Genoemde typen komen normaliter te weinig voor om aparte procedures te rechtvaardigen. Algemene procedures volstaan, behalve voor virussen, waarvoor veel aparte normen in het HBB zijn opgenomen.

- *14.1.1 Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer:*
  d verzekeren: De overheid verzekert zich niet;
  f voldoende middelen: is niet te normeren, managementbeslissing;
  g veiligheid personeel/IT-voorzieningen: hiervoor zijn voldoende normen in het HBB opgenomen;
  j. bedrijfscontinuïteitsbeheer opnemen in organisatie: is geregeld in tabel “Verantwoordelijkheidsverdeling” in deel B van het HBB.

- *15.1.2 Intellectuele eigendomsrechten: c bewustwording*
  Voor alle gedragsregels gelden normen voor bewustwording, extra aandacht is alleen nodig als de risico’s daarvoor aanleiding geven.

- *15.1.3 Bescherming van bedrijfsdocumenten: a richtlijnen, d maatregelen*
  De implementatierichtlijnen zijn te algemeen gesteld. Er zijn voldoende normen in het HBB opgenomen om invulling te geven aan de bedoelingen van deze richtlijnen.

B.8.3. British Standard BS25999

Wordt geheel gevolgd.

B.8.4. Overheid (BIR, NORA)

- NORA - Best Practices Normen IT-voorzieningen zijn volledig geïntegreerd in het HBB.
- BIR - tactisch zowel als operationeel wordt in principe geheel meegenomen.

Gebruikte afkortingen

AIVD	Algemene Inlichtingen- en Veiligheidsdienst (BZK)
ARAR	Algemeen Rijksambtenarenreglement
BCM	Business continuity management, bedrijfscontinuïteitsbeheer
BHV	Bedrijfshulpverlening
BVA	Beveiligingsambtenaar
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CAO	Centrum voor Applicatieontwikkeling en -onderhoud
CBP	College Bescherming Persoonsgegevens
CFD	Centrum voor Facilitaire Dienstverlening
CFO	Chief Financial Officer
CIE	Centrum voor Infrastructuur en Exploitatie
CIO	Chief Information Officer
CPO	Chief Personnel Officer
CSO	Chief Security Officer
DG	Directeur-Generaal
DV	Dienstverlening
FB	Fysieke beveiliging
FIOD	Fiscale Inlichtingen- en Opsporingsdienst
HBB	Handboek Beveiliging Belastingdienst
IB	Informatiebeveiliging
IC	Interne controle
ICT	Informatie- en communicatietechnologie
ICP	Intern controleprogramma
IT	Informatietechnologie
IV	Informatievoorziening
FB	Fysieke beveiliging
MT	Managementteam
MvF	Ministerie van Financiën
P&C	Planning & control
PDCA	Plan - do - check – act
PV&I	Personele veiligheid & integriteit
PZ	Personeelszaken
RAD	Rijksauditdienst
RPVB	Reglement Personeelsvoorschriften Belastingdienst
SBO	Strategisch beveiligingsoverleg
TBO	Tactisch beveiligingsoverleg

B.I. Bijlage: Architectuur aanpak IT-voorzieningen

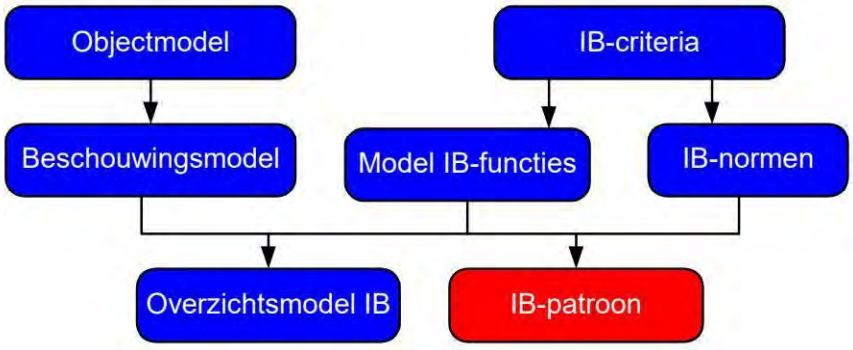
B.I.1. Inleiding

Deze best practice beschrijft de aanpak waarmee invulling kan worden gegeven aan het analyseren, adviseren en toetsen van informatiebeveiligingsaspecten in architectuurmodellen. In deze aanpak wordt een verbinding gelegd tussen architectuurmodellen en een standaard model voor IB-functies met het daarbij behorende normenkader, zie NORA best practice: Normen Informatiebeveiliging IT-voorzieningen.
Architectuurmodellen voor informatiebeveiliging richten zich meestal op de IT-oplossingen, die in een organisatie worden gekozen voor beveiligingsfuncties. In de NORA-benadering wordt uitgegaan van informatiebeveiliging als kwaliteitsaspect.
Deze NORA architectuuraanpak wordt verder uitgebouwd en geconcretiseerd met IB-patronen, die als architectuurmodules kunnen worden gezien. De patronen volgen de abstractieniveaus van de NORA best practice: Normen Informatiebeveiliging IT-voorzieningen.

Doelgroep
De doelgroep van de IB-architectuur is de architect, ontwerper, IB-specialist en IT-auditor. Die kunnen de modellen gebruiken als gereedschap voor het maken van IT-ontwerpen voor informatiebeveiliging, het adviseren over het treffen van beveiligingsmaatregelen of het toetsen van ontwerpen aan normen.

B.I.2. Modelleringaanpak

Voordat de verschillende stappen in de modelleringaanpak worden uitgelegd, geeft
Figuur **5** een overzicht van deze stappen.



Figuur 5 NORA aanpak architectuur IB

Informatiebeveiliging beschouwen wij als een kwaliteitsaspect van de bedrijfsvoering van een organisatie. Dat betekent dat we eerst iets over die bedrijfsvoering moeten weten om vandaar uit naar informatiebeveiliging te kunnen kijken. De bedrijfsvoering wordt in architectuurplaten meestal afgebeeld in een z.g. *objectmodel* met bedrijfsfuncties, objecten en interacties.

Omdat beveiliging als *aspect* geheel verweven is in de architectuur van de bedrijfsvoering en kwaliteitsaspecten niet als bedrijfsfuncties kunnen worden afgebeeld, hebben we een aparte plaat nodig om duidelijk te maken waar beveiligingsfuncties in een architectuur werkzaam moeten zijn.

Beveiliging komt in IT-ontwerpen voor als afzonderlijk herkenbare objecten, zoals bijvoorbeeld firewalls en toegangsmodules maar ook in niet direct herkenbare gedaantes, zoals parameters in een besturingssysteem of een functiescheiding. Om de beveiligingsobjecten en functies in een architectuur af te kunnen beelden, gebruiken we de architectuurplaat: *beschouwingsmodel*.

In het beschouwingsmodel tekenen we vervolgens de IB-functies met hun onderlinge relaties, waaruit een architectuurplaat ontstaat voor Informatiebeveiliging. Deze plaat noemen we het *overzichtsmodel-IB*. Omdat de compartimentering (zonering) van netwerken en de positionering van IT-systemen daarin in belangrijke mate bepaald wordt door beveiliging, kiezen we er voor om de architectuurplaten daarmee vorm te geven. Voor inzicht in details van de oplossingen worden IB-patronen gebruikt.

Samengevat omvat in deze aanpak van een IB-architectuur dus een model of een reeks van modellen, dat laat zien hoe het bedrijfsfuncties samenhangen met het kwaliteitsaspect Informatiebeveiliging.

Een IB-patroon, als onderdeel van de IB-architectuur is een standaard beschrijving van een probleem en oplossing binnen een bepaalde context, met als doel dat de oplossing algemener inzetbaar wordt. Patronen zijn te beschouwen als *bouwstenen* op architectuurniveau.

De hier geschetste architectuuraanpak wordt momenteel door een community van de PvIB verder uitgebouwd door het modelleren van veel voorkomende beveiligingssituaties in IB-patronen. De focus van de IB-patronen is daarbij vooralsnog gericht op IT.

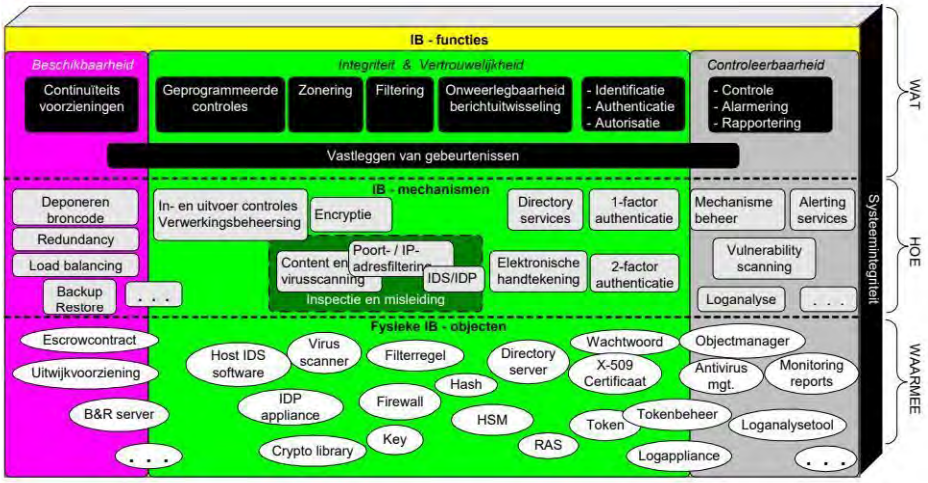
B.I.3. Model IB-functies

Het referentiekader voor de modelleringaanpak wordt gevormd door het model IB-functies van Figuur 6, dat bedoeld is om te ordenen en te verbinden. Het model is een NORA-doorontwikkeling van ISO-NEN 7498-2[5] Een IB-functie is een logische groepering van geautomatiseerde activiteiten, die op een bepaald beveiligingsdoel is gericht. In samenhang worden de negen afgebeelde beveiligingsfuncties dekkend geacht voor de informatiebeveiliging van IT voorzieningen (zwarte functieblokken).

In het architectuurmodel zijn deze IB-functies geprojecteerd op de kwaliteitscriteria voor informatiebeveiliging: Beschikbaarheid, Integriteit, Vertrouwelijkheid en Controleerbaarheid. In *samenhang* vormen ze de WAT-laag van het model.

. . . . . .

[5] ISO-NEN 7498-2[5] Information processing systems : Open Systems Interconnection Basic Reference Model – Part 2: Security Architecture uit 1991.



Figuur 6 Model IB-functies

De IB-functies met bijbehorende mechanismen en fysieke objecten, zijn voor de eenvoud van afbeelding, op de criteria geprojecteerd, die ze *primair* ondersteunen, maar de functies voor integriteit en vertrouwelijkheid dragen bijvoorbeeld ook bij aan beschikbaarheid. Per IB-functie wordt een doelstelling, definitie, toelichting en motivering gegeven in de NORA best practice Normen informatiebeveiliging IT-voorzieningen.

De IB-mechanismen vormen de HOE-laag en zijn *technische* concepten (technieken) die het WAT van de IB-functies invullen. Omdat techniek zich steeds verder ontwikkelt, illustreert de figuur slechts een aantal bekende voorbeelden.

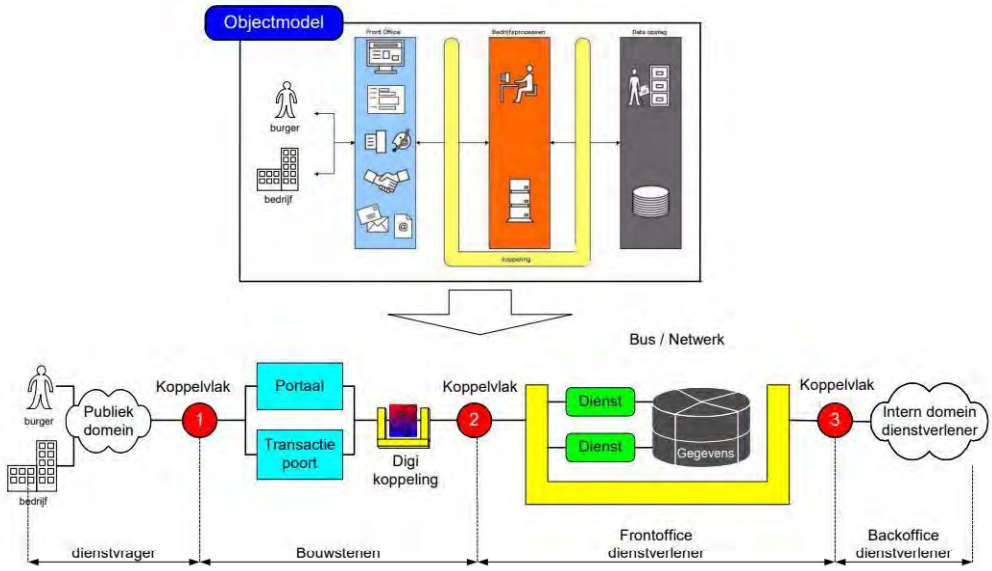
De fysieke IB-objecten vormen de WAARMEE-laag. Dit zijn IT-onderdelen, die de IB-mechanismen daadwerkelijk uitvoeren. Ze kunnen onderdeel zijn van een besturingsprogramma of applicatie, maar worden ook als afzonderlijke fysieke modules uitgevoerd. Ook hier zijn slechts enkele bekende voorbeelden getekend. Hoewel referentiearchitecturen de HOE- en WAARMEE-laag meestal niet beschrijven, is dat hier wel gedaan om duidelijk te maken hoe en waarmee beveiligingsfuncties uiteindelijk werkzaam kunnen zijn in de IT.

In de beschrijving die nu volgt is aangegeven welke modellen we gebruiken om informatiebeveiliging in een ontwerp inzichtelijk te maken.

B.I.4. Beschouwingsmodel

Het beschouwingsmodel is een vertaling van het objectmodel, die we gebruiken om de relatie met IB-functies aan te geven. Figuur 7 geeft aan hoe een beschouwingsmodel van bijvoorbeeld een NORA- keten er uit kan zien waarbij de “Basisarchitectuur overheidsorganisatie” als objectmodel dient.

De vertaalslag bestaat eruit dat alleen IT-voorzieningen in beschouwing worden genomen en dat er koppelvlakken worden gebruikt om netwerkzones zichtbaar te maken. De koppelvlakken zijn genummerd om ze afzonderlijk voor beveiliging te kunnen beschouwen.



Figuur 7 Beschouwingsmodel van een NORA keten

Als toelichting op het NORA voorbeeld nog het volgende:
De IT-voorzieningen *Portaal* en *Transactiepoort* die centraal voor de overheid als frontoffice dienen, zijn in een afzonderlijke netwerkzone opgenomen onder de term Bouwstenen, omdat ze in de NORA zo worden aangeduid.

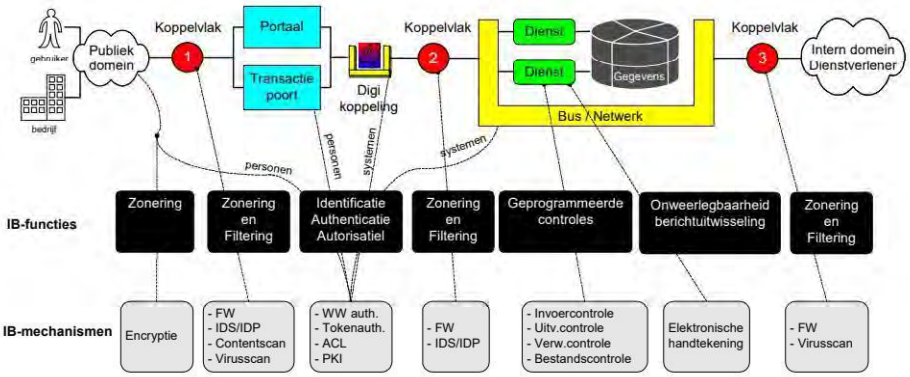
Ook *Digikoppeling*, als een reeks standaarden voor het uitwisselen van elektronische gegevens binnen de overheid is zo'n bouwsteen.

Met *dienstverlener* wordt de desbetreffende overheidsinstantie bedoeld, die informatie wil uitwisselen met burgers en bedrijven.

B.I.5. Overzichtsmodel-IB

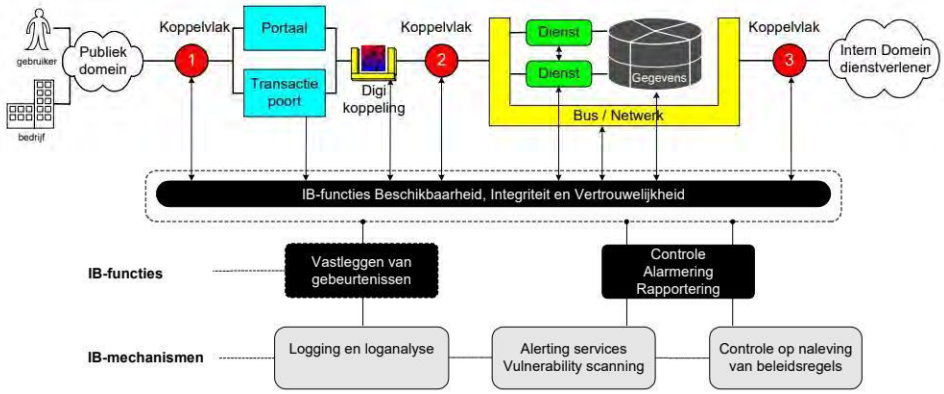
Het overzichtsmodel ontstaat door op het beschouwingsmodel de relevante IB-functies af te beelden met de bijbehorende IB-mechanismen. De daarmee verkregen schets van functies en uitvoerende mechanismen is hier als voorbeeld niet uitputtend, maar dient voor het verkrijgen van overzicht en inzicht in de plek waar IB werkzaam is in bedijfsketens en infrastructuren.

Voor de eenvoud beperken we de scope van het overzichtsmodel bijvoorbeeld tot het afbeelden van de vereiste Integriteit en Vertrouwelijkheid voor een bepaalde infrastructuur, of alleen voor het criterium Controleerbaarheid. Op dit globale niveau worden de fysieke IB-objecten weggelaten. De IB-functie continuïteitsvoorzieningen blijkt in de praktijk niet eenvoudig te kunnen worden afgebeeld in overzichtsmodellen. Daarvoor is een gedetailleerder en meer fysiek georiënteerd model nodig, zoals een configuratieschema.



Figuur 8 Overzichtsmodel voor integriteit en vertrouwelijkheid van een NORA keten

Als voorbeeld van een overzichtsmodel laat Figuur 4 zien hoe de IB-functies voor de criteria Integriteit en Vertrouwelijkheid in een NORA-keten uitwerken. Voor betrouwbare communicatie tussen burger en overheid is een vertrouwd toegangspad gewenst tot het portaal van de overheid. Daarvoor is encryptie gebruikt.
Vanaf het portaal tot aan het interne domein van de ketenpartner is er sprake van een besloten netwerk. Ook dit kan als een vertrouwd toegangspad worden beschouwd, mede door de werking van de andere in dit pad gepositioneerde IB-functies. Merk op dat de functies Zonering en Filtering op verschillende plaatsen in de keten door IB-mechanismen op een andere manier wordt ingevuld. De positionering van geprogrammeerde controles kan in dergelijke globale modellen uiteraard maar beperkt zichtbaar worden gemaakt als gevolg van de verwevenheid daarvan met applicaties (hier Dienst genoemd). Dit geldt in zekere zin ook voor alle andere mechanismen.
De zeggingskracht van deze overzichtsmodellen zit met name niet in de *volledigheid* van het afbeelden van beveiligingsmaatregelen, maar veel meer in het *totale* en (dus) *globale* inzicht. Voor een meer gedetailleerd inzicht kunnen onder meer de IB-patronen worden gebruikt.



Figuur 9 Overzichtsmodel voor controleerbaarheid van een NORA-keten

Figuur 9 laat zien welke IB-functies voor Controleerbaarheid werkzaam zijn in een NORA-keten. IB-mechanismen voor integriteit en vertrouwelijkheid worden ingesteld en beheerd door afzonderlijke tools of met tooling die in de IT-voorzieningen zelf is geïntegreerd.

Beveiligingsgebeurtenissen die in de IT-keten hebben plaatsgevonden, worden vastgelegd voor controledoeleinden. Dit vastleggen (loggen) vereist aparte infrastructurele voorzieningen. Wanneer drempelwaarden worden overschreden van bijvoorbeeld een firewall, IDS of virusscanner, dan moet een mechanisme zorgdragen voor alarmering naar een systeembeheerder of een CERT[6].

Evenals geldt voor de criteria Integriteit en Vertrouwelijkheid, worden voor Controleerbaarheid door de keten heen steeds dezelfde functies toegepast, maar de toegepaste mechanismen en objecten kunnen per situatie verschillen.

B.I.6. IB-patronen

Een patroon is een abstractie van een probleem en oplossing binnen een bepaalde context, met als doel de oplossing algemener inzetbaar te maken. Patronen zijn vooral bedoeld als *middel* om oplossingen op een compacte standaard manier te beschrijven en die oplossingen daarmee toegankelijk te maken.

De Open Group[7] heeft voor patronen een beschrijvingsmodel ontwikkeld die voor de IB-patronen zijn aangevuld met enkele extra rubrieken om beter praktisch bruikbaar te maken, zie de Template.

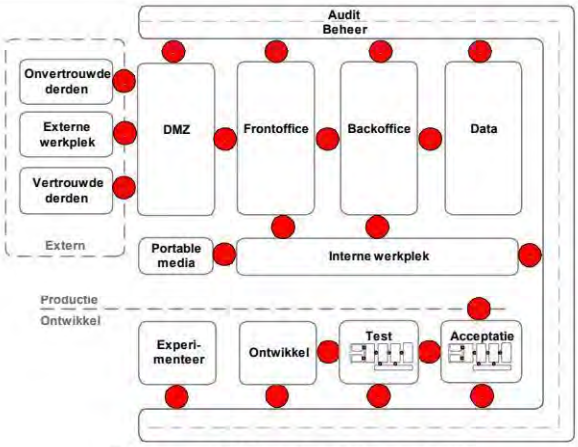
IB-patronen kunnen zowel thematisch als hiërarchisch worden gerubriceerd. We onderkennen daarbij patronen die een oplossing bieden voor één specifiek probleem (b.v. Digitale Handtekening), maar ook patronen die een bepaald thema beschrijven, zoals b.v. koppelvlakken en Identity & Access Management (IAM). Elk thema kan daarbij bestaan uit verschillende specifieke patronen.

In de vakliteratuur (o.a. de Open Group) zijn patroonbeschrijvingen (“security patterns”) beschikbaar. Deze worden in de praktijk echter weinig gebruikt omdat ze in de academische wereld zijn ontstaan en blijven hangen in een (te) hoog abstractieniveau De hier bedoelde IB-patronen worden in de community van het PvIB door beroepsgenoten ontwikkeld vanuit de praktijk. Daarnaast wordt in de patronen de link gelegd naar normen voor informatiebeveiliging.

B.I.7. Template van een IB-patroon

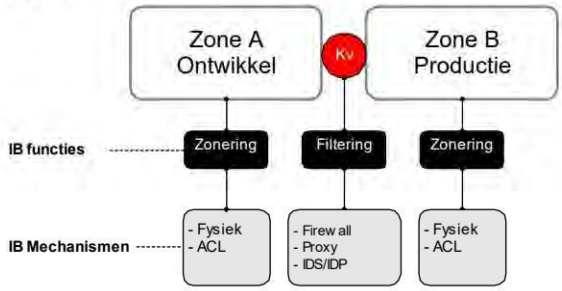
Rubriek	Omschrijving
	Naam Vat het doel van het patroon kort samen, bij voorkeur in termen van de oplossing
Criteria	Welke van de IB-criteria: *Beschikbaarheid*, *Integriteit*, *Vertrouwelijkheid* en *Controleerbaarheid* zijn aan de orde?
Context	Hoe ziet de omgeving er uit waarin het probleem zich voordoet, bij voorkeur te benaderen aan de hand van de standaard context: het patroon Zonering

[6] CERT = Computer Emergency Response Team
[7] Open Group: Technical Guide for Security Design Patterns, April 2004, [4]



Figuur 10 Voorbeeld context

Probleem	Welk risico moet worden beheerst?
Oplossing	Welke (technische) beveiligingsmaatregelen zijn er als (standaard) oplossing te geven?



Figuur 11 Voorbeeld oplossing

Afwegingen	Wat zijn de voor- en nadelen en doorslaggevende argumenten voor de keuze van de oplossing?
Voorbeelden	Welke beproefde toepassingsvoorbeelden van de oplossing zijn er te geven?
Implicaties	Wat moet de organisatie doen om gebruik te kunnen maken van de geboden oplossing van een patroon? (impact en randvoorwaarden) Wat zijn de gedragskenmerken tijdens operationeel gebruik?
Gerelateerde patronen	Van welke patronen is de oplossing (van dit patroon) afhankelijk?
Normen	Aan welke Beheersmaatregelen dan wel Implementatierichtlijnen van NORA Best practice Normen Informatiebeveiliging IT-voorzieningen geeft dit patroon invulling?

	IB functie	**Beheersmaatregel**	**Implementatierichtlijnen**
	5. Zonering	5.1 Zonering technische infrastructuur	1. Er zijn aparte zones voor Ontwikkeling, Test, Acceptatie en Productie (bijvoorbeeld)
	6. Filtering	6.1 Controle op communicatieged rag	3. Al het gegevensverkeer vanuit externe of onvertrouwde zones wordt real-time inhoudelijk geïnspecteerd op inbraakpogingen. (bijvoorbeeld)

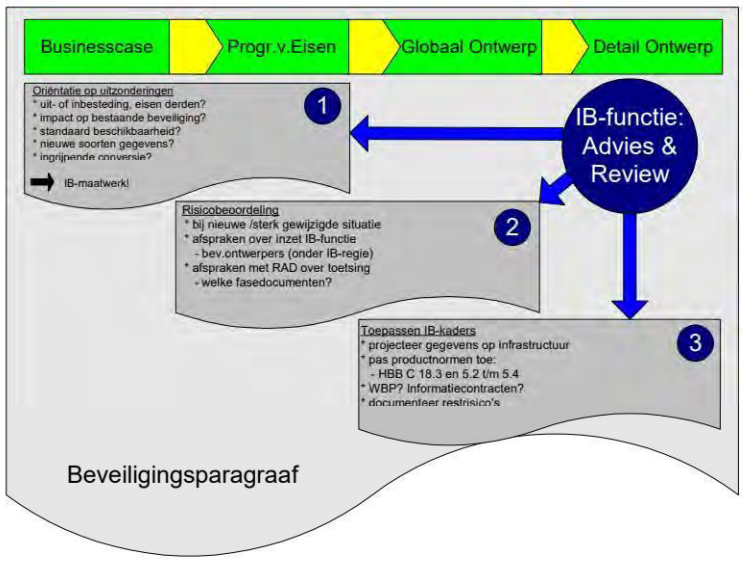
B.II. Bijlage: Beveiliging in het ontwerp van processen

B.II.1. Aanpak

In elk ontwerpproduct, c.q. opdracht (PvE, Definitiestudie) wordt aan de hand van een aantal attentiepunten en de normen uit het HBB een beveiligingsparagraaf opgenomen.

Beveiligingsparagraaf
De ontwerpmethodiek is erop gericht de beveiligingsparagraaf op basis van voortschrijdend inzicht in te vullen aan de hand van een drietal opeenvolgende stappen. Aangezien beveiliging als aspect een integraal deel uitmaakt van het gehele ontwerp, kan deze beveiligingsparagraaf deels ook als een view of (verwijzend) resumé worden vormgegeven.
In elke ontwerpfase wordt de uitwerking in een vorige fase gevalideerd.
In onderstaande figuur wordt de inhoud van de stappen kort aangeduid en aan de ontwerpfasen gekoppeld:

Relatie met ontwerpproces



B.II.2. Eerste fase: oriëntatie op uitzonderingen

Voor het treffen van de juiste beveiligingsmaatregelen is het van belang elke opdracht voor een procesontwerp te kunnen positioneren ten opzichte van de beveiligingsstandaards, de impact op bestaande beveiliging en recht te doen aan beveiligingsverantwoordelijkheden binnen en buiten de Belastingdienst.

Afwijkende situaties vroeg signaleren

Bij de oriëntatie gaat het er met name om afwijkende situaties zo vroeg mogelijk aan het licht te brengen. Afwijkende situaties kunnen namelijk aanleiding geven tot het treffen van maatregelen in andere verantwoordelijkheidsgebieden, waarop apart moeten worden gestuurd of tot het maken van extra afspraken om input te leveren vanuit de beveiligingsdiscipline.

Voor het ontwerpen van de beveiligingsparagraaf kan het namelijk wenselijk zijn ondersteund te worden door beveiligingsspecialisten. Deze ondersteuning kan variëren van het voeren van een afstemmingsgesprek met een Procesarchitect Beveiliging tot en met het participeren in het ontwerp of het inhuren van IB-specialisten.

De volgende attentiepunten zijn in de oriëntatiestap aan de orde:

Uit- en inbesteding, eisen derden?

TPM beheer en exploitatie

De Belastingdienst kan ontwerp-, bouw- en/of technisch beheer en exploitatiediensten aan derden uitbesteden. In dat geval zal de Belastingdienst beveiligingseisen moeten stellen aan die derden. Bij uitbesteding van technisch beheer en exploitatie zal bijvoorbeeld een Third Party Mededeling inzake beheer en beveiliging gevraagd moeten worden. De eisen kunnen worden ontleend aan de normen van het HBB.

Belastingdienst als serviceorganisatie

De Belastingdienst kan ook voor derden als serviceorganisatie optreden, waarbij ontwerp-, bouw- en/of technisch beheer en exploitatiediensten geleverd worden. In dat geval zal nagegaan moeten worden welke eisen derden aan de Belastingdienst stellen en of de Belastingdienst daaraan kan en wil voldoen. De invulling daarvan is vooralsnog maatwerk.
E.e.a. heeft ook betekenis voor tenders/offertes en werkt ook door in de Service Niveau Overeenkomsten.

Belastingdienst in ketens

Ingeval de Belastingdienst voor derden optreedt als taakorganisatie of derden dat voor de Belastingdienst gaan doen (werken in ketens), moet worden vastgesteld welke eisen de Belastingdienst moet stellen bij verwerking van haar gegevens bij externen en omgekeerd welke eisen derden aan de Belastingdienst als taakorganisatie stellen bij verwerking van externe gegevens. In dergelijke situaties kan het zijn dat er aparte financiële of beheerverantwoording moet worden afgelegd. De invulling daarvan is vooralsnog maatwerk. Tijdige inschakeling van de accountantsdiscipline van beide partijen is hierbij ook van belang.

Impact bestaande beveiligingsvoorzieningen?

Het is van belang tijdig vast te stellen dat op een goede wijze gebruik wordt gemaakt van de bestaande ICT-voorzieningen. Introductie van niet-standaard infrastructuurcomponenten of ander dan bedoeld gebruik van bestaande ICT-voorzieningen kan beveiligingsrisico's opleveren. Maar het kan ook gewenst zijn het beleid en/of de normen aan te passen aan deze nieuwe ontwikkelingen. Voorts is het van belang vast te stellen dat geen oplossingen worden ontworpen, die reeds in portfolio zijn.

Standaard beschikbaarheidsniveau?

De maatregelen om een bepaald beschikbaarheidsniveau voor processen te kunnen handhaven en bij calamiteiten te kunnen uitwijken, zijn zoveel mogelijk generiek van aard en niet snel aan te passen. Om die reden is het van belang om tijdig te bepalen of er eventueel hogere beschikbaarheids-eisen te stellen zijn dan standaard voor de portfolio van toepassingen wordt geboden.

Indien hogere eisen aan de orde zijn, zal moeten worden uitgewerkt:
- wat de maximaal toegestane uitvalsduur (MTU) is;
- wat het maximaal toegestaan digitaal gegevens verlies (MDV) is;
- hoe niet-digitale informatie gereconstrueerd kan worden.

Bedrijfscontinuïteitsbeheer

Vanuit het aparte kennisgebied Bedrijfscontinuïteitsbeheer kan hierbij ondersteuning worden geboden, bijvoorbeeld door een hierop toegesneden Business Impact Analysis (BIA).

Nieuwe soorten gevoelige gegevens?
Het basis beveiligingsniveau gaat uit van massale, privacygevoelige en financiële gegevens. In termen van de Wet Bescherming Persoonsgegevens betreft het klasse II Verhoogd Risico.
Voor sommige gegevenscategorieën is een hoger niveau van beveiliging noodzakelijk dan wel wenselijk op grond waarvan aanvullende beveiligingsmaatregelen aan de orde kunnen zijn.
Het is van belang tijdig te onderkennen of de daarvoor gebruikelijk te treffen maatregelen hierop toegesneden zijn of dat hiervoor unieke maatregelen moeten worden getroffen, die extra inzet van beveiligingsspecialisten noodzakelijk maken.

Maatwerk

Vooralsnog zijn dergelijke aanvullende maatregelen niet ondergebracht in één algemeen classificatiesysteem, dus zal er sprake moeten zijn van maatwerk.

Ingrijpende conversie van gegevens?
Voor conversie is vooralsnog geen basis beveiligingsniveau te duiden. Het gaat er om of er conversieproblemen zijn te verwachten, die om extra controles vragen. Dit hangt sterk af van de aard (complexiteit, samenhang) en omvang van de betrokken gegevensverzamelingen en de mate waarin er veranderingen optreden.

Extra maatregelen

Voor conversie zijn geen normen geformuleerd. Om die reden volgen hier enkele mogelijke maatregelsoorten:

Aanvullende éénmalige maatregelen in applicaties
- extra invoercontroles
- weergeven van extra gedetailleerde verwerkingstotalen

Aanvullende éénmalige maatregelen in de AO/IC
- extra handmatige juistheidcontroles steekproefsgewijs dan wel integraal
- extra verbandscontroles
- aparte verantwoordingsrapportage
- extra onafhankelijke audits

B.II.3. Tweede fase: risicobeoordeling

Het treffen van beveiligingsmaatregelen behoort te worden gebaseerd op de risico's. Dat betekent dat er eerst een risicobeoordeling dient te worden uitgevoerd, ook wel een afhankelijkheids- en kwetsbaarheidsanalyse genoemd.

Voorwerk in eerdere fase(n)

In de eerste stap bij het invullen van de beveiligingsparagraaf in de ontwerpdocumenten heeft er een oriëntatie plaatsgevonden met betrekking tot mogelijk afwijkende situaties. Indien deze fase geen bijzonderheden oplevert en als het gaat om vertrouwde processen en oplossingen, bieden de normen in het HBB voldoende houvast voor het treffen van maatregelen

In alle andere situaties is het van belang een specifieke risico- en impactanalyse uit te voeren, die als aanvulling op het volgen van de normen volgens het basis beveiligingsniveau kan worden gezien.

Falsificeren procesflow

Bij het ontwerp van processen bevelen wij aan het falsificeren van de procesflow toe te passen. Deze methode beoogt met een globale systeemflow als input materiedeskundigen en beveiligingsspecialisten in een vrije sessie over risico's te laten brainstormen. Doel is het inventariseren wat er in de gegeven omstandigheden per gegevensstroom mis kan gaan, waarna bezien kan worden of er andere dan de standaardmaatregelen van toepassing kunnen zijn. Geprogrammeerde controles worden gebruikt als algemeen vertrekpunt voor de soorten risico's die in beschouwing worden genomen.

Afspraken over inzet van deskundigen

Op grond van de oriëntatiestap en de risico- en impactanalyse ontstaat er een goed beeld over de mate waarin het ontwerp langs standaard paden kan verlopen als het gaat om informatiebeveiliging of dat het gewenst dan wel noodzakelijk is gebruik te maken van de inzet van beveiligingsdeskundigheid in de verdere uitwerking. Beveiligingsdeskundigen kunnen medewerkers van IV-beleid zijn dan wel onder regie van IV-beleid worden ingehuurd of vanuit andere organisatiedelen worden ingezet.

Als het gaat om belangrijke vernieuwingen van processen waarbij jaarlijkse ontvangsten of uitgaven van enige omvang zijn gemoeid en als er in- of uitbesteding aan de orde is, is afstemming met RAD noodzakelijk. Er zullen dan afspraken moeten worden gemaakt over toetsing van ontwerpdocumenten. In voorkomende gevallen moet RAD worden betrokken in het overleg met andere partijen over externe verantwoordingstrajecten.

B.II.4. Derde fase: toepassen productnormen

Projecteer gegevens op de infrastructuur

In de derde fase worden de productnormen toegepast plus eventuele extra maatregelen vanwege eerdere risicobeoordelingen. Om dat te kunnen doen is het noodzakelijk eerst inzicht te hebben in de positionering van gegevensstromen op de datacommunicatieservices en de positionering van gegevensverzamelingen op de platformen. Ook moet duidelijk hoe de (sub)processen moeten worden getypeerd: batch, on-line of

Typeer de processen

berichtverwerking. Dit inzicht is noodzakelijk om te weten welke soort maatregelen waar getroffen moeten worden.

Het treffen van de maatregelen vindt plaats op basis van de normen van het HBB Deel C, *Beveiligingsparagraaf procesontwerp*.

Pas de normen toe

Omdat sommige beveiligingsregels niet anders dan op een hoog abstractieniveau kunnen worden weergegeven, heeft de normerende betekenis zijn beperkingen en komt het aan op de vertaling naar de specifieke situatie. Inschakelen van specialisten kan hierbij ondersteunend zijn.

Aan meldingsplicht WBP voldaan?

Volgens de Wet Bescherming Persoonsgegevens moet vastgesteld worden of de gegevenstypen (indien van toepassing) vallen onder de laatste privacymelding van de Belastingdienst aan het College Privacy Bescherming of onder het Vrijstellingsbesluit WBP. Is dat niet het geval, dan moet deze situatie worden gemeld aan de WBP-coördinator.

Informatiecontracten bij externe geg.uitwisseling

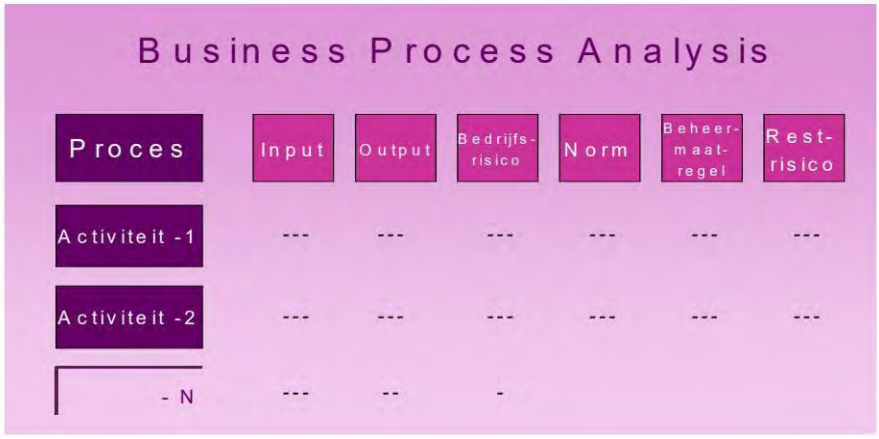
Gegevensuitwisseling met externen kan plaatsvinden via bestands-uitwisseling of via het verlenen van toegang tot informatiesystemen.
In schriftelijke afspraken wordt vastgelegd onder wiens verantwoordelijkheid de gegevensuitwisseling plaatsvindt, aan welke beveiligingseisen de uitwisseling voldoet en welke maatregelen door partijen worden getroffen.

Voor het opstellen van contracten zijn uitgebreide normen in het HBB opgenomen.

Business Process Analysis

Om vast te stellen of bij het Detail Ontwerp van het proces een sluitend en evenwichtig geheel van beveiligingsmaatregelen is ontworpen en om deze kort samen te vatten, wordt aanbevolen een Business Process Analysis (BPA) op te stellen. Geaccepteerde (rest)risico's worden expliciet vastgelegd met een motivering waarom hiervoor geen beveiligingsmaatregelen worden getroffen.

De optimale vorm om dit vast te leggen wordt hieronder weergegeven:



Ministerie van Financiën

Handboek Beveiliging Belastingdienst

Mei 2011

Het Handboek Beveiliging Belastingdienst:

"Van onbewust risico's lopen naar bewust risico's aanvaarden"

De maatschappij verandert en stelt andere eisen aan de Belastingdienst dan voorheen. Overheidsinitiatieven ontstaan om ons heen, normen en waarden veranderen.

We hebben taken gekregen die samenwerking met partners vereisen, in ketens. Met organisaties die een onderdeel zijn van een totaal proces, als informatieafnemer of juist als leverancier.
We willen werken in de actualiteit, op basis van gebeurtenissen, begrijpelijk en uit te leggen. We willen de afstand tot burgers en bedrijven verkleinen en ons imago - en dat van de gehele overheid - verstevigen om compliant gedrag in de hand te werken.

Missie Rijksoverheid

De Belastingdienst staat voor een integere organisatie. Belastingplichtigen, toeslaggerechtigden en partners van de Belastingdienst moeten erop kunnen vertrouwen dat de Belastingdienst integer is. Hiermee sluiten we aan bij de missie van de Rijksoverheid: met hart voor de publieke zaak, integer en met kennis van zaken. Dit speelt een belangrijke rol in het bevorderen van compliant gedrag van belastingplichtigen.

Permanente opdracht

Basiswaarden

De bedrijfsdoelstellingen staan beschreven in de bedrijfsplannen van de Belastingdienst, evenals de permanente opdracht en de uitgangspunten voor de inrichting en verandering van onze organisatie. Van de kwaliteit van de totale bedrijfsvoering van de Belastingdienst is beveiliging een onlosmakelijk onderdeel. De grondslagen zijn betrouwbaarheid, bescherming van gegevens, houding en gedrag. Het vertaalt zich naar de drie basiswaarden:

- *Geloofwaardigheid*. De Belastingdienst neemt zijn opdracht serieus en houdt zich aan afspraken;
- *Verantwoordelijkheid*. De Belastingdienst gaat verantwoord om met de bevoegdheden en legt hierover verantwoording af;
- *Zorgvuldigheid*. De Belastingdienst behandelt iedereen met respect en houdt rekening met verwachtingen, rechten en belangen.

Het komt neer op het voldoen aan maatschappelijke verwachtingen, zoals naleven van de wet- en regelgeving en het afleggen van adequate verantwoording daarover. We aanvaarden daarbij bewust risico's.

De basiswaarden zijn het visitekaartje van de Belastingdienst, maar gelden ook intern voor de manier waarop medewerkers onderling met elkaar omgaan. De Belastingdienst streeft naar een open cultuur waarin integriteit bespreekbaar is, medewerkers elkaar aanspreken en leidinggevenden en medewerkers met elkaar in gesprek gaan over integriteitsdilemma's.

In het Handboek Beveiliging Belastingdienst worden de bedrijfsplannen vertaald naar beveiliging. Het handboek draagt bij aan de besturingsafspraken voor de IV-keten: beschikbaar, betrouwbaar, bestuurbaar, betaalbaar.

Beveiligingsprincipes

De bedrijfsprincipes zijn aangevuld met beveiligingsprincipes. Belangrijke kernzinnen hierin zijn "vertrouwen voorop, controle achteraf" en "bewust kiezen voor aanvaardbare risico's".
Vertrouwen is hier *vertrouwen met gezond verstand*. Dus niet naïef of blind vertrouwen! Met gezond verstand bedoelen we *gerelateerd aan risico's, waar het management het over eens is*. Maar vertrouwen is ook: controleren of het werkt. Zulke controles zijn vanzelfsprekend, er valt immers niets te verbergen. Dat geeft bewegingsvrijheid en verantwoordelijkheid.
Terecht, want waarom zouden wij onszelf en onze collega's niet vertrouwen?

Bewust kiezen betekent dat we voor die keuze gaan. Het betekent ook dat je keuze transparant moet zijn en dat je hem moet kunnen uitleggen. Daarvoor zullen wij ons kwetsbaar op moeten kunnen stellen. Zolang we dit nog afwijkend vinden, is daar lef voor nodig. Er is ook lef nodig om de cultuurverandering in te gaan, temeer omdat we bij voorkeur alles (technisch) dichttimmerden. Deze gedachten zitten achter het beveiligingsbeleid. Ze hebben impact op de veiligheid en integriteit van medewerkers, de fysieke beveiliging en de informatiebeveiliging. Het betekent dat we gaan van onbewust risico's lopen naar bewust risico's aanvaarden.

Persoonsgegevens

Doel en reikwijdte van het handboek

Beleidsterreinen beveiliging

Beveiliging omvat de volgende beleidsterreinen:

- *Personele veiligheid en integriteit*: de veiligheid voor medewerkers en bezoekers en de invulling van de begrippen "goed ambtenaarschap" en "goed werkgeverschap";
- *Fysieke beveiliging*: de veiligheid van gebouwen en terreinen;
- *Informatiebeveiliging*: de beschikbaarheid, vertrouwelijkheid en integriteit van alle vormen van informatie en verwerking daarvan (zowel handmatig als geautomatiseerd);
- *Bedrijfscontinuïteit*: het omgaan met risico's die de ongestoorde bedrijfsvoering van de Belastingdienst bedreigen.

Kwaliteit bedrijfsvoering

De overlap van deze terreinen met elkaar behoeft geen uitleg. Alleen in samenhang kunnen de uiteindelijke maatregelen doeltreffend en doelmatig zijn, onder de noemer van beveiliging. De impact die een calamiteit heeft of kan hebben op de organisatie, bepaalt of deze op het terrein van bedrijfscontinuïteit ligt: alles wat de kritische bedrijfsfuncties kan verstoren. Ook bestaat samenhang met de kwaliteit van de gehele bedrijfsvoering: beveiliging is een onderdeel daarvan en zodoende ook een integraal onderdeel van de interne controle.

Doelstelling

De doelstelling van het handboek is het vastleggen van het beveiligingsbeleid en de beveiligingsnormen van de Belastingdienst. Zodoende worden de voorwaarden gecreëerd, waarmee:

- van toepassing zijnde wet- en regelgeving wordt nageleefd;
- de Belastingdienst aan zijn primaire doelstellingen kan voldoen;
- bedrijfsschade en persoonlijk letsel zoveel mogelijk wordt voorkomen;
- veilige (arbeids)omstandigheden worden geboden aan medewerkers en bezoekers.

Om tot een geslaagde implementatie en naleving van beveiliging binnen de Belastingdienst te komen zijn de volgende factoren van wezenlijk belang:

- één handboek beveiliging voor de gehele Belastingdienst.
- een organisatieonafhankelijke opzet, met het oog op de houdbaarheid bij samenwerking met andere (overheids)partijen en in- of uitbesteding.
- een benadering ten aanzien van het implementeren van beveiligingsrichtlijnen die past binnen de organisatiecultuur;
- zichtbare ondersteuning en betrokkenheid van het management;
- een goed begrip van beveiligingsrisico's, risicoanalyse en risicomanagement;
- medewerkers die bekend zijn met en actief bijdragen aan realisatie van een acceptabel niveau van beveiliging;
- een evenwichtig meetsysteem, dat gebruikt wordt om de effectiviteit van het beveiligingsbeleid te beoordelen en verbeteringen aandraagt.

Doelgroepen

Het handboek is bedoeld voor het lijnmanagement en degenen die tot taak hebben organisatie, processen en facilitaire voorzieningen in te richten en medewerkers te instrueren.
Het handboek vormt de basis voor het stellen van eisen aan (externe) leveranciers van diensten. Het dient voor het stellen van

betrouwbaarheidseisen aan ketenpartners, waarvan de Belastingdienst in de bedrijfsvoering afhankelijk is. Omgekeerd dient het als verantwoordingsmiddel naar ketenpartners, die voor hun bedrijfsvoering afhankelijk zijn van de Belastingdienst.
Het handboek vormt de basis voor inrichtingsadviezen door beveiligingsmedewerkers. Controlemedewerkers baseren ten slotte hun interne controles mede op dit handboek.

Reikwijdte

De reikwijdte van het handboek is de gehele bedrijfsvoering van de Belastingdienst, de materiële- en immateriële eigendommen en alle personen die zich op locaties van de Belastingdienst bevinden.
Daarnaast vallen activiteiten die door de Belastingdienst zijn inbesteed of uitbesteed aan externe leveranciers, alsmede eigendommen van derden die ter beschikking staan van de Belastingdienst onder de reikwijdte van het handboek.

Indeling van het handboek

Het Handboek Beveiliging Belastingdienst bestaat uit dit algemene hoofdstuk met inleiding, doel en reikwijdte, indeling en inhoudsopgave. Het omvat verder een aantal delen, te weten:

A. **Het strategisch kader beveiliging**, met daarin de belangrijkste beleidsmatige uitgangspunten voor beveiliging. De diverse verantwoordelijkheden en hun coördinatie staan beschreven, aangevuld met definities en principes. De baselinebenadering, classificatie, controle en rapportage worden uitgelegd.
B. **De algemene uitvoeringsrichtlijnen**, met het tactisch kader beveiliging. De organisatie van beveiliging is weergeven met het beeld van de daarvoor benodigde rollen en functies. Verder wordt aandacht besteed aan risicoanalyse, het principe "pas toe of leg uit", controle, audit en rapportage. Algemene en principiële keuzes worden nader belicht. Ook zijn de hogere beveiligingsniveaus, de kruisverwijzing naar de standaarden en de *verklaring van toepasselijkheid* opgenomen.
C. **De normen**[1], waarin een aantal verplichte onderdelen voor elk bedrijfsonderdeel, in een samenhangend geheel.
   - Voor de bedrijfsonderdelen, de "business": informatie- en procesbeheer, personeels- en continuïteitsbeheer (BCM), leveranciers- en beveiligingsbeheer (vraagzijde IV-keten);
   - Voor het leveren van technisch beheer en exploitatie, (aanbodzijde IV-keten);
   - Voor het leveren van applicaties (aanbodzijde IV-keten);
   - Voor het leveren van diensten voor fysieke beveiliging;
   - Voor het leveren van diensten voor personele veiligheid.

[1] Normen bestaan uit hiërarchisch geordende doelstellingen, beheersmaatregelen en implementatierichtlijnen, conform NEN-ISO 27002.

Inhoudsopgave

Ministerie van Financiën

Handboek Beveiliging Belastingdienst

Deel A
Strategisch Kader Beveiliging

Mei 2011

A. Strategisch kader beveiliging

A.1. Het belang en doel van beveiliging

Continuïteit van de bedrijfsprocessen

Het halen van de bedrijfsdoelstellingen van de Belastingdienst is in hoge mate afhankelijk van goed functionerende informatiesystemen. Een informatiesysteem is een geheel van gegevensverzamelingen, de daarbij behorende personen, procedures, gebouwen, processen en programmatuur en de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.
Uitval van computers, netwerken, personeel of gebouwen, het in het ongerede raken van gegevensbestanden of het onbevoegd kennis nemen dan wel manipuleren van gegevens kunnen ernstige gevolgen hebben voor de continuïteit van de bedrijfsprocessen en de persoonlijke levenssfeer (privacy) van de betrokken belastingplichtigen, toeslaggerechtigden en partners van de Belastingdienst.
Indien de Belastingdienst deze risico's onvoldoende beheerst, kan het vertrouwen van burgers en bedrijven in de Belastingdienst worden geschaad. Dit beïnvloedt de bereidheid van belastingplichtigen om aan hun verplichtingen te voldoen nadelig. Verstoring van de continuïteit van de gegevensverwerking heeft een directe invloed op de kasstroom naar en van de overheid en bij de Douane tevens op het (inter)nationale handelsverkeer.

Interne, externe en technologische ontwikkelingen

De Belastingdienst heeft in zijn bedrijfsvoering niet alleen met interne ontwikkelingen te maken, maar ook met maatschappelijke en technologische factoren, die van invloed zijn op beveiliging.

A.1.1. Interne ontwikkelingen

a. Uitgaan van vertrouwen betekent een groter belang van beveiligingsbewustzijn, houding en gedrag.

b. Bewust risico's aanvaarden vereist helderheid over wat aanvaardbaar en wat onaanvaardbaar is, samen met een duidelijke verantwoordelijkheidsverdeling.

c. Klantgerichte benadering betekent onder meer integratie van processen en daardoor extra risico's door concentratie van taken en gegevens bij één of enkele medewerkers.

d. Werk is niet exclusief gebonden aan kantoor. Wisselende omgevingen vereisen dat medewerkers een goed inzicht hebben in de risico's daarvan.

e. Van-klant-tot-klantprocessen verlopen steeds vaker zonder menselijke tussenkomst, waardoor aan hoge eisen van betrouwbaarheid van informatiesystemen moet worden voldaan, ook omdat steeds grotere volumes aan gegevens in kortere tijd worden verwerkt.

A.1.2. Externe ontwikkelingen

f. Als grote uitvoeringsorganisatie spelen we een voortrekkers- en voorbeeldrol bij een aantal projecten van de e-overheid. Integratie van overheidsprocessen en samenwerking in overheidsketens vragen om organisatieonafhankelijkheid, standaardisatie van informatiebeveiliging, afstemming met ketenpartners en het afleggen van verantwoording over het naleven van beveiligingsstandaards.

g. De populariteit van sociale netwerken e.d. en de deelname van medewerkers hierin (zgn. functionele contacten met derden) vereisen een heldere definitie en begrip van "goed ambtenaarschap".

h. Het mede verantwoordelijk stellen van klanten en ketenpartners voor de betrouwbaarheid van brongegevens van Belastingdienstprocessen stelt hoge eisen aan betrouwbare, externe ontsluitingsmechanismen.

A.1.3. Technologische ontwikkelingen

i. Het gebruik van de veelzijdige en voortdurend veranderende (externe) communicatiemiddelen vraagt om continue evaluatie van risico's en de manier waarop deze middelen worden gebruikt.

j. Standaardisatie van de gegevensuitwisseling betekent een verruiming van de koppelingsmogelijkheden waardoor de risico's van onbevoegde veranderingen en kennisneming bij gegevensuitwisseling toenemen.

A.2. Beveiligingsprincipes[2]

De principes van de Belastingdienst bestaan uit bedrijfs-, sturings-, inrichtings- en beveiligingsprincipes. De laatste twee groepen bevatten de uitgangspunten voor beveiliging:

De Belastingdienst maakt bewuste keuzes op basis van aanvaardbaar risico (inrichtingsprincipe).
Op basis van risicobeheersing maken we gemotiveerde keuzes voor beveiliging met het oog op bedrijfscontinuïteit, een veilige werkomgeving en een betrouwbare informatievoorziening.

a. Beveiliging zit in het ontwerp van processen, producten, diensten en gebouwen.
Vanaf de start van het ontwerp van processen, producten, diensten en gebouwen nemen we beveiliging mee en is daarmee een integraal onderdeel van de informatievoorziening. In principe wordt niets in gebruik genomen zonder dat er aandacht aan beveiliging is besteed.

b. Beveiliging gaat uit van een basisniveau met beperkte aanvullingen.
Beveiliging definiëren we op een doelmatig generiek niveau, de baseline. Waar verhoogde risico's bestaan treffen we aanvullende maatregelen, zoals bij Vips of bijzondere opsporingsinformatie.
Op basis van aanvaardbaar risico kiezen we voor het geschikte niveau. Dit maakt beveiliging instelbaar.

[2] *Principes van de Belastingdienst*, juni 2007, geactualiseerd.

c. Beveiliging biedt toegang tot de benodigde bedrijfsmiddelen.
We autoriseren medewerkers tot het raadplegen en verwerken van die gegevens, het binnentreden van die ruimten en het gebruik van die middelen, die zij voor hun werk nodig kunnen hebben: need-to-do.

d. Beveiliging werkt vanuit het eigen beveiligingsbewustzijn.
Het uitgangspunt is het vertrouwen in de eigen medewerkers, die bedrijfsmiddelen gebruiken waarvoor ze bedoeld zijn. Ze raadplegen alleen die gegevens en gebruiken alleen die ruimten of middelen die ze nodig hebben, hoewel ze wellicht ruimere toegang hebben: need-to-know.

e. Beveiliging houden we simpel.
Duidelijke en eenvoudige opzet van beveiliging bevordert doelmatigheid, doeltreffendheid, acceptatie en beheersbaarheid.

f. Beveiliging ondersteunt het werk.
Beveiliging draagt bij aan een onverstoorde bedrijfsvoering en werpt geen onnodige belemmeringen op.

A.3. Risicobeheersing

Uitgangspunten risicomanagement

Bedrijfsvoering adresseert risicomanagement en streeft er naar dat[3]:
- het management zich bewust is van de impact van risico's op het realiseren van de bedrijfsdoelstellingen;
- risico's continu, expliciet en systematisch geïdentificeerd en geanalyseerd worden;
- risico's voortdurend gewogen worden;
- maatregelen toegesneden zijn op het handhaven van de acceptabel geachte risiconiveaus.

Doelstellingen hiërarchie

Risico's zijn altijd gekoppeld aan doelen. Een risico wordt immers gedefinieerd als de mogelijke oorzaak van het niet halen van doelen. Een belangrijk element voor adequaat risicomanagement is dan ook een heldere doelstellingenhiërarchie, waarmee duidelijk wordt welke doelstellingen moeten worden gehaald. Pas dan kun je de risico's identificeren en mitigeren.

Risicomanagement omvat volgens het Risicomodel Belastingdienst een veelheid van risico's, zoals:
- omgevingsrisico's zoals uit de politiek, wetgeving, maatschappelijke ontwikkelingen, imago, behoeften van burgers en bedrijven;
- procesrisico's zoals in logistiek en operatie, financiën, integriteit, ICT;
- informatie- en sturingsrisico's vanuit strategie, organisatie en besturing, verantwoording en rapportage en empowerment.

Positie van beveiliging

In het HBB staan beleid, beheersmaatregelen en implementatierichtlijnen uitgewerkt. Deze zijn een onderdeel van de verzameling maatregelen om bovenstaande bedrijfsrisico's te beheersen. Ook hieruit blijkt dat beveiliging een integraal onderdeel is van de gehele bedrijfsvoering, zoals eerder gesteld.

[3] *Beleidsplan Risicomanagement* v2.1, november 2008.

A.3.1. Bedreigingen voor beveiliging

Specifieke bedreigingen

Risico's (voor beveiliging) betreffen de kans dat bedreigingen zich voordoen. Inbreuken op de beveiliging van gegevens en processen houden in dat niet-geautoriseerde personen processen en functies kunnen activeren of toevoegen, waardoor ze gegevens kunnen raadplegen, muteren, toevoegen of vernietigen. Verder kunnen infrastructurele voorzieningen buiten gebruik worden gesteld door personen, technisch falen en door "natuurlijke" bedreigingen zoals storm en blikseminslag.

Bedreigingen worden veroorzaakt door:

- personen (derden en eigen medewerkers, al dan niet opzettelijk), die verantwoordelijk zijn voor fouten, diefstal, fraude, staking, sabotage, afluisteren en verbale of fysieke agressie;
- technisch falen, veroorzaakt door bijvoorbeeld brand, water- en weersoverlast, virussen, apparatuur- en softwarestoringen.

De Belastingdienst houdt in het beveiligingsbeleid geen rekening met extreme bedreigingen zoals gewapende conflicten, daden van terreur, atoomkernreacties en aardbevingen. De processen van de Belastingdienst worden niet gerekend tot de vitale infrastructuur van Nederland[4].

A.3.2. Beveiligingsbewustzijn

Bevorderen beveiligings-bewustzijn

Beveiliging kan zeker niet alleen rusten op procedures en techniek. Beveiliging is vooral ook een kwestie van mentaliteit van medewerkers, die techniek of procedures bewust of onbewust zouden kunnen omzeilen. Het gedrag van medewerkers is sterk medebepalend voor de beheersing van de risico's. Om deze reden kiest de Belastingdienst voor een structurele en periodieke voorlichting aan zijn medewerkers. Het lijnmanagement is verantwoordelijk voor het stelselmatig bevorderen van het beveiligingsbewustzijn.

A.3.3. Basisniveau beveiliging: risicoanalyse

Standaards en best practices

Voor zover beveiligingsrisico's algemeen van aard zijn, d.w.z. niet specifiek zijn voor de Belastingdienst, spelen de standaards en best practices, die mede als referentie gelden voor dit handboek, hierop voldoende in. Uit de combinatie van de bestaande kaders wordt het basisniveau beveiliging afgeleid.

Basisniveau Beveiliging

Figuur 1: Afleiden basisniveau beveiliging

[4] Rapport *Bescherming vitale infrastructuur*, paragraaf 2.7, BZK september 2005 / NAVI.

Toelichting bij de figuur:

- De belangrijkste wet- en regelgeving is: de Ambtenarenwet en het Algemeen Rijksambtenarenreglement (ARAR), het Reglement Personeelsvoorschriften Belastingdienst (RPVB), de Algemene wet bestuursrecht (AWB), de Wet Computercriminaliteit (WCC), de Wet Bescherming Persoonsgegevens (WBP), het Besluit Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR), het Besluit Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie 2004 (VIR-BI), te vervangen door het VIR – Gerubriceerde Informatie (VIR-GI), het Besluit Beveiligingsvoorschrift Rijksdienst 2005, de Archiefwet en de Arbowet.
- Als standaarden en best practices worden gehanteerd: NEN-ISO 27001 Management Systemen voor Informatiebeveiliging en NEN-ISO 27002 Code voor Informatiebeveiliging, die zijn voorgeschreven onder het regime "pas toe of leg uit" door het College Standaardisatie voor de e-overheid. In dat kader zijn eveneens van toepassing de afgeleide principes voor Sturing en verantwoordelijkheid, respectievelijk Betrouwbaarheid van de Nederlandse Overheids Referentie Architectuur (NORA) versie 3.0 en het dossier Informatiebeveiliging. Voor Bedrijfscontinuïteit is de BS 25999 Specification for Business Continuity Management als meest gebruikte standaard van toepassing. Deze standaard is iets uitgebreider en praktischer dan hoofdstuk 14 van NEN-ISO 27002.
- De Baseline Informatiebeveiliging Rijksdienst (BIR) is een informatiebeveiligingsnormenkader dat door het ICCIO wordt vastgesteld[5] voor de Rijksdienst.
- Contractuele eisen hebben betrekking op afspraken gemaakt met ketenpartners. Als deze de eigen Belastingdienstuitgangspunten overstijgen, worden ze in het handboek aangevuld.

A.3.4. Basisniveau beveiliging: classificatie

Hoog basisniveau van beveiliging

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. Voordeel hiervan is ook dat het basisniveau beveiliging met generieke normen kan worden ingevuld. Dit vereenvoudigt het beheer en beperkt de kosten.

Bijzondere informatie

Bij de Belastingdienst wordt in de regel[6] geen bijzondere informatie volgens VIR-BI danwel VIR-GI gegenereerd. Voor zover de Belastingdienst 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.

. . . . . .

[5] Nog niet formeel.

[6] Uitzonderingen bestaan bijvoorbeeld bij gegevensverwerking door de FIOD.

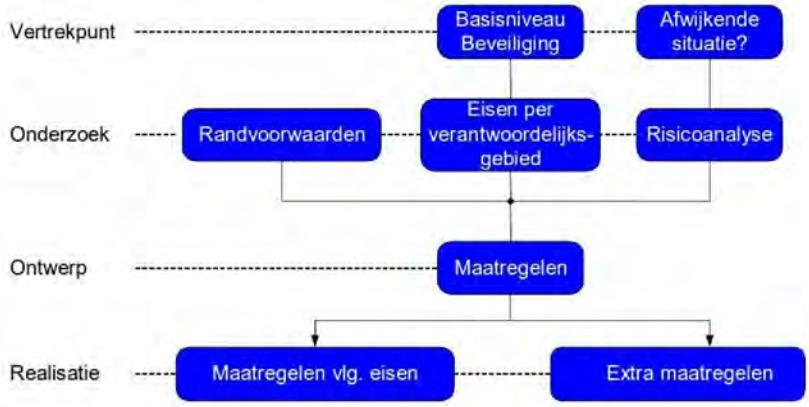
Vertrouwensfuncties

In de Belastingdienst zijn vertrouwensfuncties aan te wijzen. Het gaat om functies waarin het noodzakelijk is te werken met staatsgeheimen, waarin door integriteitsaantastingen de nationale veiligheid in het geding kan zijn of functies die van vitaal belang zijn voor de instandhouding van het maatschappelijk leven[7].
Daarnaast worden veiligheidsonderzoeken ingesteld indien de samenwerking met externe partners dit vereist.

A.3.5. Basisniveau beveiliging: het treffen van maatregelen

Cyclisch onderhoud

Op basis van de bedrijfsdoelstellingen en risico's wordt op cyclische wijze onderhoud gepleegd aan de bestaande handboeken, die invulling geven aan het begrip 'basisniveau beveiliging'. Ook komen risico's aan de orde bij het treffen van maatregelen per verantwoordelijkheidsgebied.



Figuur 2: Onderhoud maatregelen

Toelichting bij de figuur:

- Voor het merendeel van de verantwoordelijkheidsgebieden worden de maatregelen getroffen volgens het basisniveau. Daarbij is het van belang om vooral bij vernieuwingen en onderhoud van verantwoordelijkheidsgebieden van beveiliging vast te stellen of er sprake is van afwijkende situaties, die risico's met zich brengen die onvoldoende in het basisniveau zijn inbegrepen. Afwijkende situaties bij informatiesystemen kunnen onder meer betrekking hebben op hogere beschikbaarheidseisen, anders dan standaard gebruik van bestaande technologie, toepassing van nieuwe technologie, gegevens met een bijzonder belang en conversieproblematiek.
- Er zijn meer factoren op grond waarvan er in specifieke situaties afgeweken kan worden van de implementatierichtlijnen: te hoge kosten, onvoldoende haalbaarheid, de mate van effectiviteit in de specifieke situatie, de ouderdom van het gebouw of informatiesysteem etc. Die factoren worden hier samengevat onder het begrip "randvoorwaarden".
- Verantwoordelijkheidsgebieden corresponderen met de onderdelen van dit handboek en de indeling van de normen.

[7] De Belastingdienst sluit aan bij de *Leidraad aanwijzing vertrouwensfuncties 2011*, AIVD.

A.4. Organisatie van beveiliging

Beveiliging is als onderdeel van integraal management en bedrijfsvoering een verantwoordelijkheid van het lijnmanagement op de diverse niveaus in de organisatie.

Verantwoordelijkheids-verdeling

Op het hoogste niveau binnen de Belastingdienst geldt de volgende verdeling van beveiligingsverantwoordelijkheden:

- de eindverantwoordelijkheid ligt bij de Chief Security Officer (CSO), alsook de verantwoordelijkheid voor bedrijfscontinuïteit;
- de verantwoordelijkheid voor personele veiligheid en integriteit bij de Chief Personnel Officer (CPO), het concernpersoneelsbeleid;
- de verantwoordelijkheid voor informatiebeveiliging bij de Chief Information Officer (CIO);
- de verantwoordelijkheid voor fysieke beveiliging bij het verantwoordelijke MT-lid van de Facilitaire Dienst.

A.4.1. Strategisch beveiligingsoverleg (SBO)

In het SBO vindt afstemming plaats tussen de CSO en de verantwoordelijken voor de drie aspectgebieden. Het SBO bepaalt het beleid en bespreekt de (jaarlijkse) rapportages van de bedrijfsonderdelen. De CSO stemt af met de beveiligingsambtenaar van het Ministerie van Financiën en communiceert in de lijn via het overleg van de Chief Financial Officers (CFO's). Jaarlijks worden door het SBO met de RAD afspraken gemaakt over de thema's waarover gerapporteerd of waarop gecertificeerd dient te worden en waarop een (eventuele) externe audit op zal worden uitgevoerd om extra zekerheid te verkrijgen over de implementatie van beveiligingsrichtlijnen.

A.4.2. Tactisch beveiligingsoverleg (TBO)

Het TBO is een adviesorgaan voor 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 het respectievelijke bedrijfsonderdeel. De deelnemers zijn vertegenwoordigers van alle bedrijfsonderdelen. Het TBO dient voor de afstemming tussen het strategisch niveau en de eenheden.

A.4.3. Clusters en eenheden

Het lijnmanagement op de diverse niveaus wordt ondersteund door eigen beveiligingsfunctionarissen zoals de beleidsadviseurs beveiliging, meestal bij bedrijfsvoering, maar bij de IV-keten op diverse plaatsen in de organisatie. Vanuit deze functionarissen wordt de vertegenwoordiging in clusters en TBO ingevuld. Op het operationele niveau vinden diverse vormen van afstemming plaats.

A.4.4. Beveiligingsbeheersingscyclus

Het VIR geeft de beveiligingsbeheersingscyclus op deze wijze weer:

Proces voor risicobeheersing

Figuur 3: Beheersingscyclus

De betrouwbaarheidseisen (hier verder beveiligingseisen genoemd) komen tot uitdrukking in de doelstellingen en implementatierichtlijnen zoals deze in dit handboek zijn uitgewerkt.
De feitelijke maatregelen worden op basis van de normen in dit handboek ontworpen. Voor geautomatiseerde systemen bijvoorbeeld door informatiemanagement en procesinrichting. De normen vormen tevens onderdeel van de in- en externe controle. Leemten, die bij controles zijn vastgesteld, geven aanleiding tot het aanpassen van de feitelijke maatregelen. Incidentrapportage, uitzonderingsrapportage, uitkomsten van de controles en veranderde in- en externe omgevingsfactoren worden als input gebruikt voor evaluatie en bijstelling van de beveiligingseisen.
Over de check- en actfase wordt teruggerapporteerd aan de Chief Security Officer. De beheersingscyclus speelt zich feitelijk af op zowel het strategische, tactische als operationele niveau van de Belastingdienst.

De verantwoordelijkheden voor het lijnmanagement op het hoogste niveau zijn als volgt:

Plan: Beveiligingseisen

- visievorming op de betekenis van beveiliging door voortdurende beeldvorming over risico's en oplossingsrichtingen voor maatregelen passend bij het Belastingdienstbeleid;
- vaststellen doelen voor beveiliging en beleid om die doelen te bereiken;
- toewijzen van de beveiligingsverantwoordelijkheden voor interne en externe ketens van informatiesystemen aan lijnmanagers.

Do: Treffen maatregelen

- goedkeuren uitvoeringsrichtlijnen;
- bijdragen aan voorlichtings-, bewustwordings- en opleidingsprogramma's voor beveiliging;
- besluitvorming over belangrijke afwijkingen van normen en accepteren restrisico's.

Check: Controle

- het voeren van de centrale regie bij geven van periodieke en incidentele opdrachten tot het verrichten van interne onderzoeken en (externe) audits;
- beoordelen van interne en externe (audit)rapportages over beveiliging en toezien op de naleving van afspraken over oplossing van leemten.

Act: Evaluatie en aanpassen

- beoordelen ontwikkelingen in de maatschappij en de relevante omgeving voor de Belastingdienst;

- beoordelen van incidentrapportage;
- evalueren resultaten checkfase;
- geven van opdrachten tot bijstelling van visie en beleid en aanpassing van uitvoeringsrichtlijnen op basis van evaluaties.

A.5. Kosten

Kosten als onderdeel van investeringsbeslissingen

Inherent aan het uitgangspunt dat beveiliging een integrale management-verantwoordelijkheid is, komen de kosten van beveiliging ten laste van de budgetten van de verantwoordelijke lijnmanagers. De financiering geschiedt daarmee via de reguliere budgetcyclus van de Belastingdienst. Kosten van fysieke beveiliging zijn een apart onderdeel van de Huisvestingsnota.

A.6. Planning- en controlcyclus

Prestatie-indicatoren: meten via controle

De kwaliteit van de bedrijfsvoering wordt geborgd door te werken volgens de Planning en Control cyclus. Dit is de jaarlijkse terugkerende beleids-, begrotings- en verantwoordingscyclus waarbinnen alle relevante bedrijfsvoeringaspecten in samenhang een plaats hebben. De interne sturing maakt daarbij gebruik van SMART geformuleerde prestatie-indicatoren. Om tot een evenwichtig, samenhangend en afdoend stelsel van beveiligingsmaatregelen te komen, wordt beveiliging geïncorporeerd in die cyclus inclusief prestatie-indicatoren. De prestatie-indicatoren voor beveiliging zijn de beheersmaatregelen van dit handboek. Het meten geschiedt via in- en externe controle.

In control statement

Over deze cyclus wordt onder meer ten behoeve van ketenpartners, burgers en bedrijven verantwoording afgelegd in een *in control statement* in het jaarverslag en uitzonderingsrapportage. Hierbij verklaart het management van de Belastingdienst dat de interne risicobeheersings- en controlesystemen adequaat en effectief zijn.

Gebruikte afkortingen

AIVD	Algemene Inlichtingen- en Veiligheidsdienst (BZK)
BCM	Business continuity management, bedrijfscontinuïteitsbeheer
BVA	Beveiligingsambtenaar
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CAO	Centrum voor Applicatieontwikkeling en -onderhoud
CFD	Centrum voor Facilitaire Dienstverlening
CFO	Chief Financial Officer
CIE	Centrum voor Infrastructuur en Exploitatie
CIO	Chief Information Officer
CPO	Chief Personnel Officer
CSO	Chief Security Officer
DG	Directeur-Generaal
FIOD	Fiscale Inlichtingen- en Opsporingsdienst
HBB	Handboek Beveiliging Belastingdienst
IB	Informatiebeveiliging
ICCIO	Interdepartementale Commissie Chief Information Officers
IV	Informatievoorziening
FB	Fysieke beveiliging
MvF	Ministerie van Financiën
NAVI	Nationaal Adviescentrum Vitale Infrastructuur
PV&I	Personele veiligheid & integriteit
PZ	Personeelszaken
RAD	Rijksauditdienst
SBO	Strategisch beveiligingsoverleg
SMART	Specifiek, meetbaar, acceptabel, realistisch en tijdgebonden
TBO	Tactisch beveiligingsoverleg

Handleiding

Van herinneringsbrief tot ambtshalve aanslag Vpb

Applicatie AH-VPB

Vanuit de Landelijke Regie Vpb en Procesadoptie aanslagbelastingen (Vpb), inmiddels genaamd Domein aanslagbelastingen (Vpb), kwam begin 2008 de wens om een landelijke applicatie m.b.t. de ambtshalve aanslagen te bouwen met als doel om enerzijds het ITO-proces te ondersteunen door het genereren van voorstellen m.b.t. de hoogte van de belastbare winsten en anderzijds om zoveel mogelijk ambtshalve aanslagen 'automatisch' af te handelen.

In februari 2008 is een start gemaakt met het landelijke project AH-VPB. In samenwerking met Pré-SOS (onderdeel van B/CPP) is toen begonnen met het uitwerken van de ideeën. De opzet van Pré-SOS is om binnen 12 weken een werkbare applicatie af te leveren.

Door wat tegenslag met betrekking tot met name de datalevering is pas laat in 2008 de ontworpen applicatie tot een goed einde gekomen. Dit heeft geresulteerd in een applicatie waarbij op basis van een aantal criteria (rekenregels, zie bijlage 1) voorstellen voor de belastbare winsten (en belastbare bedragen) worden gegenereerd. Daarnaast wordt gekeken of voor de op te leggen ambtshalve aanslagen aan voorgedefinieerde uitworpcriteria (bijlage 2) wordt voldaan. Zo ja, dan vindt uitworp plaats en krijgen de eenheden in pdf-formaat vooringevulde 'AH-kaarten' (bijlage 3) aangeleverd. Als er geen sprake is van enige vorm van uitworp, dan zal de aanslag 'automatisch' worden opgelegd, dus zonder tussenkomst van de eenheden (bijlage 4).

Bij de ontwikkeling is zo veel mogelijk aangesloten bij de gebruikerswensen en ideeën die er waren. Door deze manier van werken is echter geen ruimte meer voor nadere gebruikerswensen. Alleen als sprake is van evidente fouten zal aanpassing van de applicatie nog kunnen plaatsvinden.

De gegevens die door de applicatie worden gegenereerd, zullen tevens in een archief worden geplaatst om op een later moment (bijvoorbeeld: bezwaar- en/of beroepsfase) de onderbouwing voor de bepaling van de hoogte van de aanslag te kunnen raadplegen. Dit archief is gebouwd in een web-applicatie. Deze applicatie is raadpleegbaar via de volgende hyperlink: http://10.25.50.246/webahvpb/main.aspx.
Bij het opstarten van deze applicatie wordt om een userid en wachtwoord gevraagd. In beide velden dient u 'ahvpb' in te toetsen.

Voorbeeldschermen van deze webapplicatie treft u als bijlage 6 aan.

Oude situatie

1. Aanmaning

In EVBN vindt u in ieder boekingstijdvak de rubriek *Geplande binnenkomst dd*. Dit houdt in dat uiterlijk deze datum het biljet binnengeboekt moet zijn. Is het aangiftebiljet niet op de datum van de 'geplande binnenkomst' ingestuurd en binnengeboekt dan wordt een aanmaning (VPB 28) geselecteerd (met het programma V36039) en aan belastingplichtige verzonden.

2 Aanmaken 'AH-kaarten'

In de regel wordt na het verstrijken van de aanmaningstermijn (zie hiervoor in het betreffende boekingstijdvak de rubriek Uiterste datum na aanmaning) het programma V53039 gedraaid.

In het betreffende boekingstijdvak wordt voor de groep belastingplichtigen die geen aangifte hebben gedaan, automatisch de indicator bij de rubriek *Ambtshalve aangifte* op 'J' gezet. Het ambtshalve biljet wordt aangemaakt met daarop een balk die ingevuld kan worden.
Vervolgens wordt door de heffer VPB op basis van historische VPB-gegevens en uit IKB een ambtshalve definitieve aanslag vastgesteld. Hierbij bestaat ook de keuze tot het opleggen van een verzuimboete of een vergrijpboete.

Nadelen van deze oude situatie:
-Er worden ten onrechte zeer veel AH-kaarten aangemaakt
-Heffer wordt niet voorzien van 'voorgekookte' informatie
-Heffer moet zelfstandig verzuimboete bepalen
-Ambtshalve aanslagen worden regelmatig te lang aangehouden
-Geen eenheid van beleid en uitvoering

Nieuwe situatie

1. Herinnering (vanaf boekjaren 2008)
Op het moment dat de geplande datum binnenkomst is verstreken, wordt door F.A.A. (Fiscale Afspraken Aanslag) een standaard herinneringsbrief (bijlage 5) gestuurd naar belastingplichtige waarin wordt aangegeven dat nog geen aangifte vennootschapsbelasting is gedaan. Het bestand waarin staat welke belastingplichtigen nog géén aangifte hebben gedaan, wordt uitgezet op de regiokantoren alwaar men als voorwerk kan nagaan wat er met betreffende belastingplichtigen aan de hand is (mogelijk in liquidatie, onjuist adres, etc.).

2. Aanmaning
In EVBN vindt u in ieder boekingstijdvak de rubriek *Geplande binnenkomst dd*. Dit houdt in dat uiterlijk deze datum aangifte moet zijn gedaan. Is op de datum van de 'geplande binnenkomst' geen aangifte gedaan dan wordt een maand na de herinnering (zie onder 1. hierboven) een aanmaning (VPB 28) gegenereerd (met het programma V36039) en aan belastingplichtige verzonden door B/CA. Vanaf de boekjaren 2008 zal het versturen van aanmaningen geschieden door F.A.A., dit zal dan plaatsvinden ongeveer 1 maand na het versturen van de herinneringsbrieven.

3. Jaren die in aanmerking komen - als ambtshalve jaren aanmerken
In de regel wordt na het verstrijken van de aanmaningstermijn (zie hiervoor in het betreffende boekingstijdvak de rubriek Uiterste datum na aanmaning) het programma V53039 gedraaid.

In het betreffende boekingstijdvak wordt voor de groep belastingplichtigen die geen aangifte hebben gedaan, automatisch de indicator bij de rubriek *Ambtshalve aangifte* op 'J' gezet. Door het Vpb-systeem wordt het ambtshalve biljet aangemaakt met daarop een balk die ingevuld kan worden (in PDF). Deze balk hoeft niet meer te worden afgedrukt.

Door het programma V53039 wordt een bestand aangemaakt, geheten 'AANLYST'. Hierin staan de belastingplichtigen die een ambtshalve aanslag moeten krijgen. Dit bestand wordt als invoerbestand aangemerkt voor het draaien van een zestal queries Vpb.

Vervolgens worden deze queries tezamen met gegevens uit RAM (betreffende omzet- en loonsomgegevens) aangeboden aan de applicatie AHVPB.

Binnen de applicatie vinden allerlei handelingen plaats en uiteindelijk wordt op basis van diverse criteria (de rekenregels, zie bijlage 1) een voorstel voor het opleggen van de ambtshalve aanslag gegenereerd (zowel belastbare winst als belastbaar bedrag, alsmede verzuimboete en tariefcode).

Tevens bekijkt de applicatie of sprake is van één of meer uitworpredenen (bijlage 2).

Als er géén sprake is van minimaal één uitworpreden, dan zal de ambtshalve aanslag 'automatisch' worden opgelegd (vooralsnog door Rijnmond voor het gehele land, maar de bedoeling is dat een koppeling zal komen tussen EVBN en de applicatie AHVPB) (bijlage 4). Deze posten worden afgedaan op sapnummer P-gv. Dit betekent dat op het lokale lijstwerk aanslagpartijen AH van de eenheden de USERID van deze medewerker P-gv. is te zien wat inhoudt dat de AH automatisch is opgelegd. Deze posten krijgen als 'soort post' indicatie AO of AB mee (administratief onbelast/belast).

Is er wel sprake van een uitworpreden, dan zal per eenheid een verzameling vooringevulde 'AH-kaarten' in pdf-formaat (bijlage 3) worden aangemaakt. Op het moment dat deze kaarten zijn aangemaakt, ontvangen de regiokantoren een mailbericht in de postbus van het lijstwerk Vpb. Daarin zal worden aangegeven dat er mogelijk AH-kaarten klaar staan voor verdere verwerking (deze pdf-files staan in een centrale map alwaar op eenheidscode en datum de bestanden zijn te vinden, bijvoorbeeld voor ZGO Rotterdam is dit **uitworp142 (15-01-2009).pdf**).
Deze posten dienen te worden afgedaan met de 'soort post' indicatie IO of IB (traditioneel onbelast/belast).

Voordelen van deze nieuwe situatie:
-Door voorwerk bij herinneringsbrieven minder aanmaak 'AH-kaarten'
-Eenheid van beleid en uitvoering
-Deel automatische verwerking, dus tijdsbesparing
-Deel ambtshalve aanslagen worden niet onnodig lang aangehouden
-Vooringevulde 'AH-kaarten', ook hier tijdsbesparing
-Verzuimboete wordt automatisch bepaald
-Te verrekenen verliezen worden automatisch berekend, rekening houdend met de tariefcodes

Draaiboek cyclus van herinnering tot AH-aanslag

Voor de stroom op te leggen ambtshalve aanslagen en het vooraf beoordelen op juistheid van de gegevens om onnodig extra werk te voorkomen (op voorhand bestandszuivering, signalering curatorposten etc), is het idee geboren om de volgende cyclus aan te houden.

Herinneringsbrief

Voor de boekjaren 2007 en ouder zal géén herinneringsbrief worden gestuurd door B/CA of F.A.A..
(Als de regiokantoren zelf herinneringsbrieven willen sturen, moet wel rekening worden gehouden met het feit dat de aanmaningen voor deze boekjaren voor de meeste belastingplichtigen worden gestuurd in de maand volgend op de maand waarin de geplande binnenkomst eindigt.)

Voor de boekjaren 2008 zal (door F.A.A. en pas vanaf juli 2009) **maandelijks** een herinneringsbrief worden gestuurd en wordt aan de regiokantoren een bestand verstrekt met de belastingplichtigen aan wie deze brieven zijn gestuurd
(In EVBN zal niet zichtbaar zijn dat een herinneringsbrief is gestuurd, daar is namelijk geen veld voor aanwezig).
Dit bestand zal dan beoordeeld dienen te worden zoals beschreven in het hoofdstuk 'Ambtshalve aanslagen Vpb' in het 'Rapport doorlichting administratieve processen', opgemaakt door Rijnmond (enkele passages zijn te vinden in bijlage 7).

Aanmaning

Voor de boekjaren 2007 en ouder zullen **maandelijks** aanmaningen worden verstuurd (door B/CA).

Voor de boekjaren 2008 zullen **maandelijks** aanmaningen worden verstuurd (door F.A.A. en pas vanaf juli 2009). Deze aanmaningen zullen volgen circa 1 maand na het versturen van de herinneringsbrieven.

AH-programma

In beginsel draait B/CA het programma V53039 (programma die de voor een ambtshalve aanslag in aanmerking komende posten in het jaarscherm het veld AH op 'J' zet) maandelijks en wel op de 2e donderdag van de maand (tenzij sprake is van 5 donderdagen in een maand, dan de 3e donderdag van de maand).
Het door B/CA draaien van de queries Vpb op de output van voornoemd programma dient direct na voornoemd programma plaats te vinden (dus op de vrijdag erna).
Het draaien van de **applicatie AH-VPB** (door Rijnmond) geschiedt daar weer na.

In afwijking van de maandelijkse cyclus is afgesproken dat het programma V53039 draait op de volgende data, resp.:

-2e / 3e week februari
-2e / 3e week juli
-2e / 3e week september
-2e / 3e week december

Voor de automatisch op te leggen aanslagen, zal hiervan de dagtekening van de aanslag ongeveer zijn in, resp.:

-maart
-augustus
-oktober
-januari

Tariefcode, verliesverrekening en verzuimboete

In het voortraject bij de bouw van deze applicatie is overleg gevoerd met de afdeling Formeel Recht van B/CPP.
Op basis hiervan zijn de volgende bepalingen meegenomen in de ontwikkeling van de applicatie.

Tariefcode
De applicatie bepaalt op basis van de tariefcode van voorgaand jaar de tariefcode voor het ambtshalve jaar.
Mocht voorgaand jaar niet geregeld zijn, dan zal op de 'AH-kaart' bij de tariefcode een '?' staan.

Het bepalen van de tariefcode heeft namelijk ook gevolgen voor het volgende onderdeel, namelijk de verliesverrekening.

Verliesverrekening
Eventueel aanwezige te verrekenen verliezen worden verrekend bij het opleggen van de ambtshalve aanslag.
De applicatie houdt op basis van de tariefcode van de afzonderlijke verliesjaren en de tariefcode van het jaar van de op te leggen ambtshalve aanslag rekening met het feit of wel/niet verrekend kan worden.

Door de applicatie wordt op de 'AH-kaart' onderaan bij het voorstel aangegeven welk bedrag op basis van de tariefcode kan worden verrekend.

Verzuimboete
Door de applicatie wordt voor de boekjaren die aanvangen voor 1 januari 2008 de verzuimboete bepaald. Dit gebeurt door in voorgaande vijf jaren na te gaan hoeveel keer een verzuimboete is opgelegd.

Mocht bepaling van de verzuimboetereeks niet mogelijk zijn, omdat voorgaand jaar niet geregeld is, dan zal op de 'AH-kaart' bij de verzuimboete een '?' staan.

Voor de boekjaren die aanvangen op of na 1 januari 2008 geldt het nieuwe boetebesluit en is de verzuimenreeks niet meer van toepassing. De applicatie zal voor deze boekjaren bij het veld "Code boete" i.p.v. de verzuimenreeks een 'J' zetten op zowel het uitworpformulier als in het bestand met automatisch op te leggen aanslagen. Er wordt uitgegaan van de standaardwaarde van € 567.

Voor deze boekjaren die aanvangen op of na 1 januari 2008 houdt het tevens in dat door de applicatie niet wordt gekeken hoe vaak belastingplichtige in verzuim is. Dit heeft tot gevolg dat niet wordt beoordeeld of sprake is van het stelselmatig niet of te laat aangifte doen (nieuwe BBBB, § 21-6), op basis waarvan wellicht een hogere verzuimboete (tot max. € 1.134) kan worden opgelegd. Of dit terecht is, zal nader moeten worden beoordeeld door de afdeling Formeel Recht van B/CPP.

Bijlage 1 Rekenregels

De applicatie AH-VPB bepaalt op 8 manieren een voorstel voor de belastbare winst van de op te leggen ambtshalve aanslag. Van de bevonden uitkomsten wordt de hoogste waarde gebruikt om de ambtshalve aanslag op te leggen.

De rekenregels die door de applicatie worden gehanteerd, zijn als volgt:

1. **Voorlopige aanslaggegevens jaar AH**
   Vanuit EVBN worden de aanslaggegevens van de voorlopige aanslagen en de verminderingen op de voorlopige aanslagen van het AH-jaar opgehaald en wordt de laatst bepaalde waarde door de applicatie uitgelezen.

2. **Aanslaggegevens navorderingen voorgaand jaar**
   Vanuit EVBN worden de aanslaggegevens van de navorderingsaanslagen en de verminderingen op de navorderingsaanslagen van het voorgaande jaar opgehaald en wordt de laatst bepaalde waarde door de applicatie uitgelezen.

3. **Aanslaggegevens definitieve aanslagen voorgaand jaar**
   Vanuit EVBN worden de aanslaggegevens van de definitieve aanslagen en de verminderingen op de definitieve aanslagen van het voorgaande jaar opgehaald en wordt de laatst bepaalde waarde door de applicatie uitgelezen.

4. **Belastbare winst op basis van omzetgegevens branche in jaar-AH**
   Vanuit RAM (Risico Analyse Model) worden per finr gegevens aangeleverd met betrekking tot de totale omzet en totale aangegeven/vastgestelde belastbare winst per jaar van alle posten die tot dezelfde branche behoren.
   Op basis van deze informatie wordt de factor totale omzet/totale belastbare winst losgelaten op de omzet van de betreffende vennootschap, waardoor een belastbare winst tot stand komt (zie onderstaand voorbeeld).

5. **Belastbare winst op basis van loonsomgegevens branche in jaar-AH**
   Vanuit RAM (Risico Analyse Model) worden per finr gegevens aangeleverd met betrekking tot de totale loonsom en totale aangegeven/vastgestelde belastbare winst per jaar van alle posten die tot dezelfde branche behoren.
   Op basis van deze informatie wordt de factor totale loonsom/totale belastbare winst losgelaten op de loonsom van de betreffende vennootschap, waardoor een belastbare winst tot stand komt (zie onderstaand voorbeeld).

Rekenvoorbeeld voor de rekenregels 4 en 5

Totaal aangegeven/vastgestelde belastbare winsten branche in jaar-AH *Totale omzet cq loonsom branche in jaar-AH*	= =	*15.000.000* *60.000.000*
Omzet cq loonsom van de belastingplichtige in jaar-AH	=	*320.000*
OB-factor cq LB-factor is 15.000.000 : 60.000.000	=	*0,25*
Voorstel: OB-factor cq LB-factor x omzet cq loonsom bel.p. = 0,25 x 320.000	=	***80.000***

6. **Belastbare winst op basis van omzetgegevens vennootschap in voorgaande 3 jaren**
   Per finr wordt per jaar een factor bepaald aan de hand van de omzet en de aangegeven/vastgestelde belastbare winst van dat individuele finr.
   Vervolgens worden de uitkomsten opgeteld en gedeeld door het aantal keer dat een waarde is gevonden, hierdoor ontstaat een factor. Deze factor wordt vervolgens losgelaten op de omzet van de vennootschap in het jaar van de ambtshalve aanslag en komt een belastbare winst tot stand (zie onderstaand voorbeeld).

7. Belastbare winst op basis van loonsomgegevens vennootschap in voorgaande 3 jaren

Per finr wordt per jaar een factor bepaald aan de hand van de loonsom en de aangegeven/vastgestelde belastbare winst.
Vervolgens worden de uitkomsten opgeteld en gedeeld door het aantal keer dat een waarde is gevonden, hierdoor ontstaat een factor. Deze factor wordt vervolgens losgelaten op de loonsom van de vennootschap in het jaar van de ambtshalve aanslag en komt een belastbare winst tot stand (zie onderstaand voorbeeld).

Rekenvoorbeeld voor de rekenregels 6 en 7

Aangegeven/vastgestelde belastbare winst bel.pl. in jaar-AH -3		=	*1.500.000*
Aangegeven/vastgestelde belastbare winst bel.pl. in jaar-AH -2		=	*1.800.000*
Aangegeven/vastgestelde belastbare winst bel.pl. in jaar-AH -1		=	*1.100.000*
Omzet cq loonsom van de belastingplichtige in jaar-AH -3		=	*7.500.000*
Omzet cq loonsom van de belastingplichtige in jaar-AH -2		=	*7.500.000*
Omzet cq loonsom van de belastingplichtige in jaar-AH -1		=	*5.000.000*
Omzet cq loonsom van de belastingplichtige in jaar-AH		=	*6.250.000*
OB-factor cq LB-factor in jaar-AH -3 is 1.500.000 : 7.500.000 =	*0,20*		
OB-factor cq LB-factor in jaar-AH -2 is 1.800.000 : 7.500.000 =	*0,24*		
OB-factor cq LB-factor in jaar-AH -1 is 1.100.000 : 5.000.000 =	*0,22*		
Gemiddelde OB-factor cq LB-factor is	*0,66 : 3 =*		*0,22*
Voorstel: OB-factor cq LB-factor x omzet cq loonsom bel.pl. = 0,22 x 6.250.000		**=**	***1.375.000***

8. Belastbare winst op basis van vaste waarde

In de applicatie is een standaardwaarde ingegeven, die is bepaald op EUR 1.000,-
(Dit bedrag is variabel én aan te passen door de beheerders van de applicatie)
Het bedrag van EUR 1.000,- is totstandgekomen na overleg met de afdeling Formeel Recht van B/CPP).
Op deze rekenregel zal worden teruggevallen als de waarden van de vorige zeven rekenregels leiden tot een voorstel belastbare winst van minder dan EUR 1.000,-.

Na evaluatie (eind 2009) wordt gekeken of in overleg met de afdeling Formeel Recht van B/CPP dit bedrag aangepast moet worden.

Bijlage 2 Uitworpredenen

De uitworpregels die door de applicatie worden gehanteerd, zijn als volgt:

1. **Is sprake van Functionele Valuta?**
   Als in het jaar-AH sprake is van functionele valuta, dan uitworp.
   Er wordt in dit geval géén voorstel BW en BB gemaakt. De behandelaar dient zelfstandig de hoogte van de op te leggen aanslag te bepalen.
   Tekst uitworp: Er is sprake van functionele valuta

2. **Is voorgaand jaar geregeld?**
   Als voorafgaand jaar geen datum regeling heeft, dan uitworp.
   Tekst uitworp: In de voorliggende periode is geen definitieve aanslag opgelegd

3. **Is een behandelvoornemen aanwezig?**
   Als in het jaar van de ambtshalve aanslag een behandelvoornemen indicatie 'trad' in EVBN voorkomt, dan uitworp.
   Tekst uitworp: Behandelvoornemen "traditioneel" aanwezig

4. **Is sprake van vijfde verzuim?**
   Als in het jaar van de ambtshalve aanslag sprake is van een vijfde verzuim, dan uitworp.
   Voor boekjaren die aanvangen op of na 1 januari 2008 vervalt deze uitvraag, want dan is namelijk de verzuimenreeks uit het Besluit Bestuurlijke Boeten Belastingdienst (BBBB) verdwenen.
   Tekst uitworp: Code boete 5

5. **Is sprake van ZGO-post?**
   Als in het veld 'aandachtscategorie' in EVBN de waarde 'I' staat, is sprake van een ZGO-post.
   In dat geval uitworp.
   Tekst uitworp: Post betreft een zeer grote onderneming

6. **Is sprake van MGO-post?**
   Als in het veld 'aandachtscategorie' in EVBN de waarde 'II' staat, is sprake van een MGO-post.
   In dat geval uitworp.
   Tekst uitworp: Post betreft een middelgrote onderneming

Voor uitworpreden 5 en 6 geldt:
Onderdeel van het vernieuwde ambtshalve traject is dat de aandacht voor de klant naar voren gehaald wordt. Dus na verzending van de aanmaning (later ook herinnering) zou dan al contact opgenomen moeten worden met de belastingplichtige, en niet wachten tot voor de betreffende klant een 'AH-kaart' wordt gemaakt. Dit betekent dat deze uitworp over enige tijd wordt uitgezet en dan dus niet mee gaat draaien als uitworp.

7. **Is sprake van eerste boekjaar?**
   Als in het jaar van de ambtshalve aanslag sprake is van het eerste boekjaar (datum oprichting ligt in periode van boekingstijdvak), dan uitworp.
   Tekst uitworp: Dit jaar is het eerste boekjaar

8. **Is sprake van einde belastingplicht?**
   Als in het jaar van de ambtshalve aanslag sprake is van einde belastingplicht (veld '*niet meer bel.pl. m.i.v.*' is gevuld), dan uitworp.
   Tekst uitworp: Niet meer belastingplichtig m.i.v. x-x-xxxx, code x

   De code is al volgt te verklaren:

1	=	ontbinding
2	=	fiscale eenheid
3	=	dubbele opvoering
4	=	stichting / vereniging
5	=	rechtsvormwijziging
6	=	juridische fusie
7	=	juridische splitsing