relatie tot het stelsel) getroffen.

Methoden en standaarden

Vakkundigheid

Voor het doen van risicoafwegingen in het algemeen bestaan vele methoden, standaarden en nog veel meer praktische uitwerkingen daarvan in de markt. Vooralsnog is er geen standaard methode ontwikkeld, die zich richt op specifieke bedreigingen bovenop de “normale” waarop het basisniveau is gebaseerd. Het is de vraag of dat nodig is als er voor het treffen van extra maatregelen geput kan worden uit de maatregelensets, die ontwikkeld worden vanwege toepassing van het VIR-GI. Het beoordelen welke extra maatregelen geschikt zijn om de extra bedreigingen af te dekken is een zaak van vakkundige beoordeling en het rekening houden met de randvoorwaarden. Er is geen methode die dat beoordelingsproces kan overnemen, anders dan hetgeen hierover in de toelichting op de normen van het basisniveau is gezegd.

### B.2.2. Pas toe of leg uit

Voor de kaderstelling van beveiliging zijn twee benaderingen mogelijk:
- risicomanagement, gepaard met een slank beveiligingskader gekoppeld aan een degelijke verantwoordingsplicht of
- een lijviger beveiligingsnormenkader en een beperktere verantwoordingsplicht. Impliciet daarbij is de keuze voor het beginsel *comply or explain* (pas toe of leg uit).

Comply or explain

De Belastingdienst kiest nadrukkelijk voor de tweede benadering.

Verplichte beheers-maatregelen, te volgen implementatierichtlijnen

In hoeverre zijn beheersmaatregelen en implementatierichtlijnen verplicht? Beheersmaatregelen zijn verplicht, tenzij aangetoond kan worden (leg negatief uit) dat ze niet van toepassing zijn. Implementatierichtlijnen zijn niet verplicht, maar omdat ze als best practice zijn vastgesteld moet bij het afwijken ervan aangetoond worden (leg positief uit) dat een andere implementatie tot het voldoen aan de beheersmaatregel leidt.
Hierbij zijn de volgende kanttekeningen te maken:
- Om te voldoen aan een beheersmaatregel zal op basis van de implementatierichtlijnen in- of externe controle moeten worden uitgeoefend. Indien van de best practice wordt afgeweken zal eerst (bij voorkeur in een operationeel beleidsdocument) gemotiveerd moeten worden en vastgelegd hoe de beheersmaatregel anders wordt geïmplementeerd om in- of externe controle mogelijk te maken.
- Als bij de gezamenlijke evaluatie van het normenkader door allen die het moeten toepassen, blijkt dat velen tot een andere implementatie komen, zal de best practice moeten worden aangepast.

### B.2.3. Dreigingsprofiel

Het algemene dreigingsprofiel voor het basis beveiligingsniveau is vastgesteld op de volgende bedreigers:

Bedreigers

- de onbetrouwbare of wraakzuchtige medewerker;
- de verontruste burger;
- de actiegroep;
- de crimineel opportunist;
- de contractor;
- de georganiseerde internet crimineel (*cybercrime*).

Hierbij zijn de volgende bedreigingen aan de orde:

Bedreigingen

- publiek benaderbare sociale netwerken;
- verhoor (fysiek geweld tegen personen);
- hacking (op afstand);
- malware met en zonder remote control;
- crypto kraken;
- draadloze netwerken (interceptie/actief benaderen);
- beproeving van fysieke, technische en elektronische weerstand.

Naast de bovenstaande specifieke bedreigingen gaat het basisniveau ook uit van een set algemene dreigingen waarvan de hoofdgroepen zijn:
- opzettelijk of onopzettelijk menselijk handelen;
- onbeïnvloedbare externe factoren;
- technisch falen.

Uitgesloten zijn de volgende bedreigers:
- terreurgroep;
- inlichtingendienst;
- georganiseerde criminaliteit behoudens *cybercrime*.

## B.3. Views

### B.3.1. Betekenis van views

Door de modulaire opbouw van het normenkader, kunnen de normen niet één op één aan organisatiedelen worden toegewezen als verantwoordelijkheid om na te leven, zoals in voorgaande versies van beveiligingshandboeken gebruikelijk was. Het betekent tevens dat de samenhang tussen de modules niet op voorhand duidelijk is of ondubbelzinnig uit de structuur zelf is af te leiden. Om effectief gebruik te maken van het normenkader, en voor het verkrijgen van inzicht in de samenhang, werken we met views op de inhoud.

De volgende views staan in dit hoofdstuk uitgewerkt:
- View naar verantwoordelijkheid voor naleving:
  - per dienstonderdeel;
  - per manager in zijn personeelsverantwoordelijkheid;
  - per manager in zijn bedrijfsvoeringsverantwoordelijkheid.
- View naar onderwerp:
  - logische toegangsbeveiliging;
  - bedrijfscontinuïteit;
  - aspect ten behoeve van beheer en evaluatie in het clusteroverleg.

De uitgebreide views worden weergegeven als matrices.

### B.3.2. Verantwoordelijkheidsverdeling in een organisatie

| Verantwoordelijkheidsgebieden HBB onderdelen | Concern | Informatie-beheer | Algemene bedrijfsvoering | Applicatie-ontwikkeling | Exploitatie IT | Huisvesting |
|---|---|---|---|---|---|---|
| 1 Strategisch bev.beleid & -org. | X | | | | | |
| 1.3 Betrokk. mgmt. bij beveiliging | | | X | | | |
| 2 Tactisch uitv.beleid beveiliging | X | | | | | |
| 3.2 Sturing FO en implementatie | | Processen | | | TIS | |
| 3.3 Fasering ontwerp en onderh. | | Processen | | Applicaties | TIS | |
| 3.4 Kwaliteitsbeheer | | Processen | | Applicaties | TIS | |
| 3.5 Centraal uitv. informatiebeheer | | X | | | | |
| 3.6 Openbaar beschikbare info | | X | | | | |
| 3.7 Beheersing externe diensten | | X | | | | |
| 4 Functioneel productbeheer | Arbeids-ovk. | Proc.geg. & infouitw.-ovk, toegang derden-ovk. | Huisv.-ovk, IT-diensten, keten-ovk, inhuur-ovk. | Applicatie-ontwerp en/of bouw-ovk. | TIS, IT-diensten, IT-voorz. | Geb. & inst, algemene dienst-ovk. |
| 5.2 Procesinrichting | | | X | | | |
| 5.3 Aansturen operationele IT | | | X | | | |
| 5.4 Verwerken geg. obv. vraagtalen | | X | X | | | |
| 5.5 Rapporteren over het proces | | | X | | | |
| 5.6 Beheersen en evalueren proces | | | X | | | |
| 6 Personeelsbeheer | | | X | | | |
| 7 Leveranciersbeheer | | | Huisvesting, IT-diensten, inhuur derden | Applicatie-ontwerp en/of bouw | IT-diensten, IT-voorz. | Algemene diensten |
| 8 Afnemersbeheer | | | Ketendiensten aan derden | | IT-diensten | Huisvest. diensten |
| 9.2 Tactisch beveiligingsbeheer | | | X | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 9.3 Centraal beheer elektr. ident. | | | | | X*) | |
| 9.4 Verstrekken auth.middelen | | | X | | | |
| 9.5 Aanvragen autorisaties | | | X | | | |
| 9.6 Beheren groeperen autorisat. | | | X | | | |
| 9.7 Beheren dec. aut. gebruikers | | | X | | | |
| 9.8 Controle van systeemgebruik | | | X*) | | X | |
| 9.9 Technisch beveiligingsbeheer | | | | | X | |
| 9.10 Fysiek sleutelbeheer | | | X | | | |
| 10 Loketfunctie | | X | | | X**) | X |
| 11 Leveren applicaties | | | | X | | |
| 12.2 t/m 12.7 Leveren beh. & expl. IT | | | | | X | |
| 12.8 Release & deployment mgmt. | | | | X | X | |
| 12.9 t/m 12.12 Lev. beh. & expl. IT | | | | | X | |
| 13 Leveren huisvesting | | | | | | X |
| 14.2 Overeenkomsten info-uitwiss. | | X | | | | |
| 14.3 Overeenk. toegang derden | | X | | | | |
| 14.4 Overeenk. inhuur derden | | | X | | | |
| 14.5 Ovk. appl.ontwerp en/of bouw | | | | X | | |
| 14.6 Overeenk. dienstverl. alg. | | | Keten-ovk. | | IT-diensten | X |
| 14.7 Ovk. techn.beh. & expl. IT | | | | | X | |
| 14.8 Overeenk. aanschaf IT-voorz. | | | | | X | |
| 15.1 Bev.paragraaf procesontwerp | | X | | | | |
| 15.2 Impl.plan processen en applic. | | X | | | | |
| 15.3 Bev.par. fasedoc. TIS | | | | | X | |
| 16.1 t/m 16.2 IT-voorzieningen | | | | | X | |
| 16.3 Geprogrammeerde controles | | X | | | | |
| 16.4 t/m 16.10 IT-voorzieningen | | | | | X | |
| 17. Gebouwen en installaties | | | | | | X |
| 18. Computerruimten | | | | | X | |

*) Belegd bij B/CA

**) Autorisatieaanvragen t.a.v. gebruikers-id's en centrale systemen bij B/CA

### B.3.3. Manager in zijn verantwoordelijkheid voor personeel

De manager is verantwoordelijk voor het handhaven van de personele beveiliging met eventuele ondersteuning door Personeelszaken.
De volgende onderdelen van de normen behoren tot deze verantwoordelijkheid:
- 6 Personeelsbeheer, excl. 6.3.1, 6.4.2 tot en met 4 en 6.9;
- 9.4 Verstrekken authenticatiemiddelen;
- 9.5 Aanvragen autorisaties.

### B.3.4. Manager in zijn algemene verantwoordelijkheid voor bedrijfsvoering

De manager is verantwoordelijk voor het doen uitvoeren van activiteiten in processen op basis van de vastgelegde inrichting ervan. Daarbij is sprake van algemene beveiligingsaspecten in processen en specifieke, die beide onderscheidelijk in het normenkader zijn te vinden. De verantwoordelijkheid voor de naleving van de algemene beveiligingsaspecten die voor iedere manager gelden, is te vinden in het volgende onderdeel van de normen:
- 5 Algemeen procesbeheer, excl. 5.6 Aansturen operationele IT.

### B.3.5. Verdeling beveiligingsonderwerpen naar de aspecten

| HBB onderdelen | TBO | IB | PV&I | BCM | FB |
|---|---|---|---|---|---|
| 1 Strategisch beveiligingsbeleid & beveiligingsorganisatie | X | | | | |
| 2.2 t/m 2.4 Tactisch beleid beveiliging | | X | | | |
| 2.5 Toegangsbeleid | | X | | | X |
| 2.6 t/m 2.11 Tactisch beleid beveiliging | | X | | | |
| 2.12 t/m 2.17 Tactisch beleid beveiliging | | | X | | |
| 2.18 Beleid voor bedrijfscontinuïteit | | | | X | |
| 3 Informatiebeheer | | X | | | |
| 4 Functioneel productbeheer | | X | | | |
| 5 Algemeen procesbeheer | | X | | | |
| 6 Personeelsbeheer | | | X | | |
| 7 Leveranciersbeheer | | X | | | |
| 8 Afnemersbeheer | | X | | | |
| 9.2.1 t/m 9.2.2 Tactisch beveiligingsbeheer | | X | | | |
| 9.2.3 Plannen bedrijfscontinuïteit | | | | X | |
| 9.2.4 t/m 9.2.5 Tactisch beveiligingsbeheer | | X | | | |
| 9.2.6 Testen, bewustwording, evaluatie & onderhoud | | | | X | |
| 9.2.7 t/m 9.9.4 Tactisch beveiligingsbeheer | | X | | | |
| 9.10 Fysiek sleutelbeheer | | | | | X |
| 10 Loketfunctie | | X | | | |
| 11 Leveren applicaties | | X | | | |
| 12 Leveren beheer & exploitatie IT | | X | | | |
| 13 Leveren huisvesting | | | | | X |
| 14 Diverse overeenkomsten | | X | | | |
| 15 Fasedocumenten ontwerp / invoering IT | | X | | | |
| 16 IT-voorzieningen | | X | | | |
| 17 Gebouwen en installaties | | | | | X |
| 18 Computerruimten | | X | | | (X) |

TBO = Tactisch beveiligingsoverleg
IB = Informatiebeveiliging
PV&I = Personele veiligheid en integriteit
BCM = Business continuity management, bedrijfscontinuïteitsbeheer
FB = Fysieke beveiliging

### B.3.6. View voor functiescheiding

| HBB onderdelen |
|---|
| 2.3 Beleid voor functiescheiding |
| 9.9.2.6 Sleutelbeheer |
| 12.2.1, 2, 3, 4 Technisch beheer en exploitatie |
| 13.2 Huisvesting |
| 16.3.1 Functie- en processcheidingen in IT-voorzieningen |
| 16.3.7.1 Aparte applicatietaken |

### B.3.7. Views voor logische toegangsbeveiliging en bedrijfscontinuïteit

| HBB onderdelen | LTB | BCM |
|---|---|---|
| 2.18 Beleid voor bedrijfscontinuïteit | | X |
| 2.5 Toegangsbeleid | X | |
| 4.4.3 Evaluatie leveranciers | | X |
| 5.2.2 Procesinrichting - onverenigbaarheid | X | |
| 5.2.3 Procesinrichting - conflicterende functies | X | |
| 5.2.12 Procesinrichting - doorbreken functiescheidingen | X | |
| 5.2.13 Procesinrichting - noodregelingen | X | |
| 5.4.1 Vraagtalen | X | |
| 6.6.1 Kritische functies | | X |
| 6.7.3 Intrekken toegangsrechten | X | |
| 9.1.3 Plannen bedrijfscontinuïteit | | X |
| 9.1.6 Testen, bewustwording, eval. en onderhoud plannen bedrijfscontinuïteit | | X |
| 9.3 Centraal beheer elektronische identiteiten | X | |
| 9.4 Verstrekken authenticatiemiddelen | X | |
| 9.5 Aanvragen autorisaties | X | |
| 9.6 Groeperingbeheer autorisaties | X | |
| 9.7 Beheren decentrale autorisaties gebruikers | X | |
| 9.8 Controle van systeemgebruik 1, a - c | deels | |
| 10 Loketfunctie | X | |
| 12.2.1.4 Toegang tot gebruikersfuncties | X | |
| 12.12.5 Maken backups | | X |
| 13.10 Beschikbaarheid huisvesting | | X |
| 14.3 Overeenkomsten toegang derden, punten 3, 4, 6, 12, en 17 | X | |
| 14.7 Overeenkomsten technisch beheer en exploitatie IT, punt 4 | | X |
| 15.1 Beveiligingsparagraaf procesontwerp, punt 6 | | X |
| 15.3 Fasedocumenten technische infrastructuur, punt 6.b en c, 7 | X | |
| 16.2 Continuïteitsvoorzieningen | | X |
| 16.3.1 Functie- en processcheidingen | X | |
| 16.7 Identificatie, authenticatie en autorisatie | X | |

## B.4. Organisatie van beveiliging

### B.4.1. Sturing van beveiliging

De sturing van beveiliging benaderen we vanuit verschillende gezichtspunten.

Maatregelsturing

- **Sturing op de maatregelen**: deze verloopt langs de primaire verantwoordelijkheidsverdeling van de Belastingdienst. Beveiliging is een integraal onderdeel van de bedrijfsvoering en alle soorten maatregelen, die een organisatie treft om haar doelen te bereiken. Beveiliging is maar één van de vele aspecten waarop in samenhang moet worden gestuurd.

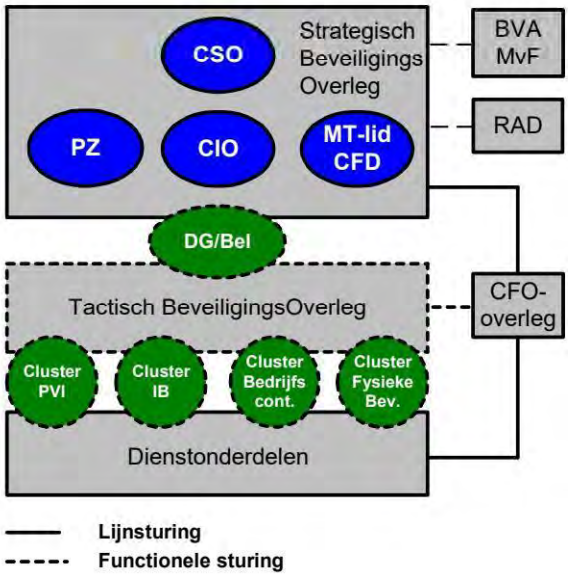
Aspectsturing

- **Lijnsturing op het aspect**: deze verloopt langs de lijn van de CFO's. Hierbij gaat het om de managementverantwoordelijkheid voor het aspect beveiliging met een accent op naleving van beveiligingskaders en samenhang van de maatregelen binnen het competentiegebied.

Functionele sturing

- **Functionele sturing**: deze verloopt van de strategisch beveiligingsadviseur tot de beveiligingsmedewerker en staat ten dienst zowel aan de lijnsturing op het aspect als de sturing op maatregelen.

Onderstaand schema brengt dit in beeld.




**Figuur 1: Sturing beveiliging bij de Belastingdienst**

### B.4.2. Tactisch Beveiligingsoverleg (TBO)

Doel TBO

Het TBO is een adviesorgaan voor het Strategisch Beveiligingsoverleg, het SBO. Het is beleidsvoorbereidend en evaluerend en kent een lijnsturing. Het geeft gevraagd en ongevraagd advies aan het SBO, de CSO of de CFO van een dienstonderdeel. Het TBO dient voor de afstemming tussen het strategisch niveau en de dienstonderdelen.

Deelnemers TBO

De deelnemers zijn vertegenwoordigers van alle dienstonderdelen.

- Voorzitter: DGBel/Cluster Bedrijf
- Secretaris: DGBel/Cluster IV-beleid

Inhoud overleg:
- Besluitvorming over onderhoud HBB;
- Evaluatie geaggregeerde en geanonimiseerde dienstonderdeelrapportages inzake beveiliging;
- Evaluatie uitkomsten beveiligingsaudits;
- Voorbespreking stukken voor CFO-overleg;
- Evaluatie jaarlijkse risicoanalyses per dienstonderdeel;
- Voorstellen beveiligingsaudits.

Frequentie overleg

Het TBO komt drie keer per jaar (aansluitend aan de rapportages) bijeen of vaker naar aanleiding van bijvoorbeeld thema's of actuele beleidsonderwerpen.

### B.4.3. Aspectclusters

Doel aspectclusters

Voor de verschillende beleidsgebieden van beveiliging zijn clusters geformeerd, waarin beveiligingsadviseurs en beveiligingsmedewerkers van dienstonderdelen de onderwerpen van bespreking in het TBO voorbereiden. Zij zijn de uitvoeringsorganen van het TBO.

Deelnemers

De deelnemers zijn vertegenwoordigers van alle dienstonderdelen.

Taken clusters
- Uitwerken voorstellen tot onderhoud HBB;
- Adviseren TBO over planning en uitvoering ICP's beveiliging.

De verdeling van onderwerpen, die in de aspectclusters beheerd worden, staat in het hoofdstuk Views (B.3) van dit deel.

### B.4.4. Escalatie

Het escaleren van incidenten, niet-opgeloste bevindingen of niet-nageleefde adviezen gebeurt volgens de hiërarchische en/of functionele lijnen dan wel via de overlegorganen zoals aangegeven. Escalatie wordt ook vermeld in de rapportage.

### B.4.5. Rollen en functies

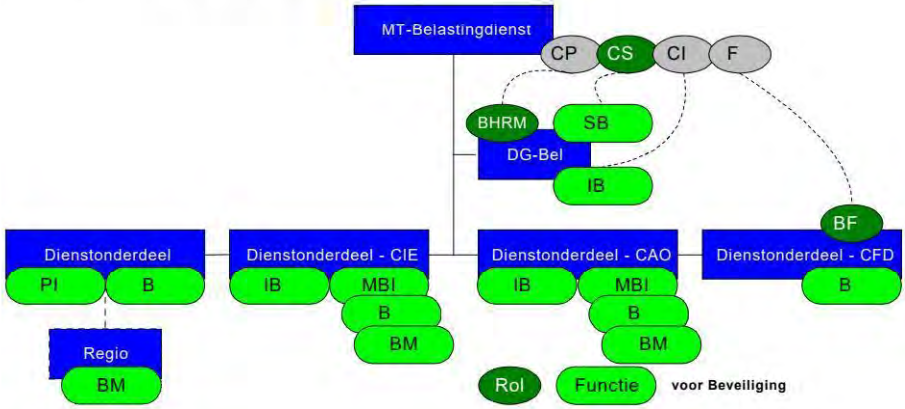
Rol of functie

In de functies van beveiliging kan onderscheid worden gemaakt naar beveiligingsrollen en -functies. Met beveiligings*rol* bedoelen we het uitvoeren van een deeltaak op het gebied van beveiliging, naast de primaire hoofdtaken van een functie. De leden van het SBO bijvoorbeeld vervullen alleen beveiligingsrollen, namelijk de beleidstaken op het gebied van beveiliging, naast hun andere beleidstaken.
Bij de beveiligings*functies* gaan we alleen uit van de adviserende functies en niet op de uitvoerende beveiligingsfuncties die met een grote verscheidenheid overal in de organisatie van de Belastingdienst voorkomen. Denk hierbij aan: portiers- en bewakingsfuncties, security administrators, firewallbeheerders, IT-security ontwerpers etc.

We onderscheiden de volgende rollen en functies voor beveiliging.

| Afk. | Rol | Afk. | Functie |
|---|---|---|---|
| CSO | Chief Security Officer | SBA | Strategisch beveiligingsadviseur |
| BHRM | Beleidsmedewerker HRM voor personele beveiliging en integriteit | IBA | Informatiebeveiligingsarchitect |
| BFB | Beleidsmedewerker fysieke beveiliging | PIB | Procesarchitect informatiebeveiliging |
| | | BA | Beveiligingsadviseur |
| | | MBI | Manager beveiliging ICT |
| | | BM | Beveiligingsmedewerker |

Deze kunnen op de organisatie van de Belastingdienst worden geprojecteerd. Zie hiertoe de figuur hieronder.




**Figuur 2: Beveiligingsrollen en -functies in de Belastingdienst**

Ter toelichting op de figuur het volgende.
- De CPO, CIO het gedelegeerd MT-lid voor de Facilitaire Dienst zijn geen beveiligingsrollen. De CSO wel, omdat de primaire functie CFO is.
- In de figuur is met een stippellijn aangegeven welke beleidsmedewerkers ondersteunend zijn aan de leden van het SBO.
- Van de beveiligingsfunctie is alleen de organieke plaats aangegeven, niet het aantal formatieplaatsen.
- Niet elk dienstonderdeel zal aparte beveiligingsmedewerkers willen positioneren bij de regio's of suborganisatiedelen.

### B.4.6. Beveiligingsrollen

In deze paragraaf staan de beelden van de beveiligingsrollen nader uitgewerkt.

#### B.4.6.1. Chief Security Officer (CSO)

Deze rol omvat de volgende taken:
- Opdrachtgever strategisch beveiligingsadviseurs;
- Vormt zich een visie op de betekenis van beveiliging voor de hele organisatie;
- Stelt doelen en beleid ter uitvoering vast;
- Draagt ervoor zorg dat er voldoende middelen voor uitvoering van het beleid aanwezig zijn;

- Draagt doelen en beleid uit in de hele organisatie;
- Draagt ertoe bij dat auditbevindingen en incidenten van ernstige aard worden opgelost.

#### B.4.6.2. Beleidsmedewerker voor een deelgebied van beveiliging

Deze rol omvat de volgende taken:
- Vormt zich een visie op de betekenis van het beleidsgebied binnen de hele organisatie;
- Draagt zorg voor het actueel houden van het tactisch beveiligingsbeleid voor het beleidsgebied;
- Bevordert dat er op strategisch niveau voldoende randvoorwaarden zijn voor het treffen van de beveiligingsmaatregelen op het beleidsgebied;
- Draagt doelen en beleid op het beleidsgebied uit in de hele organisatie;
- Draagt ertoe bij dat auditbevindingen en incidenten van ernstige aard binnen het beleidsgebied worden opgelost.

### B.4.7. Beveiligingsfuncties

Functieweging

In deze paragraaf zijn de beelden van de beveiligingsfuncties nader uitgewerkt. Bij waardering van de beveiligingsfuncties wordt gebruik gemaakt van de vigerende methode van functiewaardering.

#### B.4.7.1. Strategisch beveiligingsadviseur

Doel van de functie

Het ontwikkelen van strategie en beleid gericht op beveiliging. Bevorderen en coördineren van de ontwikkeling van uitvoeringsrichtlijnen en toezien op de realisatie van het beleid.

Functiecontext

Functioneert als zelfstandig opererend intern beleidsadviseur, ressorterend onder het lid van het MT Belastingdienst dat verantwoordelijk is voor beveiliging. Geeft functioneel leiding aan beveiligingsmedewerkers in de gehele organisatie door het geven van richtlijnen en sturing op interne rapportages over de uitvoering van het beveiligingsbeleid en het naleven van uitvoeringsrichtlijnen.

Resultaatgebieden

**Leidinggeven**
- Geeft functioneel leiding aan beveiligingsmedewerkers in de gehele organisatie;
- Treedt op als projectleider of opdrachtgever voor organisatiebrede projecten op het gebied van beveiliging;
- Organiseert en faciliteert overleg voor sturing en coördinatie op het gebied van beveiliging.

**Plan: Beveiligingseisen**
- Vormt zich een visie op de betekenis van beveiliging voor de gehele organisatie door voortdurende beeldvorming over risico's en oplossingsrichtingen voor maatregelen passend bij het organisatiebeleid;
- Stelt doelen voor beveiliging voor;
- Ontwikkelt een strategie om die doelen te bereiken;
- Ontwikkelt beleid ter uitvoering van de strategie en stelt het centraal beleids- en jaarplan samen mede op basis van de deelplannen beveiliging.

**Do: Treffen maatregelen**
- Bevordert het ontwikkelen van uitvoeringsrichtlijnen en geeft hieraan richting;
- Initieert voorlichtings- en IB-bewustzijnsprogramma's en geeft hieraan richting;
- Initieert en faciliteert risicoanalyses op niveau van de hele organisatie;
- Toetst uitvoeringsrichtlijnen aan het beleid en adviseert zonodig over verbetering;
- Bereidt organisatiebrede beslissingen op het gebied van beveiliging voor;
- Adviseert de leiding van de organisatie, dienstonderdelen en de IV-organisatie bij beleid(sbeslissingen) met consequenties voor beveiliging.

**Check: Evaluatie en controle**
- Beoordeelt rapportages van dienstonderdelen over de naleving van uitvoeringsrichtlijnen;
- Beoordeelt rapportages van in- en externe auditinstanties op relevantie voor beveiliging;
- Geeft opdrachten tot het verrichten van interne onderzoeken en audits;
- Houdt een centrale registratie bij van beveiligingsincidenten en de afhandeling en evalueert de incidenten;
- Beoordeelt ontwikkelingen in de maatschappij, de overheid en het vakgebied.

**Act: Aanpassen**
- Stelt IB-visie, -strategie en -beleid bij en bevordert aanpassing van uitvoeringsrichtlijnen op basis van evaluaties.

**Contacten**
- Intern: CSO, leiding dienstonderdelen, BVA van het ministerie, andere beveiligingsfunctionarissen;
- Extern: auditors, andere overheidsbeveiligingsfunctionarissen en beroepsgenoten.

Kennisgebieden
- IV en beveiliging (breed);
- Organisatie van informatievoorziening;
- Business processen (breed).

### B.4.7.2. Beveiligingsadviseur

Doel van de functie

Het ontwikkelen van beleid gericht op het naleven van kaders voor beveiliging, ondersteunen van de CFO van het dienstonderdeel hierbij en toezien op de realisatie van het beleid.

Resultaatgebieden

**Plan: Beveiligingseisen**
- Stelt jaarlijks het beveiligingsplan voor het dienstonderdeel op;
- Draagt bij aan beleidsplannen voor beveiliging vanuit het perspectief van het dienstonderdeel.

**Do: Treffen maatregelen**
- Adviseert over uitvoeringsrichtlijnen op het gebied van beveiliging, zowel centraal voor de Belastingdienst als bij het dienstonderdeel;
- Draagt uitvoeringsrichtlijnen op het gebied van beveiliging actief uit in de organisatie;
- Initieert voorlichtings- en bewustzijnsprogramma's en geeft hieraan richting;
- Voert risicoanalyses uit binnen zijn competentiegebied;

- Adviseert over het treffen van beveiligingsmaatregelen en bij besluitvorming binnen het dienstonderdeel met gevolgen voor beveiliging.

**Check: Evaluatie en controle**
- Beoordeelt interne rapportages op beveiligingsaspecten;
- Stelt periodiek verantwoordingsrapportage op over beveiliging;
- Beoordeelt rapportages van in- en externe controle en auditinstanties;
- Adviseert de CFO inzake het verrichten van interne onderzoeken en audits;
- Zorgt voor centrale melding van beveiligingsincidenten en beoordeelt afhandeling.

**Act: Aanpassen**
- Stelt het jaarplan beveiliging bij en adviezen over uitvoeringsrichtlijnen op basis van zijn evaluaties.

**Contacten**
- Intern: management dienstonderdeel op alle niveaus en andere beveiligingsfuncties;
- Extern: auditors en beroepsgenoten.

Kennisgebieden
- Beveiliging;
- Belastingdienst processen;
- Interne regelgeving.

Doel van de functie

### B.4.7.3. Beveiligingsmedewerker (BM)

Het ondersteunen en toezien op de realisatie van beleid gericht op het naleven van Belastingdienstkaders voor beveiliging en het management van het dienstonderdeel hierbij ondersteunen.

Resultaatgebieden

**Plan: Beveiligingseisen**
- Draagt bij aan de beleidsplannen voor beveiliging van het dienstonderdeel.

**Do: Treffen maatregelen**
- Adviseert over uitvoeringsrichtlijnen op het gebied van beveiliging bij het dienstonderdeel en de regio;
- Draagt uitvoeringsrichtlijnen op het gebied van beveiliging actief uit in de organisatie;
- Draagt bij aan risicoanalyses binnen zijn competentiegebied;
- Adviseert over het treffen van beveiligingsmaatregelen en bij besluitvorming binnen het dienstonderdeel met gevolgen voor beveiliging.

**Check: Evaluatie en controle**
- Beoordeelt interne rapportages op beveiligingsaspecten;
- Stelt periodieke verantwoordingsrapportage op over beveiliging;
- Beoordeelt rapportages van interne controle.

**Act: Aanpassen**
- Stelt adviezen over uitvoeringsrichtlijnen bij op basis van zijn evaluaties.

**Contacten**
- Intern: management regionaal dienstonderdeel op alle niveaus en andere beveiligingsfuncties;
- Extern: auditors en beroepsgenoten.

Kennisgebieden
- Beveiliging;
- Belastingdienst processen;
- Interne regelgeving.

### B.4.7.4. Procesarchitect Informatiebeveiliging

Doel van de functie

Het ontwikkelen en actueel houden van een visie op de deelarchitectuur voor het aspect informatiebeveiliging in de bedrijfs- of procesarchitectuur als concretisering van een deel van het strategisch beveiligingsbeleid en de positionering van generieke beveiligingsfunctionaliteiten daarbinnen.

Functiecontext

Procesarchitect met als specialisatie beveiliging. Vertaalt beleidskaders voor beveiliging naar bedrijfs- of procesarchitectuur en vervult daarbij zowel een architecten- als adviseursrol. Treedt met name op als procesarchitect voor generieke beveiligingsfunctionaliteiten, bijvoorbeeld op het gebied van logische toegangsbeveiliging, encryptie, logging en auditing. Ziet toe op naleving van architectuurprincipes voor beveiliging. Houdt voortdurend zicht op marktontwikkelingen op het gebied van beveiligingsproducten.

Resultaatgebieden

**Plan: Beveiligingseisen**
- Vormt zich een visie op de betekenis van beveiliging in het kader van de bedrijfs- of procesarchitectuur en houdt daarbij rekening met de organisatiestrategie voor beveiliging;
- Draagt bij aan de strategie van de organisatie voor beveiliging vanuit het perspectief van procesontwikkeling;
- Draagt bij aan de beleidsvorming en jaarplannen ter uitvoering van deze strategie binnen zijn competentiegebied.

**Do: Treffen maatregelen**
- Ontwerpt zelfstandig deelarchitectuur van de bedrijfs- of procesarchitectuur voor het domein van beveiliging of draagt bij aan het expliciet maken van het aspect beveiliging als integraal onderdeel van deze architectuur;
- Voert risicoanalyses uit binnen zijn competentiegebied;
- Toetst procesontwerpen aan architectuuruitgangspunten voor beveiliging en adviseert zonodig over verbetering van die ontwerpen;
- Toetst ontwerpen voor generieke beveiligingsfunctionaliteiten aan architectuuruitgangspunten voor beveiliging en adviseert zonodig over verbetering van die ontwerpen.

**Check: Evaluatie en controle**
- Beoordeelt procesmatige ontwikkelingen in de bedrijfsvoering met mogelijke gevolgen voor IB-aspecten;
- Beoordeelt IT-audit rapportages, rapportages over beveiligingsincidenten en gebruikersevaluaties van generieke beveiligingsfunctionaliteiten.

**Act: Aanpassen**

- Draagt zorg voor het bijstellen van het aspect beveiliging in de bedrijfs- of procesarchitectuur of implementaties daarvan op basis van zijn evaluaties.

**Contacten**
- Intern: bedrijfs/procesarchitecten, procesontwerpers, informatiemanagers, projectleiders voor procesmatige vernieuwingen, andere beveiligingsfuncties;
- Extern: IT-auditors en beroepsgenoten.

Kennisgebieden
- IV en beveiliging;
- Organisatie van informatievoorziening;
- Architectuurprincipes;
- Belastingdienstprocessen (breed en diep).

Doel van de functie

### B.4.7.5. Beveiligingsmanager ICT

Het ontwikkelen van beleid gericht op informatiebeveiliging binnen de ICT-aanbodorganisatie, ondersteunen van het management, zorgdragen voor de ontwikkeling van uitvoeringsrichtlijnen en toezien op de realisatie van het beleid.

Functiecontext

Functioneert namens het management van ICT-aanbod als zelfstandig en breed opererend adviseur en toezichthouder op het gebied van beveiliging. Geeft functioneel leiding aan beveiligingsfunctionarissen in de ICT-organisatie door het geven van richtlijnen en sturing op interne rapportages over de uitvoering van het beveiligingsbeleid en het naleven van uitvoeringsrichtlijnen. Overwint weerstand om het beleid en richtlijnen te laten naleven, die vaak als belemmerend worden ervaren in de uitvoering van het werk.

Resultaatgebieden

**Plan: Beveiligingseisen**
- Stelt jaarlijks het informatiebeveiligingsplan voor de ICT-aanbodorganisatie op;
- Draagt bij aan de centrale strategie en -beleidsplannen voor beveiliging vanuit het perspectief van de ICT-aanbodorganisatie.

**Leidinggeven**
- Geeft eventueel functioneel of direct leiding aan andere beveiligingsfuncties binnen de ICT-aanbodorganisatie;
- Organiseert en faciliteert overleg om maatregelen en evaluaties binnen de ICT-aanbodorganisatie op het gebied van beveiliging op elkaar af te stemmen.

**Do: Treffen maatregelen**
- Adviseert over uitvoeringsrichtlijnen op het gebied van beveiliging, zowel centraal voor de Belastingdienst als bij de ICT-aanbodorganisatie;
- Initieert voorlichtings- en IB-bewustzijnsprogramma's en geeft hieraan richting;
- Voert risicoanalyses uit binnen zijn competentiegebied en op centraal niveau als vertegenwoordiger van de ICT-aanbodorganisatie;
- Adviseert over het treffen van beveiligingsmaatregelen en bij besluitvorming binnen de ICT-aanbodorganisatie met gevolgen voor beveiliging;
- Ziet toe op navolging adviezen/controlebevindingen bij certificerings-processen.

**Check: Evaluatie en controle**
- Beoordeelt afdelings- en procesrapportages binnen de ICT-aanbodorganisatie;
- Beoordeelt rapportages van in- en externe controle en auditinstanties;
- Geeft opdrachten tot het verrichten van interne onderzoeken en audits;
- Beoordeelt of participeert in de afhandeling van beveiligingsincidenten;

**Act: Aanpassen**
- Stelt het beveiligingsjaarplan en adviezen over beveiligingsuitvoeringsrichtlijnen bij op basis van zijn evaluaties.

**Contacten**
- Intern: management dienstonderdeel op alle niveaus en andere beveiligingsfuncties;
- Extern: auditors, branche- en beroepsgenoten.

Kennisgebieden
- ICT en informatiebeveiliging;
- Organisatie van informatievoorziening;
- ITIL.

### B.4.7.6. Informatiebeveiligingsarchitect

Doel van de functie

Het ontwikkelen en actueel houden van het aspect beveiliging binnen de IV-architectuur dat zowel gericht is op het voldoen aan het beveiligingsbeleid en -voorschriften als op de generieke beveiligingsfunctionaliteiten binnen de technische infrastructuur. Daarbij hoort het toepasbaar maken van deze architectuur op hoofdlijnen (systeemschets) van het ontwerp en het onderhoud van de generieke beveiligingsfunctionaliteiten.

Functiecontext

IV-architect met als specialisatie beveiliging in relatie tot IV. Vertaalt beleidskaders voor beveiliging naar IV-architecturen en vervult daarbij zowel een architect- als adviseursrol. Treedt met name op als IV-architect voor generieke beveiligingsfunctionaliteiten, bijvoorbeeld op het gebied van logische toegangsbeveiliging, encryptie, logging- en auditing.
Ziet toe op naleving van architectuurprincipes voor beveiliging. Houdt voortdurend zicht op marktontwikkelingen op het gebied van beveiligingsproducten.

Resultaatgebieden

**Plan: Beveiligingseisen**
- Vormt zich een visie op de betekenis van beveiliging voor IV vanuit de centrale strategie door voortdurende beeldvorming over risico's en oplossingsrichtingen voor maatregelen passend bij het centrale beleid;
- Draagt bij aan de centrale strategie voor IV in relatie tot beveiliging;
- Draagt bij aan de beleidsvorming en jaarplannen ter uitvoering van deze strategie binnen zijn competentiegebied.

**Do: Treffen maatregelen**
- Ontwerpt zelfstandig deelarchitectuur van het IV-complex voor het domein beveiliging of draagt bij aan het expliciet maken van het aspect beveiliging als integraal onderdeel van de IV-architecturen;
- Treedt op als IV-architect voor generieke beveiligingsfunctionaliteiten;
- Toetst IV-ontwerpen aan architectuuruitgangspunten voor beveiliging en adviseert zonodig over verbetering van die ontwerpen.

**Check: Evaluatie en controle**

- Beoordeelt ontwikkelingen in de markt t.a.v. nieuwe informatiebeveiligingsrisico's en generieke oplossingen van leveranciers;
- Beoordeelt interne ontwikkelingen binnen de IV met mogelijke gevolgen voor IB-aspecten in de IV;
- Beoordeelt IT-audit rapportages, rapportages over beveiligingsincidenten en gebruikersevaluaties van generieke beveiligingsfunctionaliteiten.

**Act: Aanpassen**
- Draagt zorg voor het bijstellen van het aspect beveiliging in IV-architecturen op basis van zijn evaluaties.

**Contacten**
- Intern: IV-architecten, IV-ontwerpers, projectleiders IV, andere beveiligingsfuncties;
- Extern: IT-auditors, IV-leveranciers en beroepsgenoten.

Kennisgebieden
- IV en beveiliging;
- Architectuurprincipes;
- Standaards inzake beveiliging.

## B.5. Structuur van de normen in Deel C

Voor het samenstellen van de normen zijn een aantal uitgangspunten gehanteerd, die afwijken van de eerder gehanteerde. Deze uitgangspunten zijn tevens leidend voor het onderhoud van de normen en kunnen worden gebruikt als toetsingskader voor acceptatie van wijzigingen.

### B.5.1. Ontwerpcriteria

*Eén kader voor de hele Belastingdienst*

Samenhang

Door alle beveiligingsnormen in één handboek op te nemen is de onderlinge consistentie en volledigheid beter te borgen en het *pas toe of leg uit* beginsel van de aan de overheid opgelegde standaarden beter te handhaven.

*Onafhankelijk van de organisatie*

Authentiek en uitwisselbaar

Indien beveiligingsnormen te zeer op de organisatie van de Belastingdienst en te zeer implementatieafhankelijk worden geformuleerd is niet meer duidelijk wat de oorspronkelijke uitgangspunten van de norm zijn. Er zal dan vaker onderhoud moeten worden gepleegd omdat organisaties steeds dynamischer worden. Bovendien kunnen de normen dan niet goed meer met derden worden afgestemd en kunnen ze niet meer dienen als eisen die aan uitbestedings- of ketenpartijen zijn te stellen.
De vraag is dan wel waarom er niet rechtstreeks gebruik kan worden gemaakt van de bestaande standaarden. Dat heeft te maken met het feit dat deze niet voldoen aan de hier geformuleerde uitgangspunten, waardoor de vertaalslag naar de praktijk erg omslachtig is, met andere woorden: de praktische toepasbaarheid is beperkt.

*Onderscheid tussen proces en product*

Het maken van onderscheid naar normen voor processen en normen voor de uitkomsten van processen - dat zijn producten - dient meerdere doelen. Het onderscheid is van belang bij het stellen van eisen aan projecten en derden, omdat het daarbij vaak alleen maar gaat om het opleveren van een product, bijvoorbeeld een IT-component of alleen het ontwerp ervan. Het zelfde geldt bij fysieke objecten, zoals een gebouw of computerruimte.
De kennis die nodig is om proces- of productnormen toe te passen bij advisering en controle is verschillend.

Processen

Bij processen zijn vaak dezelfde ordeningsprincipes van toepassing: de volgorde van gebeurtenissen of de PDCA-cyclus. Bij de aantoonbaarheid van processen kan altijd dezelfde formele benadering worden gevolgd. Kennis omtrent de inhoud van de processen is niet primair vereist.

Producten

Bij producten is dit anders. Dat vergt bijna altijd specialistische kennis en een specifieke benadering bij het kunnen aantonen van de kwaliteit.
Dit onderscheid spoort met het onderscheid tussen de procesgerichte en een gegevensgerichte auditbenadering.

*Onderscheid tussen klant en leverancier (ketenoriëntatie)*

Verantwoordelijkheid, wederzijds

Organisaties (en zeker overheidsorganisaties) opereren steeds meer in ketens waarbij ze sterk van elkaar afhankelijk zijn. Uitbesteding van facilitaire diensten, zoals IT, maar bijvoorbeeld ook huisvesting, is daarvan een prominent voorbeeld. Omdat verantwoordelijkheden niet kunnen worden uitbesteed, is het van belang zekerheid te krijgen over de juiste uitvoering van de uitbestede activiteiten. Hiervoor is het noodzakelijk de juiste eisen en normen aan de ander te kunnen stellen en hierop controle te kunnen laten uitoefenen. De huidige beveiligingsstandaards zijn hierop niet ingedeeld.

*Zo klein mogelijke verantwoordelijkheidsgebieden*

Duidelijk belegde verantwoordelijkheid

De indeling van de normen moet zodanig zijn dat naleving ondubbelzinnig is toe te wijzen binnen een organisatie. Het moet niet de expertise van de controleur zijn die uiteindelijk bepaalt bij welke afdeling of als welk onderdeel van een proces normen op naleving moeten worden gecontroleerd. Het onderscheid tussen beleid en uitvoering bijvoorbeeld is in grote organisaties vaak gescheiden en dat betekent dat een dergelijk onderscheid ook moet doorwerken in de formulering van normen.

*Geen dubbele teksten*

Consistentie

In het algemeen getuigt het meerdere malen voorkomen van dezelfde of overlappende teksten (normen) in één document van een slechte structuur, tenzij daarvoor bewust is gekozen, bijvoorbeeld bij een samenvatting. Dubbele of overlappende teksten zijn niet bevorderlijk voor het goede begrip van het document en vormen een risico op inconsistenties bij het onderhoud. In de Code voor Informatiebeveiliging bijvoorbeeld is dit regelmatig te zien.

*Controleerbaar met bewijsstukken*

Ondubbelzinnige normen

Indien naleving van een norm niet rechtstreeks kan worden aangetoond met bewijsstukken is de formulering van de norm niet concreet genoeg. Vaak neigt de omschrijving meer naar een doelstelling dan een norm. Een norm moet zo min mogelijk interpretatieverschillen toelaten.
Om die reden worden de normen ingedeeld naar beheersmaatregelen op een hoog abstractieniveau en verder ingevuld met zo concreet mogelijke implementatierichtlijnen. Het is echter vanwege de organisatie-onafhankelijkheid niet altijd mogelijk interpretatieverschillen geheel te voorkomen. In de Code voor Informatiebeveiliging roepen implementatierichtlijnen regelmatig een reeks of stelsel van maatregelen op teneinde daaraan te kunnen voldoen. In het HBB proberen we juist vage formuleringen te voorkomen.

### B.5.2. Toelichting op de hoofdstructuur van de normen

Modulair normenkader

Op basis van de ontwerpcriteria ontstaat een sterk modulair opgebouwd normenkader, waarvan onderdelen bij meerdere organisatiedelen in verschillende situaties toepasbaar zijn. Het voordeel van de procesoriëntatie is dat een zekere standaardisatie mogelijk wordt.
Gestandaardiseerde processen zijn onder meer:

- Afnemers en leveranciersbeheer: deze zijn afgeleid van de ITIL-processen bij technisch beheer en exploitatie IT, te weten Supply Management en Service Level Management IT;
- Functioneel bedrijfsmiddelenbeheer, dat voor alle soorten bedrijfsmiddelen kan gelden, zoals applicaties, IT-infrastructuur en gebouwen;
- Loketfunctie, gebaseerd op ITIL waarin (aan)vragen worden opgevangen en gevalideerd voor beheer en exploitatie van IT-voorzieningen, het leveren van huisvesting en voor informatiemanagement.

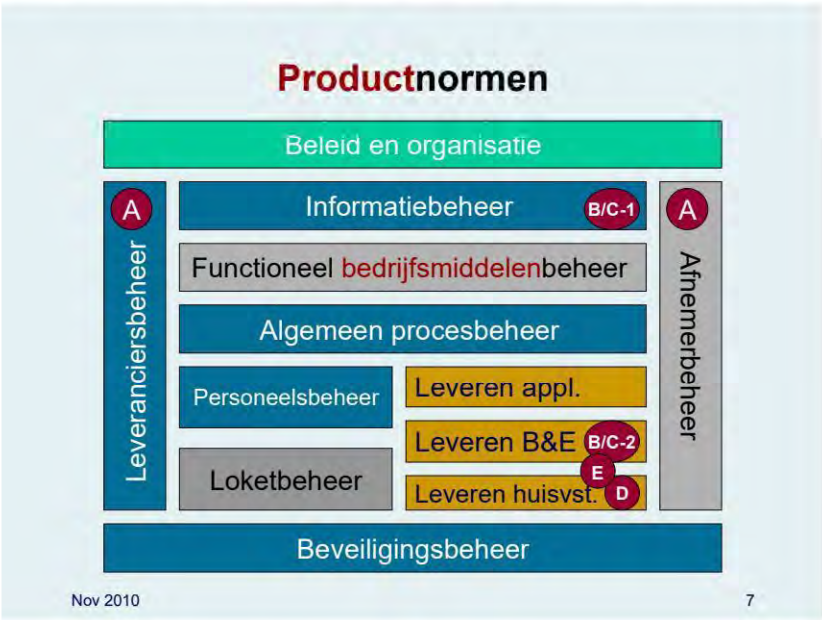
Processtructuur

De hoofdstructuur is weergegeven in de volgende figuur.


**Figuur 3: Hoofdstructuur normen basis beveiligingsniveau**

Deze hoofdstructuur heeft betrekking op de processen, met uitzondering van het overkoepelende gedeelte voor beleid en organisatie. De normen voor de bedrijfsmiddelen (producten) zijn aan deze processen gekoppeld:

Productstructuur




**Figuur 4: Productnormen basis beveiligingsniveau**

De letters in de figuur hebben de volgende betekenis:

A. Overeenkomsten
- Informatieuitwisseling derden;
- Verlenen externe toegang;
- Dienstverlening (DV) algemeen;

- Ontwerp en bouw applicaties;
- DV + beheer en exploitatie IT;
- DV + huisvesting;
- Aanschaf IT-voorzieningen.

B. Fasedocumenten ontwerp en realisatie
   1. Beveiligingsparagraaf: processen + technische infrastructuur;
   2. Implementatieplan.

C. IT-voorzieningen
   1. Geprogrammeerde controles;
   2. Generieke IB-functies.

D. Gebouwen en installaties

E. Computerruimten

### B.5.3. Betekenis en opbouw normen

Beheersmaatregelen en implementatierichtlijnen

De normen zijn onderverdeeld in twee hiërarchische niveaus, de beheersmaatregelen en daaronder de implementatierichtlijnen.
De beheersmaatregelen dienen voor oordeelsvorming en rapportage, de implementatierichtlijnen zijn best practices, die aan de maatregelen invulling geven. De interne controleprogramma's zijn op deze implementatierichtlijnen gericht om vervolgens per beheersmaatregel tot een oordeel te kunnen komen, volgens het *pas toe of leg uit* principe.

## B.6. Intern controleprogramma beveiliging

Het intern controleprogramma wordt opgenomen als bijlage.

## B.7. Rapporteren over beveiliging

In principe wordt bij de 4-maandsrapportage gerapporteerd over het halen van de beheersmaatregelen van het HBB, voor zover:
- een dienstonderdeel daarvoor verantwoordelijk is gesteld;
- er centrale afspraken zijn gemaakt over de uitvoering van het ICP.

Indien er per regio of dienstonderdeel op basis van een eigen risicobeoordeling wordt afgeweken van de centrale afspraken over de uitvoering van het ICP, wordt dit in de rapportage toegelicht.

In de 4-maandsrapportage wordt tevens verslag gedaan over de opvolging van eerdere controle- en auditbevindingen en escalaties.

## B.8. Verklaring van toepasselijkheid

### B.8.1. ISO-NEN 27001

De verklaring van toepasselijkheid volgt de eisen die ISO-NEN 27001 hieraan stelt, zie *4.2.1.j Bereid een Verklaring van Toepasselijkheid voor.*

- *4.2.1.j.1 Waarom doelen en maatregelen gekozen?*
  In het Strategisch kader beveiliging, HBB Deel A, is bij de toelichting op Figuur 1 “Afleiden basisniveau beveiliging” aangegeven welke standaarden waarom worden gehanteerd voor het basisniveau beveiliging dat geldt voor het merendeel van de verantwoordelijkheidsgebieden binnen de Belastingdienst. Voor zover normen niet zijn overgenomen, worden ze in deze paragraaf toegelicht.

- *4.2.1.j.2 Welke doelen en maatregelen gerealiseerd?*
  Op niveau van de Belastingdienst is het niet mogelijk een compleet en actueel inzicht hierin te geven; het aantal informatiesystemen en omgevingen waarin deze geïmplementeerd moeten worden is te omvangrijk en te complex. Daarom wordt deze paragraaf alleen benaderd vanuit het HBB zelf.

- *4.2.1.j.2 Welke doelen/maatregelen uitgesloten en waarom?*
  Hierop wordt in deze paragraaf in zijn algemeenheid toelichting gegeven.

Aan de volgende normen van ISO-NEN 27001 wordt niet of niet volledig voldaan dan wel wordt een andere invulling gegeven.

- *4.2.1.a Definitie van reikwijdte en grenzen ISMS in termen van doelen, organisatie, locaties, bezittingen en technologie*
  Een globale beschrijving is niet interessant voor betrokkenen bij het ISMS, een eigen beschrijving is gezien de omvang, complexiteit en dynamiek van de Belastingdienst niet wezenlijk betekenisvol gezien de inspanningen om een dergelijke beschrijving te maken.
  Geïnteresseerden in het antwoord op deze vraag zullen gebruik kunnen maken van de beschikbare algemene documentatie van de Belastingdienst zelf.

- *4.2.1.b.2 Wet- en regelgeving, contracten*
  Van toepassing zijnde contracten stellen - voor zover kenbaar - aan de Belastingdienst inhoudelijk geen andere eisen dan die de Belastingdienst aan zichzelf stelt voor zover het gaat om het basisbeveiligingsniveau, waarop deze verklaring van toepasselijkheid betrekking heeft.

- *4.2.1.b.4 Stel evaluatiecriteria vast*
- *4.2.1.c.2 Ontwikkel acceptatiecriteria voor aanvaardbare risiconiveaus*
- *4.2.1.e Analyseer en evalueer de risico’s*
  Vooralsnog lijkt het niet zinvol dan wel praktisch mogelijk om deze niveaus objectief en meetbaar te bepalen. Per situatie zal het verantwoordelijk management moeten beslissen over niet-afgedekte risico’s, mede op basis van advies van de beveiligingsfunctie. Zie ook HBB Deel A: “Basisniveau beveiliging: het treffen van maatregelen”, toelichting bij figuur 2.

- *4.2.1.d.3 Identificeren kwetsbaarheden*
- *4.2.1.d.4 Identificeren impact verlies BIV*
  Het identificeren van generieke kwetsbaarheden (wel bedreigingen) en impact daarvan past niet bij de baseline benadering van de Belastingdienst in overeenstemming met het VIR 2007.

- *4.2.1.f.4 Doorschuiven risico's naar verzekeraars:*
  Is niet mogelijk bij de rijksoverheid.

- *4.2.2.c Implementeren normen*
  Maatregelen worden niet getroffen als gevolg van het implementeren van de normen, maar worden getroffen tijdens het inrichten of herinrichten van processen en producten (zie *Toelichting op de hoofdstructuur van de normen*). De Belastingdienst is te omvangrijk en te complex om vanuit de normen te vertrekken teneinde maatregelen te treffen.

- *4.2.2.d Hoe meten effectiviteit controles*
  Het aantal controles bij de Belastingdienst is dermate omvangrijk en verscheiden van aard, dat het niet haalbaar is (generiek) aan te geven hoe deze in directe zin gemeten kunnen worden, anders dan door de indirecte methoden zoals bedoeld bij 4.2.3 *Bewaak en review ISMS*.

- *4.2.2.f Bewaak uitvoering ISMS*
  Dit is normale managementtaak, die gezien de verscheidenheid aan controls niet zinvol te specificeren is. Voor beveiliging is deze bewaking niet anders dan de normale bedrijfsvoeringsmechanismen. Gezien de hiervoor vermelde toelichtingen op de toepasselijkheid, kan hieraan geen andere invulling worden gegeven, dan zoals onder 4.2.3 *Bewaak en review ISMS* wordt bedoeld.

- *4.2.2.g Bewaak bronnen ISMS*
  Idem 4.2.2.f.

- *4.2.3.c Meet effectiviteit beheersmaatregelen*
  Zie commentaar bij 4.2.2.d

- *4.2.3.d Review risicoanalyses en acceptatieniveaus risico's*
  Het (aanvullend) treffen van beveiligingsmaatregelen op basis van risicoanalyse en het accepteren van restrisico's is uitgewerkt in B.2.1 en maakt als zodanig onderdeel uit van de IC/externe audit op de normen bij de goedkeuring van de inrichting van processen en producten.

- *4.2.3.h Leg acties/gebeurtenissen vast met impact ISMS*
  Deze norm is niet concreet te maken en haalbaar/controleerbaar te implementeren in een organisatie van de omvang en complexiteit van de Belastingdienst. Het geheel van beveiligingsnormen en de interne controle daarop is het maximale wat als haalbaar en voldoende wordt beschouwd.

- *4.2.4 Onderhoud en verbeter ISMS*
  Op het niveau van de feitelijke maatregelen geldt de normale P&C managementcyclus. In combinatie met de PDCA cyclus van het tactische beveiligingsproces, mede ondersteund door de uitvoering van IC en audits, alsmede de bewaking op afdoening van bevindingen wordt dit voldoende geacht om invulling aan deze norm te geven. Het tactisch

beveiligings(beheer)proces is geformuleerd in HBB Deel C.

- *4.3.2 Beheersing van documenten, a. goedkeuring, b. review en update, c. identificeren status, d. beschikbaarheid versies, e. leesbaar, f. toegankelijk voor bevoegden, g. onderscheid in/extern, h. beheerste verspreiding, i. voorkomen oneigenlijk gebruik oude versies, j. geschikte identiteit voor bewaring*
  Het aantal documenten met een belang voor beveiliging en het aantal procedures voor het beheer van die documenten is dermate omvangrijk en verscheiden dat die niet centraal te overzien zijn binnen de Belastingdienst. Eén centrale procedure voor het documentbeheer wordt niet als een zinvol en realistisch uitgangspunt gezien.
  Het aantal en de verscheidenheid van documenten en beheerprocedures is zo overweldigend groot, dat pogingen om daar centraal greep op te krijgen een veel te groot middelenbeslag zouden vragen t.o.v. het nut dat dat zou kunnen opleveren.

- *4.3.3 Beheersing bewijsstukken*
  Zie ook vorige. Of aan de eisen wordt voldaan blijkt uit het uitoefenen van interne controle, dat niet zonder die bewijsstukken kan en waarbij gebreken automatisch tot controlebevindingen zullen leiden.

- *5.1 Management commitment*
  *a instellen van ISMS, b verzekeren doelen plannen, c instellen rollen en verantwoordelijkheden, d communicatie belang doelen, beleid, verantwoordelijkheden en verbeteringen, e beschikbaarstellen voldoende middelen, f. beslissen over risico/acceptatiecriteria en -niveaus, g. zorgen dat audits plaatsvinden en h uitvoeren management reviews.*
  De eisen in de huidige fase van verbetering zijn niet met verwijzingen naar documenten aan te tonen, anders dan hiervoor aangegeven. Aan veel van deze eisen wordt op één of andere wijze voldaan, maar dat vergt een uitgebreide beschouwing, waarvan we hier afzien.

- *5.2.1 Voorzien in middelen*
  De eisen in de huidige fase van verbetering zijn niet met verwijzingen naar documenten aan te tonen, anders dan hiervoor aangegeven. Alle hieronder begrepen eisen zijn verwerkt op tal van plaatsen in het HBB Deel C. Door middel van IC en audits kan in principe vastgesteld worden of aan de eisen wordt voldaan.

- *5.2.2.c evalueer effectiviteit*
  Er bestaat geen specifieke evaluatie, anders dan IC op de naleving van beveiligingstraining en opleiding (Zie HBB Deel A).

### B.8.2. ISO-NEN 27002

Het HBB bevat de Belastingdienstinterpretatie van ISO-NEN 27002. De normen voor het strategisch beleid (hoofdstuk 1 van Deel C) staan voor een deel uitgewerkt in Deel B om te voorkomen dat Deel A te gedetailleerd wordt. Het onderscheid tussen strategisch en tactisch is niet principieel van aard.
Aan de volgende normen van ISO-NEN 27002 wordt niet of niet volledig voldaan dan wel wordt een andere invulling gegeven.

- *06.1.7.f Contact met speciale belangengroepen: geschikte aanspeekpunten*

Over incidenten wordt in principe niet met externe belangengroepen gecommuniceerd. De bedoeling van deze richtlijn is niet duidelijk.

- *6.2.2 Beveiliging behandelen in de omgang met klanten: c reden, eisen, voordelen voor toegang*
  In die zin kent de Belastingdienst geen klanten.

- *6.2.3 Beveiliging behandelen in overeenkomsten met een derde partij: c, d,e,f,h,m*
  Niet duidelijk wanneer deze zaken een rol spelen, anders dan de nu reeds in de normen opgenomen onderwerpen.

- *7.2.2 Labeling en verwerking van informatie*
  Niet van toepassing op het basisbeveiligingsniveau. In de general IT-controls is labeling niet haalbaar.

- *7.1.1 Inventarisatie van bedrijfsmiddelen: f registratie reputatie of imago*
  Er wordt geen toegevoegde waarde onderkend van het vastleggen van het imago van de Belastingdienst, het belang en daarmee imago van de organisatie is evident.

- *08.1.1.a/d Rollen en verantwoordelijkheden: functie-eisen beveiliging*
  Functiebeschrijvingen worden tegenwoordig niet meer zo gedetailleerd opgesteld gezien de dynamiek in de organisatie, zodat er geen voertuig is voor de beheersmaatregel. De maatregelen op personeelsgebied worden voldoende geacht.

- *9.1.5 Werken in beveiligde ruimten: a het niet-hebben van kennis.*
  Oncontroleerbare maatregel, preventieve maatregelen voldoende, zie C.2.19.1.j en 17.2.2.13.

- *9.1.6 Gebieden voor laden en lossen: e/f registeren/fysiek scheiden*
  Buiten scope beveiliging, te detaillistisch.

- *9.2.1 Plaatsing en bescherming van apparatuur: h. industriële omgeving*
  Niet van toepassing.

- *9.2.3 Beveiliging van kabels: e. gebruik gedocumenteerde patchlijst*
  Te gedetailleerde en uit enig verband gehaalde norm om ergens in een proces onder te brengen. Er zijn geen andere procesnormen voor de beveiliging van kabels.

- *10.4.1 Maatregelen tegen virussen: c niet-geautoriseerde bestanden.*
  Te bewerkelijke maatregel, niet realistisch.

- *10.6.1 Maatregelen voor netwerken: e coördineren beheeractiviteiten*
  Niet concreet.

- *10.7.1 Beheer verwijderbare media: f vrijgeven stations*
  Onduidelijke maatregel

- *10.7.2 Verwijderen van media: b, e vervangen door c*
  Geen onderscheid gevoelige media.

- *10.7.3 Procedures voor de behandeling van informatie*
  Dit normenkader behandelt alleen het basisniveau beveiliging.

- *10.7.4 Beveiliging van systeemdocumentatie: b toegangslijst en c op openbaar netwerk:*
  Valt onder regime van logische toegangsbeveiliging.

- *10.9.1 E-commerce*
  Deels niet van toepassing bij overheid, voorts in de geest opgenomen in andere implementatierichtlijnen, zoals ook in de Code zelf aangegeven.

- *10.9.3 Openbaar beschikbare informatie*
  De implementatierichtlijnen a, b en c kunnen niet worden toegewezen, omdat ze te globaal zijn geformuleerd. In de geest daarvan zijn voldoende implementatierichtlijnen in het HBB opgenomen.

- *11.2.1 Registratie van gebruikers: d bevestiging toegangsrechten, e ondertekenen verklaring*
  Te bewerkelijke maatregel i.v.m. omvang en verscheidenheid BD-platformen versus nut. Gedragsregels naleven wordt voldoende geacht.

- *11.2.3 Beheer van wachtwoorden: a verklaring ondertekenen*
  Te bewerkelijke maatregel i.v.m. omvang en verscheidenheid BD-platformen versus nut. Gedragsregels naleven wordt voldoende geacht.

- *11.2.2 Beheer van speciale bevoegdheden: c autorisatieproces*
  Implementatierichtlijn lastig toewijsbaar aan individuele HBB-richtlijnen i.v.m. globale formulering. De speciale bevoegdheden maken onderdeel uit van het reguliere autorisatieproces.

- *11.2.2 Beheer van speciale bevoegdheden: f ander userid*
  Beheertechnisch te lastig in centrale gebruikersregistratie via HRM-registratie.

- *11.2.3 Beheer van gebruikerswachtwoorden: f ontvangstbevestiging wachtwoorden*
  Overbodige maatregel t.o.v. gedwongen wijziging bij eerste gebruik. Bovendien kost dit teveel beheeractiviteit, namelijk ontvangst moet dan wel gecontroleerd worden.

- *11.5.6 Beperking van verbindingstijd: b beperken verbindingstijd*
  Past niet bij primaire processen Belastingdienst (Douane en FIOD moeten permanent kunnen werken) en telewerken.

- *12.2.4 Validatie van uitvoergegevens: a plausibiliteitscontrole, c verschaffen info, d reactieprocedures, f logbestand*
  Dit type maatregelen is te ingrijpend voor het nut dat ermee beoogd wordt. Zie onze norm Invoercontroles als maatregel met hetzelfde doel (systeemvreemde omgeving).

- *12.5.1 Procedures voor wijzigingsbeheer: b bevoegde gebruikers*
  Zie de vele extra normen voor functiescheidingen in het HBB. Omdat er zo veel verschillende soorten changes en omgevingen zijn, kan hier geen zinvolle concrete norm van worden gemaakt.

- *12.5.4 Uitlekken van informatie*
  Dit type maatregelen is nauwelijks praktisch toepasbaar in een grote en complexe infrastructuur. Gecertificeerde producten passen vaak niet in het infrastructuurbeleid. Onze basisverwerking op het mainframe is nauwelijks gevoelig voor trojaanse paarden.

- *12.6.1 Beheersing van technische kwetsbaarheden: h auditlog, i controle, j prioriteren*
  Bedoelde richtlijnen voegen te weinig toe: alle maatregelen moeten aantoonbaar zijn en gecontroleerd worden op basis van risicoanalyse. De grootste risico's moeten altijd als eerste worden opgelost.

- *13.2.1 Verantwoordelijkheden en procedures: a procedures ter type incident*