Bijlage 2 Uitworpredenen (vervolg)

9. Is sprake van tariefcode 'B'?
Als in het jaar van de ambtshalve aanslag sprake is van tariefcode 'B', dan uitworp.
Tekst uitworp: Tariefcode B

10. Is sprake van een curatorpost?
Als in het jaar van de ambtshalve aanslag sprake is van een curatorpost (in het veld 'naam' in het scherm 'potloodadres' begint het veld naam met 'CUR), dan uitworp. Deze posten dienen op basis van de werkinstructie 'Curatorposten' verder behandeld te worden.
Tekst uitworp: Curatorpost

11. Is sprake van een zogenaamde VOW-post?
Als in het jaar van de ambtshalve aanslag sprake is van een VOW-post ('vertrokken, onbekend waarheen') (in het veld 'adres' komt het woord 'VOW' voor), dan uitworp.
Tekst uitworp: Vertrokken, onbekend waarheen

12. Is voorgaand jaar AH opgelegd en geen bezwaar (en geen navordering)?
Als het jaar voorafgaand aan het jaar van de ambtshalve aanslag ook ambtshalve is opgelegd en er is geen bezwaar aangetekend en ook geen navordering opgelegd, dan uitworp.

De vraag of de aanslag is betaald (koppeling met GOA/COA), is achterwege gelaten. Enerzijds omdat een koppeling met de GOA/COA niet zinvol was (i.v.m. uitfasering van deze programma's en de intrede van ETM met de onderzekerheden voor koppeling hiermee) en anderzijds omdat het in feite niet uitmaakt of belastingplichtige wel of niet betaald heeft, in beide gevallen dient onderzoek plaats te vinden.
Als belastingplichtige wel betaald heeft is dit een reden om na te gaan of de ambtshalve aanslag in voorgaand jaar te laag is geweest.
Als niet is betaald, dan is het zaak om na te gaan waarom niet (wellicht in liquidatie) en of de ontvanger de aanslag als oninbaar heeft aangemerkt.
Tekst uitworp: In voorliggende periode is een AH opgelegd waartegen geen bezwaar werd aangetekend

13. Is de voorlopige aanslag de hoogste waarde en is boekjaar ongelijk aan kalenderjaar?
Als voor het voorstel de keuze is gevallen op de waarde van de voorlopige aanslag en er is sprake van een gebroken boekjaar, dan uitworp.
deze uitworp is gekozen i.v.m. mogelijke tariefsdalingen na het opleggen van de VA waardoor sprake is van een negatieve AH incl. heffingsrente.
In eerste instantie is ook gedacht aan de situatie m.b.t. 2008 waarbij met terugwerkende kracht (!) het tarief voor de Vpb is verlaagd. Na overleg met procesadoptie en Landelijke regie is besloten, dit risico niet mee te nemen als uitworp.
Tekst uitworp: Berekende BW is gelijk aan BW VA en boekjaar is ongelijk aan kalenderjaar

14. Is sprake van het eerste jaar na ontvoeging?
Als het jaar van de ambtshalve aanslag het eerste jaar is na ontvoeging fiscale eenheid Vpb (begin boekjaar is gelijk aan datum 'ontvoegd m.i.v.'), dan uitworp.
Tekst uitworp: Betreft eerste jaar na ontvoeging, voorstel nader beoordelen

15. Staat het jaarscherm AH-jaar op naam behandelaar?
Als bij het jaar van de ambtshalve aanslag in EVBN de code van een behandelaar staat ingevuld, dan uitworp.
Tekst uitworp: Het AH-jaar is in het Vpb-systeem afgeboekt op behandelaar xxxxx (xxxxx is sapnr)

16. Is sprake van een negatieve correctie belastbaar bedrag t.o.v. VA?
Als het voorstel voor het belastbaar bedrag kleiner is dan het vastgesteld belastbaar bedrag bij de voorlopige aanslag, dan uitworp.
deze uitworp is gekozen i.v.m. negatieve AH aanslag (bijvoorbeeld: VA zonder carry forward, terwijl wel sprake is van carry forward bij AH aanslag, er is dan mogelijk sprake van teruggaaf van heffingsrente
Tekst uitworp: Belastbaar bedrag AH < Belastbaar bedrag VA (mogelijke teruggaaf heffingsrente)

Bijlage 2 Uitworpredenen (vervolg)

17. Is sprake van een voorstel BW van meer dan EUR 100.000 en is óf totale omzet óf loonsom groter dan EUR 500.000?
Als het voorstel voor de belastbare winst groter is dan EUR 100.000 en óf de omzet óf de loonsom is groter dan EUR 500.000, dan uitworp.
(Deze bedragen zijn variabel én aan te passen door de beheerders van de applicatie)
Tekst uitworp: Berekende BW > 100.000,- en omzet en/of loonsom > 500.000,- / 500.000,-

18. Is sprake van een moeder in een F.E. Vpb?
Als de belastingplichtige in het jaar van de ambtshalve aanslag een moedermaatschappij is in een fiscale eenheid Vpb (veld '*Fiscale voeging* ' is gevuld met 'MOEDER'), dan uitworp.
Tekst uitworp: Betreft MOEDER in F.E. Vpb, voorstel nader beoordelen

19. Is sprake van een voorstel BB van meer dan EUR 1.000.000?
Als het voorstel voor het belastbaar bedrag groter is dan EUR 1.000.000, dan uitworp.
(Dit bedrag is variabel én aan te passen door de beheerders van de applicatie)
Deze uitworp is toegevoegd als extra voorwaarde, omdat de kans aanwezig blijft dat een belastbaar bedrag op onjuiste gronden wordt bepaald (bijvoorbeeld als er sprake is van een onjuiste branchecode bij een klant, waardoor onjuiste waarden worden gehanteerd). Uit voorzichtigheid wordt deze 'AH-kaart' aan de eenheid aangeboden om na te gaan of de ambtshalve aanslag wel of niet op basis van het voorstel kan worden opgelegd.
Tekst uitworp: Berekende belastbaar bedrag is gelijk aan of meer dan EUR 1.000.000,-

Bijlage 3 voorbeeld 'AH-kaart'

Uitworp vaststelling definitieve AMBTSHALVE aanslag VPB

Eenheid : 150

Gegevens belastingplichtige

Boekjaar: 200601 (1-1-2006) - 200612 (31-12-2006)

Fiscaal nummer :
Team / Dossiernr :
Naam :
Adres :
Woonplaats :

KvK-nummer :

Te verr. verliezen: 0
(vóór verrekening in dit boekjaar)

Geplande datum binnenkomst : 30-4-2008 | Uiterste datum na aanmaning : 5-9-2008 | Uiterste datum dagtekening : 30-11-2010

Uitworpreden(en)

> Behandelvoornemen 'traditioneel' aanwezig
> Post betreft een middelgrote onderneming
> Het AH-jaar is in het Vpb-systeem afgeboekt op behandelaar 62366
> In voorliggende periode is een AH opgelegd waartegen geen bezwaar werd aangetekend

Voorbeeld 1

Gevonden waarden voor vaststelling BW (in euro)

> BW laatste voorlopige aanslag (jaar AH)	23.800
> BW laatste navorderingsaanslag (jaar AH - 1)	Niet gevonden
> BW definitieve aanslag (jaar AH -1)	0
> BW indien geen verdere gegevens	1.000
> BW berekening omzet * factor (jaar AH)	11.591
> BW berekening loonsom * factor (jaar AH)	36.212
> BW omzet * gemiddelde factor vorige 3 jaar	Niet gevonden
> BW loonsom * gemiddelde factor vorige 3 jaar	0

VOORSTEL

Funct. valuta	Belastbare winst	Belastbaar Bedrag	Tariefcode	Code boete
EUR	36.212	36.212	N	3
(EUR	*[12.412]*	*[12.412]*	*- correctie t.o.v. voorlopige aanslag)*	

Opmerkingen

Datum verwerking	Sapnr	Paraaf

Uitworp vaststelling definitieve AMBTSHALVE aanslag VPB

Eenheid : 150

Gegevens belastingplichtige

Boekjaar: 200601 (1-1-2006) - 200612 (31-12-2006)

Fiscaal nummer :
Team / Dossiernr :
Naam :
Adres :
Woonplaats :

KvK-nummer :

Te verr. verliezen: 4.302.947
(vóór verrekening in dit boekjaar)

Geplande datum binnenkomst : 31-3-2008 | Uiterste datum na aanmaning : 5-9-2008 | Uiterste datum dagtekening : 31-10-2010

Uitworpreden(en)

> Behandelvoornemen 'traditioneel' aanwezig
> Post betreft een middelgrote onderneming
> In voorliggende periode is een AH opgelegd waartegen geen bezwaar werd aangetekend

Voorbeeld 2

Gevonden waarden voor vaststelling BW (in euro)

> BW laatste voorlopige aanslag (jaar AH)	0
> BW laatste navorderingsaanslag (jaar AH - 1)	Niet gevonden
> BW definitieve aanslag (jaar AH -1)	100.000
> BW indien geen verdere gegevens	1.000
> BW berekening omzet * factor (jaar AH)	0
> BW berekening loonsom * factor (jaar AH)	0
> BW omzet * gemiddelde factor vorige 3 jaar	Niet gevonden
> BW loonsom * gemiddelde factor vorige 3 jaar	Niet gevonden

VOORSTEL

Funct. valuta	Belastbare winst	Belastbaar Bedrag	Tariefcode	Code boete
EUR	100.000	0	N	4
(EUR	*[100.000]*	*[0]*	*- correctie t.o.v. voorlopige aanslag)*	

Het verrekenbare verlies (o.b.v. tariefcode) voor dit jaar werd bepaald op 4.302.947

Opmerkingen

Datum verwerking	Sapnr	Paraaf

Bijlage 4 voorbeeld 'Automatisch op te leggen AH'

Automatische vaststelling definitieve AMBTSHALVE aanslag VPB Eenheid : 150

Fiscaal nummer	:	ARA	: P-gv.
Begin Boekjaar	:	Datum	: 15012009
Correctie BW	: 1000	Soort post	: AB
BW	: 1000	Tariefcode	: N
Correctie BB	: 1000	Code boete	: 1
BB	: 1000	Adm. afd.	: J

Fiscaal nummer	:	ARA	: P-gv.
Begin Boekjaar	:	Datum	: 15012009
Correctie BW	: 1000	Soort post	: AO
BW	: 1000	Tariefcode	: N
Correctie BB	: 0	Code boete	: 2
BB	: 0	Adm. afd.	: J

Fiscaal nummer	:	ARA	: P-gv.
Begin Boekjaar	:	Datum	: 15012009
Correctie BW	: 60123	Soort post	: AB
BW	: 60123	Tariefcode	: N
Correctie BB	: 60123	Code boete	: 1
BB	: 60123	Adm. afd.	: J

Fiscaal nummer	:	ARA	: P-gv.
Begin Boekjaar	:	Datum	: 15012009
Correctie BW	: 751264	Soort post	: AB
BW	: 751264	Tariefcode	: N
Correctie BB	: 751264	Code boete	: 1
BB	: 751264	Adm. afd.	: J

Fiscaal nummer	:	ARA	: P-gv.
Begin Boekjaar	:	Datum	: 15012009
Correctie BW	: 16737	Soort post	: AB
BW	: 16737	Tariefcode	: N
Correctie BB	: 16737	Code boete	: 3
BB	: 16737	Adm. afd.	: J

donderdag 15 januari 2009 (selectiedatum 14-1-2009) 1 van 80 *Belastingdienst*

Zoals reeds eerder aangegeven, worden deze 'automatisch' opgelegde aanslagen verwerkt op sapnummer P-gv. Dit sapnummer is van een medewerker van Belastingdienst Rijnmond Persoonsgegevens
Op het lijstwerk van de eenheden komen dus de aanslagpartijen AH-aanslagen te staan waarbij de USERID van deze medewerker is te zien Persoonsgegevens Dit lijstwerk zal door de eenheden zelf behandeld worden.

Als deze 'automatische' posten worden afgehandeld, krijgen ze een 'Soort post'-indicatie in EVBN van 'AO' of 'AB' (wat staat voor ➔ administratief onbelast/belast).

Mocht om welke reden dan ook een aanslag op het lijstwerk tevoorschijn komen (en dus de aanslag géén dagtekening heeft gekregen), dan dient de lokale eenheid de melding te behandelen en de aanslaggegevens opnieuw in te toetsen.
De bepaling van de hoogte van het voorstel van de belastbare winst is te vinden in het archiefbestand. 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.

Voorbeeldenschermen van deze webapplicatie treft u als bijlage 6 aan.

Bijlage 5 voorbeeldbrief Herinnering

Rijnmond
kantoor Rotterdam

Telefoon 0800 - 0543
Telefax (010) 290 00 00
Unit x
Doorkiesnummer (010) 290 00 00

> Postbus 50960 3007 BB ROTTERDAM

Geen Aangifte BV
Ambtshalvestraat 14
9999 AA AHKAARTDAM

Datum
15 februari 2009

Uw kenmerk
0000.00.000

Kenmerk
0000.00.000/2007/Herinnering

Betreft
Herinnering tot het doen van aangifte vennootschapsbelasting

Geachte heer/mevrouw,

U moet over het jaar 200701/200712 aangifte doen voor de vennootschapsbelasting.

De termijn voor de indiening van deze aangifte is op 31 januari 2009 verstreken. Misschien bent u vergeten om aangifte te doen.

Wat kunt u doen?
U wordt alsnog in de gelegenheid gesteld aangifte te doen. Deze aangifte dient uiterlijk 25 april 2009 bij ons binnen te zijn.

Mocht sprake zijn van een andere reden waarom u geen aangifte heeft gedaan, dan verzoek ik u dit, bij voorkeur schriftelijk, aan ons mede te delen.

Hoe kunt u aangifte doen?
U moet digitaal aangifte doen. U heeft van ons een gebruikersnaam en wachtwoord ontvangen voor het beveiligde gedeelte van de internetsite.

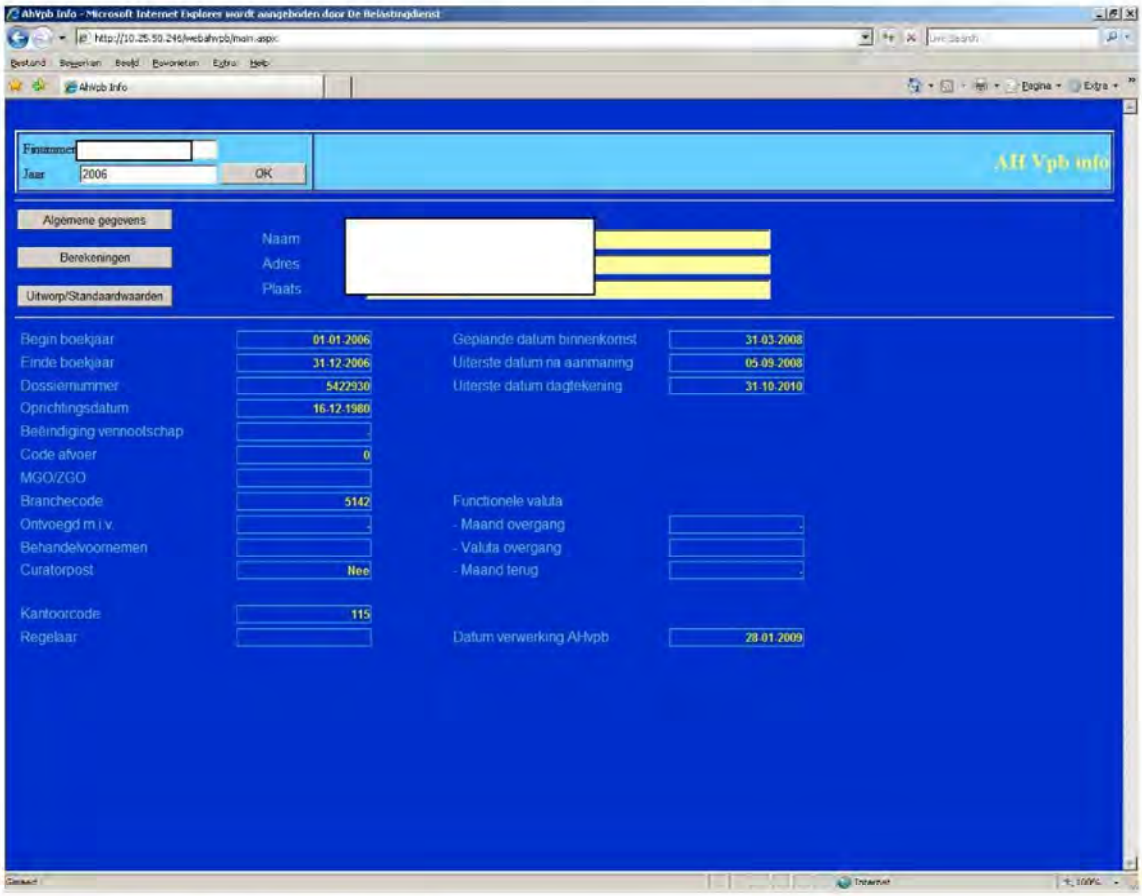
Wat gebeurt er als u niet op deze herinnering reageert?
Als u niet binnen de gestelde termijn aangifte doet, krijgt u een aanmaning. Ook krijgt u een boete als u niet of te laat op de aanmaning reageert.

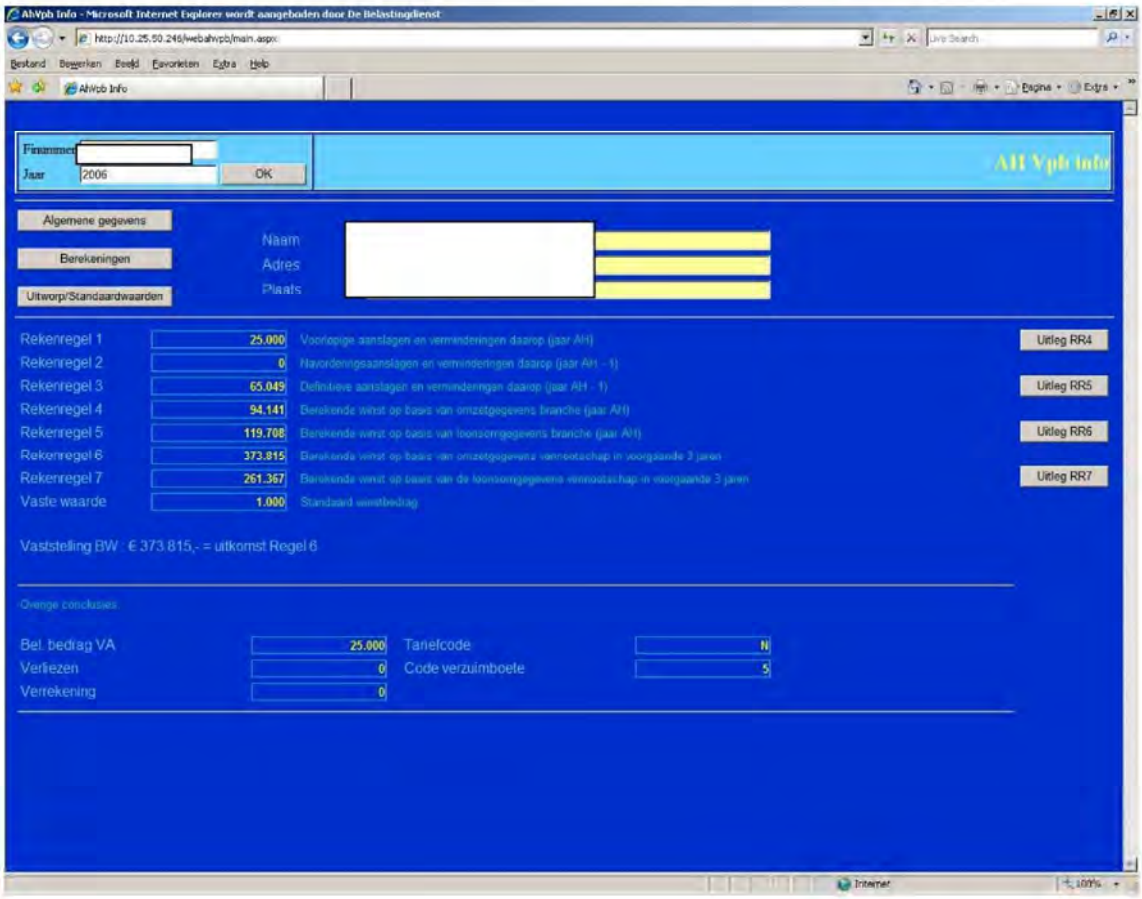
Hoogachtend,

Belastingdienst/Rijnmond/kantoor Rotterdam
Persoonsgegevens
namens deze,

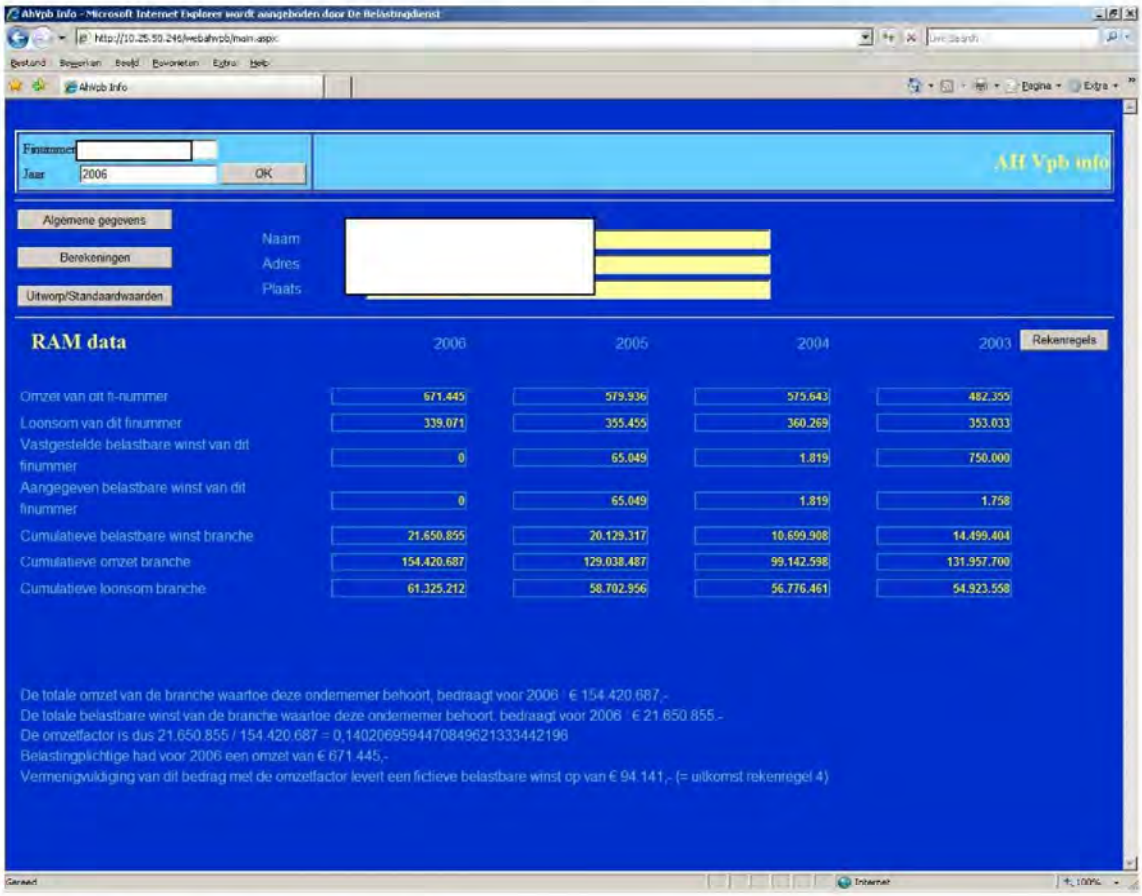
Persoonsgegevens

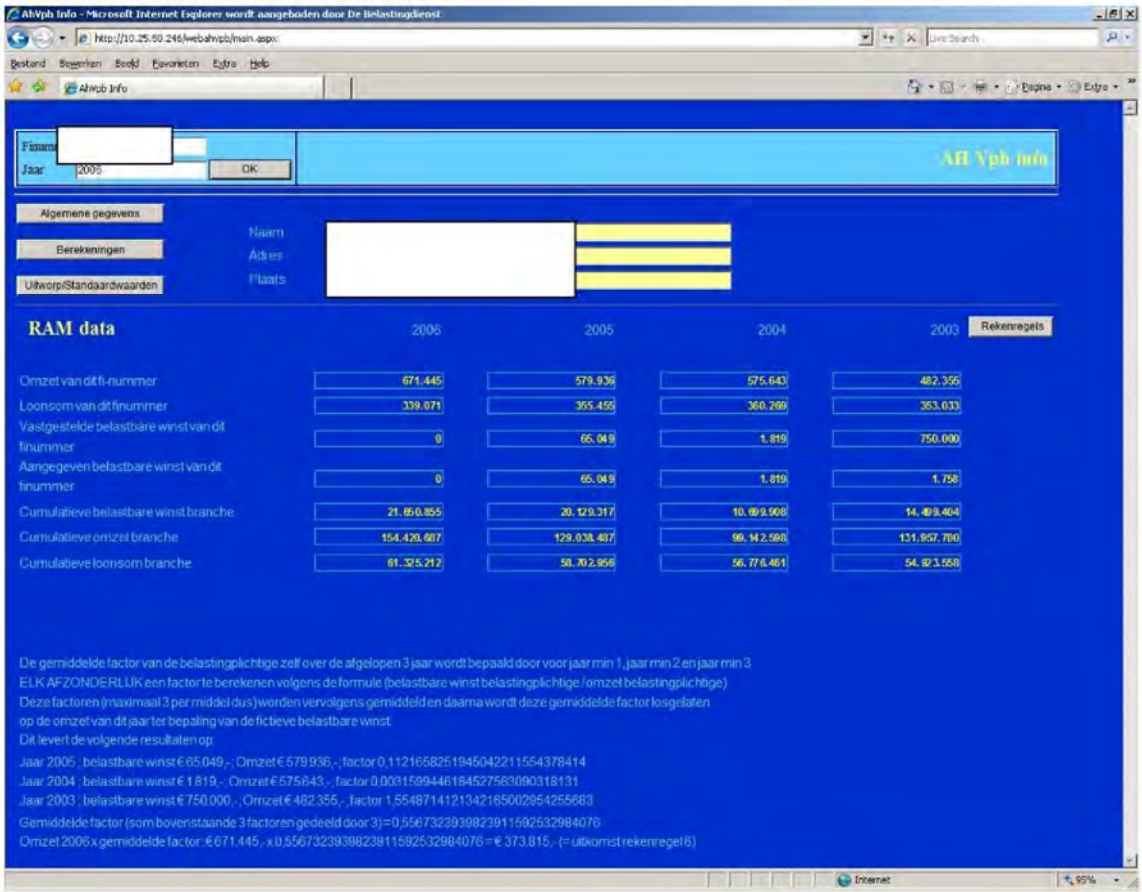
Bijlage 6 voorbeeldschermen Archief-applicatie



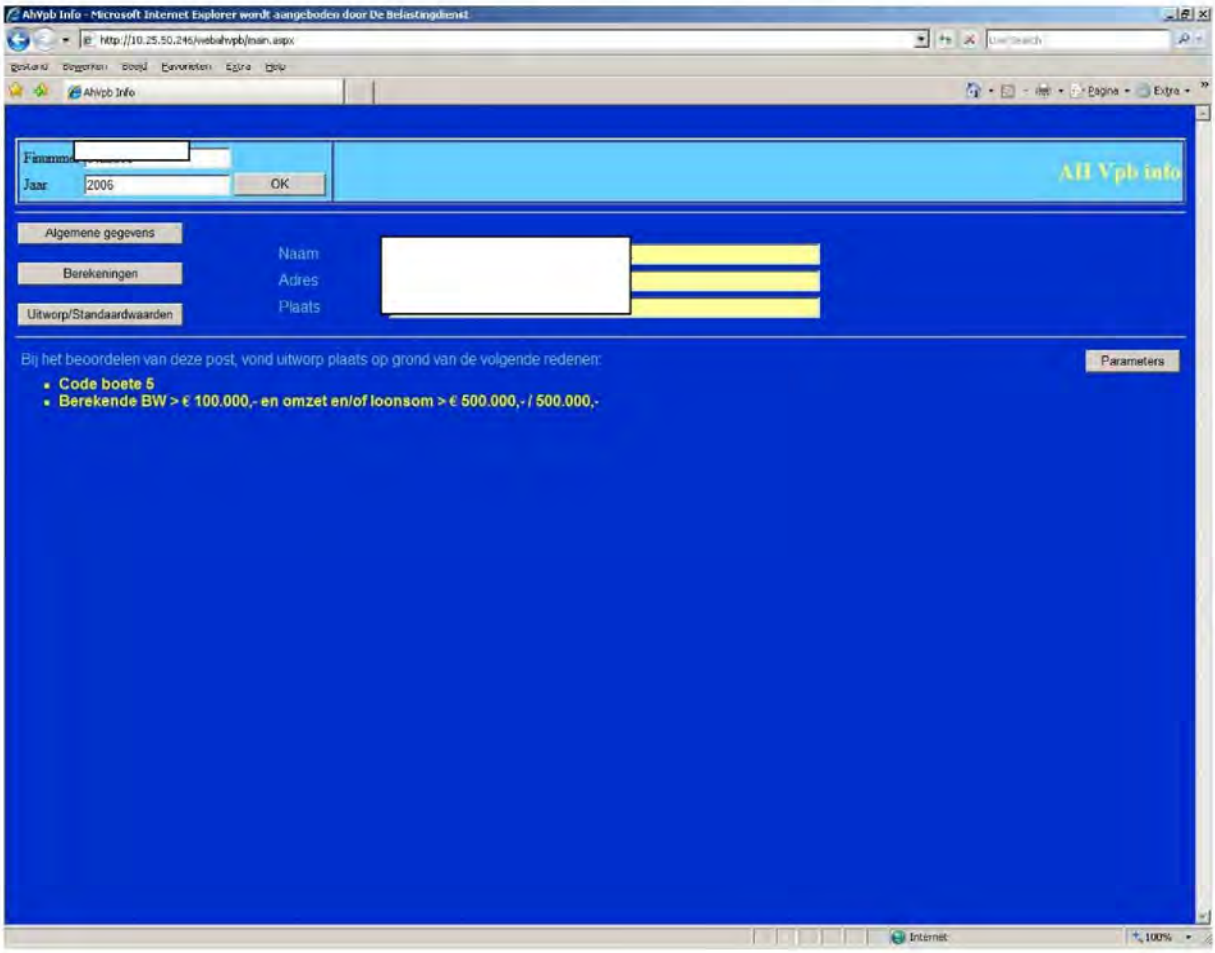


Bijlage 6 voorbeeldschermen Archief-applicatie (vervolg)





Bijlage 6 voorbeeldschermen Archief-applicatie (vervolg)



Bijlage 7 Passages uit Rapport doorlichting administratieve processen

2.4. Knelpunten en kroonjuwelen

Kroonjuwelen
In de inventarisatiefase zijn er door de regio's geen kroonjuwelen gemeld.
Tijdens de herontwerpfase is door de adoptieregio Rijnmond ten aanzien van het proces ambtshalve gemeld dat men in overleg met B/CPP en de Snelle Ontwikkel Service bezig is dit proces vergaand te automatiseren. De ontwikkeling en implementatie van de applicatie wordt voorzien ultimo 2008. De applicatie is dan vanaf januari 2009 voor de regio's beschikbaar en zal tot een efficiënter en effectiever ingericht proces leiden. De administratieve werkzaamheden binnen dit proces verleggen zich dan naar het voortraject van behandelen herinneringsbrieven en actualiseren bestand.

3.6.1. Beschrijving proces

Het proces 'Aangifteverwerking bewaking ambtshalve' omvat het behandelen van de uitvalberichten op de maandelijks aangeleverde lijst 39039 'Overzicht foutmeldingen aanmaningen', het behandelen van schriftelijke of telefonische reacties van belastingplichtigen met betrekking tot de verzonden aanmaningen, en het verwerken van de eveneens maandelijks aangeleverde lijst 55039 'Controleren binnenkomst aangifte' waarop wordt gesignaleerd welke aangiften, na het verstrijken van de termijn van de aanmaning, niet zijn ingeleverd.

3.6.4. Herontwerp

Het herontworpen proces voorziet, anders dan het huidige proces, in de verzending van een herinneringsbrief voorafgaand aan de selectie en verzending van de aanmaningen. Het is dan zaak om het bestand verzonden herinneringsbrieven snel, zo mogelijk vóór de aanmaningenselectie, te beoordelen. Ervaring binnen de procesadoptieregio Rijnmond leert dat circa 50 procent van het bestand ziet op afkeuringen VOW, foutieve NAW-gegevens en wijziging/einde belastingplicht. De signalen van de lijst 55039 worden uiteindelijk via de applicatie Ambtshalve VBN omgezet in een voorstel ambthalve aanslag. De voorstellen zullen naar het zich laat aanzien grotendeels automatisch leiden tot het vaststellen van een ambtshalve aanslag. Voor een ander deel gaan de voorstellen in de vorm van een pdf-bestand als uitworp naar de regio. Het beoordelen en verwerken van de uitworp voor het MKB-segment vindt plaats op de administratie. De uitworp voor de segmenten MGO en ZGO wordt beoordeeld door ITO-medewerkers. De procesplaat van het herontwerp is opgenomen als bijlage 6.

Ten aanzien van het proces 'Aangifteverwerking bewaking ambtshalve' wordt in het herontworpen proces geen onderscheid meer gemaakt tussen de segmenten MKB en MGO/ZGO. De daarmee te realiseren efficiencywinst wordt ingezet in het voortraject van dit proces, te weten het verzenden van een herinneringsbrief en bestandswerkzaamheden.

3.6.8. Samenvatting

Na herontwerp wordt voorafgaand aan de aanmaning een herinneringsbrief verzonden. Dit zou bij adequate behandeling het aantal te verzenden aanmaningen en bij gevolg ook het aantal uiteindelijk op te leggen ambthalve aanslagen moeten reduceren. De geautomatiseerde verwerking van de signalen van de lijst 55039 met behulp van de applicatie Ambtshalve VBN leidt voor een omvangrijk deel tot het automatisch (door de kelder) opleggen van ambtshalve aanslagen. De hoeveelheid aan de hand van de door de applicatie Ambtshalve VBN gegenereerde voorstellen, die door administratie (MKB-segment) of ITO (MGO en ZGO-segment) moeten worden beoordeeld, neemt significant af ten opzichte van de situatie nu.

Opdracht:	Selecteer 300 controleposten tweedehands autohandel t.b.v. aandachtsgebied MKB Handel & Transport
Opdrachtgever:	Persoonsgegevens
Projectleider	
Projectcode	2075
Uitgevoerd door:	Persoonsgegevens
Datum rapportage:	1 juni 2015

Algemeen:

De handel in tweedehands auto's is onderdeel van "Handel en Transport" (verder H&T) en bestaat voor MKB uit bijna 26.000 entiteiten. Ongeveer 16.000 entiteiten zijn op basis van indelingsregels opgenomen in aandachtsgebied "Kleine Ondernemingen"; bijna 10.000 zijn ondergebracht in het aandachtsgebied H&T. Er zijn bedrijven die enkel en alleen handelen in gebruikte auto's, maar ook autoreparatiebedrijven en dealers van nieuwe auto's handelen in gebruikte auto's. Daarom is niet enkel de focus gericht op bedrijven met branchecode 6622. Met behulp van bestanden van RDW en RAM zijn bedrijven in beeld gebracht die zich daadwerkelijk met de autohandel bezighouden. De selectie van de boekenonderzoeken is gericht op de entiteiten die opgenomen zijn in aandachtsgebied H&T, omdat daar de behandeling plaats zal gaan vinden. Uitgesloten zijn de entiteiten die het etiket convenantpost of VIP hebben. Verder zijn op basis van het laatst bekende teamnummers de entiteiten waarvan de behandeling plaatsvindt in de bijzondere behandelteams (vrijplaatsen, veelplegers, TBA etc.) ook uitgezonderd.

Autobedrijven komen niet alleen voor in aandachtsgebied H&T, maar ook in de andere aandachtsgebieden, omdat de indeling nu eenmaal plaatsvindt op entiteitniveau en niet op sofinummerniveau. De opdracht is uit te gaan van de entiteiten die behoren tot het aandachtsgebied H&T. Het kan dus ook voorkomen dat er branchevreemde activiteiten in een "autodossier" plaatsvinden; bij de selectie van de boekenonderzoeken is geen uitzondering gemaakt voor deze bedrijven. M.a.w. er kunnen in de geselecteerde boekenonderzoeken ook bedrijven voorkomen met een activiteit dat niet gericht is op autohandel.

Uitwerking opdracht
We zijn op zoek gegaan naar actieve autohandelaren, dus er moet sprake zijn van enige omzet (minimaal € 200.000 in 2014 en moeten er in tenminste in 2 van de 3 jaren (2012, 2013 of 2014) minimaal 50 auto's zijn verkocht zijn dan wel dat de combinatie van bestanden RAM, HSB en LCA aangeeft dat in 2014 minimaal 50 auto's verkocht zijn.

Als er nu al een boekenonderzoek heffing loopt dan wel in 2014 of 2015 is afgedaan dan hebben we de entiteit NIET geselecteerd; als er een onderzoek is ingesteld in de jaren 2012 of eerder met een correctie > € 5.000 dan is de entiteit wel geselecteerd.
Als er geen informatie aanwezig is dat een onderzoek vóór het jaar 2009 is ingesteld dat is de entiteit ook geselecteerd.

De onderzoeken zijn geselecteerd door risico's te benoemen bij deze groep ondernemingen; dat kunnen risico's zijn op het gebied van onjuistheid of onvolledigheid van de aangiften, maar ook op de niet tijdigheid van aangifte en betaling. Indicatoren die daar op duiden zijn opgenomen in het Risicomodel Rivierenland (RDM) en de risicoklasse. Hieronder is weergegeven welke indicatoren bij deze selectie zijn verwerkt. Dit is een eerste aanzet. Met input van de collega's uit het toezicht, vaktechniek en intelligence kan gewerkt worden aan verbeterde selecties.

Beschrijving indicatoren
Hieronder zal per indicator een korte beschrijving volgen en de score worden vermeld. De scores staan in de kolommen met de ORANGE kleur. Er zijn ook bedrijven geselecteerd waarbij een specifieke problematiek is onderkend. Deze moeten in alle gevallen behandeld worden; zij krijgen een dusdanige score dat zij in alle gevallen meelopen in de uiteindelijke selectielijst.

Om het bestand te doorgronden zijn de velden uit het bestand beschreven:

Onderstaande kolommen van het bestand bevatten algemene informatie, veelal afkomstig uit IKB en BVR. In de rode kolom is de selectie gemaakt voor het aandachtsgebied.

Kolom	Omschrijving
Dos.nr	
Dossiernaam	
Dos. Branchecode	
Brancheomschrijving dossiernummer	
Kantoorcode indeling	
Locatie	Hierin is de transitie van de kantoren verwerkt
Verzorgingsgebied	De 5 verzorgingsgebieden waarin de kantoren zijn ondergebracht
Team nummer laatst bekende dosnr in jaar	Teamnummer
Ent . Wolbsom	Belastingbedrag Ob,LH en VPB
Aand. Gebied	Indeling volgens BVR nov 2014 , getoetst t/m mei 2015
Segment	MKB
Weging	Weging is de klasseindeling binnen het aandachtsgebied
Omzet OB 2014	Totaalomzet OB
Selectie H & T= 1; VIP/ GO/CNV/ AR&D/ TBA= 0; afgevoerd én Kl. Ond en niet actieven zijn uitgezonderd	De selectie is gebaseerd enkel op behandeling binnen de teams in het aandachtsgebied H & T

Er zijn wat kenmerken verzameld die wat zeggen over het aangiftegedrag van de "entiteit" en over toezicht. Een toelichting volgt hierna.

Boekenond. vlgs definities in te stellen	Boekenonderzoek Ja betekent dat entiteit gecontroleerd kan worden
Risicoscore B.O. gewenst =1	Teller risico
Score mat batch	Is score van vergelijkbare bedrijven; hoe hoger de score, hoe hoger het risico
Risicoscore mat batch,	Teller risico
Score Rivierenland	Is vergelijkbaar met risicoklasse, maar nu bepaald op sofinr
Risicoscore Rivierenland	Teller risico
ENT_RISICOKLASSE	risicoklasse van februari 2015
Risico_RISCOKLASSE C,D,E= 1	Teller risico
Risico_weegscore CLO	Teller risico, deze weegscore wordt gehanteerd door CLO

Boekenond. vlgs definities in te stellen
Indien onlangs via een veldtoets heffing toezicht heeft plaatsgevonden dan is het nu niet wenselijk om opnieuw het bedrijf te bezoeken.

Daarom is het volgende in beeld gebracht:
- Is er een onderzoek heffing ingesteld?
- Is het onderzoek uitgevoerd en beëindigd, of nog onderhanden?
- Is het onderzoek afgerond in 2014 of 2015?
- Ligt het laatste controlejaar voor of na 2012 (m.a.w. hoe recent is het toezicht)
- Is er een positieve correctie of waardeafspraak groter of gelijk € 5.000 aangebracht?

Informatie over boekenonderzoeken van vóór 2009 is nu niet voorhanden. De geraadpleegde bestanden zijn bijgewerkt tot eind april 2015; mutaties na die datum kunnen van invloed zijn op de selectie. (niet meer onderhanden, alsnog ingetrokken of afgedaan, of reeds geselecteerd voor BO). De aandacht gaat uit naar de entiteiten met onderzoeken heffing die afgerond zijn voor 2014, en waarbij een correctie is aangebracht in de controlejaren 2009 t/m 2012. Daarbij kan men bijv. aandacht schenken of het gedrag ten aanzien van correcties in het verleden is aangepast. Ook als geen informatie over onderzoeken aanwezig is komt de entiteit in aanmerking.

Materialiteitsbatch

De materialiteitsbatch geeft een vergelijkende score van bedrijven die werkzaam zijn in een zelfde branche. Uitgangspunt daarbij is dan 70 % van de bedrijven vallen in eenzelfde bandbreedte met kengetallen. Deze kengetallen zijn Omzet/loonverhouding, Omzet/kostenverhouding, Omzet/winstverhouding. Ook de achterstand in Goa is hierin gewogen. De afwijkingen van deze 70 % norm krijgen een bepaalde waardering, die uiteindelijk leidt tot een risicoscore.
De bedrijven met score 30-39 krijgen een risicoscore 0,2
De bedrijven met score 40-49 krijgen een risicoscore 0,6
De bedrijven met score 50-59 krijgen een risicoscore 1
De bedrijven met score 60 en hoger krijgen een risicoscore 2

Risicodatamodel Rivierenland (RDM)
Er is gebruik gemaakt van RDM van februari 2015. Hierin staan scores op het gebied van het niet en/of te laat indienen/betalen van aangiften en onjuist en/of onvolledig indienen van aangiften, op sofinummerniveau. Deels komt dit overeen met de aandachtscategorie. De scores zijn verwerkt tot op entiteitniveau en gevoegd aan het selectiebestand. Scores <= 55 zijn niet geselecteerd.
De score 40- 49 heeft een risicoscore van 0,2
De score 50- 99 heeft een risicoscore van 0,4
De score 100-150 heeft een risicoscore van 0,6
De score 150-200 heeft een risicoscore van 0,7
Tussen 200-249 heeft een weging van 0,8
Boven 250 heeft een weging van 1.

Aandachtscategorie C, D en E op entiteitniveau
Deze letteraanduiding staat voor middel (C) of hoog (D) fiscaal risico en fraude (E). Als men dit combineert met de categorie fiscaal belang 1, 2, 3, wat staat voor hoog, middel of laag fiscaal belang dan geeft dat een inschatting van het risico dat de Belastingdienst loopt dat de verschuldigde belastingen onjuist, onvolledig en niet tijdig worden aangegeven en betaald. Er zijn in aandachtsgebied H&T > 5.500 entiteiten in aandachtscategorie C en D; dit ligt boven de 55 % van het totaal aantal entiteiten.

Risicoscore CLO
CLO heeft m.b.v. de OB nummers en een weging van ICL, ICV en SCAC-verzoeken een risicoklasse bepaald. Als de gemiddelde risicoklasse binnen de entiteit > 50 of de hoogste individuele score > 75 dan wordt er een risicoscore van 1 toegekend.

Specifieke onderwerpen:

Risico PIT en/of FSV	Uitworpredenen
Risico_Gefis Ja =1	Melding bij Fiod in het verleden
RISICO_ABD	Selectie via Douane
Beinvloedbaar invordering	Aandacht voor het bedrag beinvloedbare invordering
Niet_beinvloedbaar invordering	Dit kan zijn uitstel bezwaar, beroep
Openstaand bedrag	Totaal bedrag
Risico_Beinvl. achterstand	Teller 1 of 2

PIT / FSV signalen
Per entiteit is in beeld gebracht of er specifieke signalen zijn ter behandeling, zowel actueel als in het verleden. Indien dit zo is dan is dit via de score 1 tot uitdrukking gebracht.

Gefis informatie
In het geval dat er informatie bekend is dat de entiteit in het verleden in aanraking geweest is met de FIOD, dan is dit in kolom Gefis vermeld met code 1.

Risicolijst ABD
Indien de waarde van een auto bij invoer bij de Douane vragen oproept komt een signalering in de applicatie ABD (Aangiftesysteem BPM Douane)

Beinvloedbare invordering schulden

Een onderdeel bij een boekenonderzoek dat ook de aandacht moet hebben is het betaalgedrag van belastingplichtige. Een deel van de schulden is niet beïnvloedbaar; denk aan uitstel van betaling bij bezwaar. De entiteiten met een beïnvloedbare belastingschuld tussen €10.000 en € 50.000 zijn in beeld gebracht, zij hebben de risicoscore 1; boven 50.000 score 2. Het kan zijn dat een deel van het beïnvloedbare bedrag bestaat uit conserverende aanslagen. Deze worden volgens de laatste richtlijnen als niet beïnvloedbaar aangemerkt.

Risico_Fisc. Dienstverlener	Indeling FD op basis van gedrag van alle klanten
Risico_Beschikkingen	Verklaring geen prive gebruik auto
Risico_Dubieuze afnemers	Europese uitwisseling van gegevens over status afnemer auto
Inspectie, controle, toezicht	
Risico_MIA =1	Is ook sprake van desinvesteringsbijtelling?
Risico_NegNorm OB 5/6 =1	Code duidt op verplichte aandacht voor de negatieve aangifte OB
Risico_OB_Pr. Gbr.auto =1	Wel pr. gebruik auto aangegeven maar geen OB hierover
Risico_OB_Privé =1	Geen suppletie en geen omzet prive in aangifte Ob
Risico_Pga_Flg	Relatie pga in loonstaten en aangifte Ob
Risico_Bijz_Auto	Auto's niet behorend tot bedrijfsvoorraad en geen PGA
Risico_OB_BALANS_2013 1= >5000; 15000=2	Balanspost OB 2012 dan wel 2013
Risico_Relatie Omzet/Afdracht 2013	Relatie omzet hoog en afdracht OB
Risico_Vies_ICV	Relatie ICV met de aangifte OB
Risico_verzuimen	In de laatste 5 jaren > 25 aangifte /betalverzuimen

Beconnumer
Er is per entiteit onderzocht of een fiscaal dienstverlener (FD) behulpzaam is bij het doen van aangiften IH en/of VPB. Het is mogelijk dat er meerdere FD's voor belastingplichtigen in een entiteit werkzaam zijn, maar ook dat er van personen/ondernemingen niet bekend is of ze gebruik maken van een FD.

Elke FD is gewogen op meer dan 20 onderdelen die zien op tijdigheid van betalen en aangiften en op juistheid en volledigheid (op basis van navorderingen en verminderingen vrijwillig dan wel onvrijwillig).
De FD' s die meer dan 75% boven het gemiddelde scoren krijgen een score 2;
De FD 's die tussen de 20 % en 75% boven het gemiddelde scoren krijgen een score 1
De FD' s die tussen de -20 % en +20% van het gemiddelde scoren krijgen een score 0,5
De FD 's die minimaal 20% onder het gemiddelde scoren krijgen score 0
De FD 's die minder dan 10 aangiften van zakelijke klanten verzorgen en de personen/ bedrijven waarvan niet bekend is dat ze een FD hebben krijgen een score 1.

Per entiteit is zo een gewogen score bepaald op basis van bovenstaande uitgangspunten.
Het zijn dus niet per definitie slechte FD's maar de score kan een indicatie zijn dat de FD dan wel zijn klanten meer dan gemiddeld verstoringen oproepen.

Risico beschikkingen (Verklaringhouder en privé gebruik auto)
De brieven van LCA voor verklaringhouders "geen privé gebruik auto" en "Uitzondering zakelijk gebruik bestelauto (UZGB)" zijn vergeleken met de door de vermoedelijke inhoudingsplichtige toegepaste codes 2 en 7 in de loonstaten. Bij een afwijking van 3 of meer toegepaste codes is de risicoscore 1 toegekend.

Risico dubieuze afnemers
Een groot aantal lidstaten wisselt informatie uit over de actieve status van bedrijven die in auto's handelen. In he geval dat een Nederlands bedrijf bovengemiddeld handelt met bedrijven binnen Europa die als katvanger te boek staan, reeds failliet zijn, vow zijn, of verdacht zijn bij carrouselfraude is een risicocode 1 vermeld.

Inspectie, controle, toezicht

Milieu investeringsaftrek en desinvesteringen 2013

Als het investeringsbedrag ligt > € 25.000 dan bevelen we aan dat de toegepaste investeringsregeling wordt beoordeeld, tevens de milieu-investering maar ook de desinvesteringen in de beoordeling worden betrokken. Speciaal aandacht voor de milieuvriendelijke auto's die met forse subsidies zijn aangeschaft en met regelmaat binnen 5 jaren worden verkocht.

Negatieve norm 5 en 6
Deze normen worden gebruikt om aangiften OB waarin OB wordt teruggevraagd te signaleren voor een verplichte beoordeling, vanwege vermoeden van fraude. De bedrijven waarbij dit speelt zijn in het bestand terug te vinden met code 1.

Risico OB Privé gebruik auto
Het komt voor dat wel privé gebruik auto is aangegeven maar dat niet duidelijk is of de verschuldigde OB ook aangegeven is. Dit risico krijgt score 1.

Risico OB Privé
In deze branche is het gebruikelijk dat er privé gebruik wordt gemaakt van zakelijke auto's. Een aanwijzing dat de bijtelling privé gebruik achterwege is gebleven kan zijn in het geval dat de OB niet op de aangifte (veelal laatste aangifte van het jaar) wordt vermeld en dat ook de suppletie achterwege is gebleven. De selectie is gemaakt voor het jaar 2013.

Risico pga in Flg (privé gebruik auto in loonstaten)
De grondslag privé bijtelling in de loonstaten wordt vergeleken met de grondslag (omzet privé) in de aangifte OB. Bij afwijking hiertussen volgt weer een risicocode 1.

Risico bijzondere auto
In het bestand is een kolom opgenomen genaamd Taxgap Auto, waarin wordt weergegeven of in het bedrijf auto's worden gebruikt waarover geen privé gebruik bijtelling plaats heeft gevonden. Er is bij de selectie uitgegaan dat er minimaal 3 auto's een onverklaard privé gebruik kunnen hebben. Risicoscore 1.

Balanspost OB
De balanspost OB 2012 en of 2013 is bepaald aan de hand van de aangiften VPB en IH die momenteel via RAM ter beschikking staan. Helaas is dit voor het jaar 2013 een beperkt aantal. Indien in de aangifte een vermelding staat van nog verschuldigd OB is dit meegenomen in de selectie. Er zijn bijna 850 entiteiten geselecteerd waar naar verwachting een bedrag > € 5.000 aan oude openstaande OB schulden bestaat, hiervan hebben er 100 een schuld boven de € 15.000. Omdat er ook een project balansposten OB bestaat heeft afstemming plaatsgevonden. Gevraagd is het onderstaande onder de aandacht te brengen:

- bij correctie van de balanspost wordt altijd een boete wordt opgelegd, tenzij er zeer goede reden zijn hiervan af te wijken; dit zal bij hoge uitzondering zijn;
- ga voorafgaand aan het onderzoek na of in IKB, onderdeel Notities, een kantoortoets is opgestart n.a.v. de balansschuld;
- neem bij vragen contact op met Persoonsgegevens; telefoonnummer Persoonsgegevens;
- vraag in het gesprek met de ondernemer of er al over dit onderwerp met de Belastingdienst wordt gecommuniceerd;
- bij correctie vergeet niet de applicatie BAS te vullen, bij vragen hierover raadpleeg P-gv. P-gv.
- er is werkinstructie Balansschulden beschikbaar op Connect People, onder "Intensivering toezicht en omzetbelasting"

Relatie omzet en afdracht OB
In kolom Omzet_afdracht2013 is een relatie gelegd tussen de omzet hoog en het saldo OB. In de gevallen dat het saldo < 4 % van de omzet Hoog dan bestaat het risico dat sprake is van het niet verantwoorden van omzet dan wel sprake is van carrouselfraude. Let op de relatie met de voorbelasting. Indien deze incidenteel hoger is dan is het risico uiteraard lager.

Vies en ICV
Er zijn afspraken met de EU landen om intra communautaire transacties met elkaar uit te wisselen. De aankopen van de onderneming liggen vast in VIES. Er is een koppeling gelegd op dossierniveau tussen rubriek 4 b van de aangifte OB en de informatie uit VIES. Verschillen zouden kunnen duiden op niet geboekte inkopen. Op dossierniveau zijn de verschillen geselecteerd > € 50.000.

Risico verzuimen

In het geval dat er > 25 aangifte en/of betaalverzuimen zijn voor alle belastingmiddelen gedurende 5 jaren dan is een risicoscore van 1 toegekend.

Specifieke risico's aangedragen door LCA

Risico_Transformeren BTW auto naar margeauto	Dit onderwerp heeft hogere score gekregen om zeker te stellen dat dit risico opgepakt gaat worden. Neem contact op met LCA
Risico_camper	Dit onderwerp heeft hogere score gekregen om zeker te stellen dat dit risico opgepakt gaat worden. Neem contact op met LCA
Risico CO2	Dit onderwerp heeft hogere score gekregen om zeker te stellen dat dit risico opgepakt gaat worden. Neem contact op met LCA

Risico transformeren btw-auto naar marge-auto
LCA heeft een lijst van risicovolle bedrijven geselecteerd, waarin risico's voorkomen m.b.t. transformatie van btw-auto naar marge-auto. Vanwege het leereffect hebben deze bedrijven een risicoscore van 5 gekregen binnen deze selectielijst. Voor uitleg en behandeling kan contact opgenomen worden met Persoonsgegevens

CO2 (BPM)
Het risico CO2 ziet op het onjuist indelen van auto's met uitstoot in grammen CO2, waardoor te weinig BMP wordt afgedragen

Naam	Sofinummer	Entiteitnr	Aantal voert.	Kt.nr	Kantoor
Automobiel Online Groep B.V.	Persoonsgegevens		16	145	Den Haag
Autobedrijf Maat B.V.			11	153	Middelburg

De controle bij Automobiel Online Groep B.V. moet uitgevoerd worden samen met Persoonsgegevens Persoonsgegevens Voor het andere bedrijf kan contact worden opgenomen met P-gv. Persoonsgegevens

Campers
Er is een lijst van 10 camperbedrijven, waarvan er 4 in de query meelopen; zie "w".
De overige 6 camperbedrijven moeten individueel beoordeeld worden voor onderzoek.
Bij alle onderzoeken moet Persoonsgegevens betrokken worden. Persoonsgegevens Persoonsgegevens De volgende finrs zijn geselecteerd voor de individuele beoordeling:

Om deze bedrijven in alle gevallen in de selectie mee te laten lopen is een score van 10 toegekend.

Omvang bedrijf
Tot slot zijn aan het bestand een aantal kolommen toegevoegd met info over aantallen verkopen auto's; de blauwe kolommen zijn op entiteitniveau en afkomstig uit RAM en zien op diverse jaren; de groene kolommen komen uit HSB bestanden, de paarse is afkomstig van LCA. De aantallen wijken helaas af van elkaar maar geven wel richting naar omvang. Daarom is een combinatie gemaakt om te komen tot de bedrijven> 50 auto's.

Totaalscore en communicatie:

TOTAALSCORE ORANGE CELLEN	Op basis van de ranking hoog laag zijn voor de kantoren de onderzoeken geselecteerd

Bovenstaande signalen zijn gekoppeld aan de entiteiten. Vervolgens is een ranking gemaakt van de meest risicovolle entiteiten. Er worden 300 onderzoeken geselecteerd die dusdanig over de 19 kantoren verdeeld zijn, in relatie tot het totaal pakket, dat er voldoende signalen per kantoor zijn.

De algemene signalen zoals aandachtscategorie en score Risico Datamodel Rivierenland wijzen op mogelijke nalevingstekorten. Denk bijv. aan het te laat indienen van aangiften: is de administratie

niet op orde, komt daarmee de juistheid van de ingediende aangifte OB in gedrang.
Verschuivingen? De overige signalen wijzen op fiscaaltechnische risico's vaak met Ob aspecten.

Het is goed om feedback te krijgen op deze selectie; verbeteringen zijn niet enkel nuttig voor dit segment maar zijn ook van belang voor de andere aandachtsgebieden, zeker waar het gaat om niet branche gerelateerde risico's.

De selectie is gemaakt met behulp van data die in sommige gevallen enkele maanden oud is. Dit kan er toe leiden dat werkende in de actualiteit er geen aanleiding meer is om een onderzoek in te stellen; bijv. vanwege overlijden ondernemer, faillissement of dat al een onderzoek is aangevangen. Ook is het lastig uit de jaarrekeningen van samenwerkingsverbanden de juiste data te nemen, omdat de mogelijkheid bestaat ook persoonlijke jaarrekeningen in te dienen.

Behandelvoorstel
Het behandelvoorstel is om een integraal onderzoek in te stellen. In de voorbereiding van het onderzoek is aan het professioneel oordeel van de veldtoetser om eventueel af te wijken van het door EHI voorgestelde integrale beoordeling van de aangiften.
Deze beoordeling zal wel teruggekoppeld moeten worden naar EHI om de selectie en toedelingsregels te verbeteren.

Bijlage 1

De branchecodes op entiteitniveau en de verdeling van het aantal entiteiten over deze branches is weergegeven in onderstaande tabel. Het zwaartepunt ligt bij handelaren in gebruikte personenauto's en autoreparatiebedrijven. In de bovenste tabel staat de totaalverdeling, waarbij bijvoorbeeld het groot aantal autowasserijen opvalt.

Br. code entiteit	Omschrijving branchecode	Aantal entiteiten
6187	Auto's, auto-accessoires en onderdelen (ook banden)	2.411
6387	Auto's, accessoires en onderdelen (ook banden)	1.225
6621	Nieuwe personenauto's	1.340
6622	Gebruikte personenauto's	7.899
6623	Auto-accessoires en -onderdelen (ook autobanden)	1.392
6821	Autoreparatiebedrijven (garages) en dergelijke	7.204
6822	Autoplaatwerkerijen,-spuiterijen (reparatiebedrijven)	1.261
6829	Autoreparatiebedrijven, gespecialiseerd in deelbewerking	1.686
9823	Autowasserijen	1.246
		25.664

Bijlage 2

Kantoor	H&TR	KO	Eindtotaal Autohandel	H &TR verdeling
Amsterdam	186	416	602	11
Middelburg	259	256	515	12
Maastricht	306	526	832	13
Groningen	354	556	910	13
Venlo	371	493	864	13
Doetinchem	381	411	792	13
Emmen	400	582	982	14
Almere	433	605	1038	14
Leeuwarden	535	686	1221	15
Zwolle	540	681	1221	15
Hoofddorp	591	791	1382	15
Enschede	609	891	1500	16
Den Haag	680	1072	1752	16
Hoorn	698	805	1503	16
Arnhem	794	957	1751	17
Breda	838	1029	1867	18
Rotterdam	867	1225	2092	18
Utrecht	889	1113	2002	18
Eindhoven	1261	1577	2838	20
Eindtotaal	**10992**	**14672**	**25664**	**287**

14-4-2015 memo richting Persoonsgegevens
Even een update over de query:
de dataverzameling is zo goed als rond. Gisteren hebben P-gv. en ik ons gebogen over een aantal selectiecriteria die ik je niet wil onthouden. Op basis van de criteria en een weging die we daar aan verbinden willen wij de selectie maken.
De focus ligt met name op het middel Ob, daarnaast zijn er natuurlijk ook aspecten in de winstsfeer en LH te onderkennen. De eerste drie criteria zijn qua risicoduiding algemeen van aard, terwijl 5 tot en met 18 specifieke onderwerpen zijn.
Als je iets mist of op/aanmerkingen hebt laat het weten. Afhankelijk van de wens kunnen we beoordelen of we het nog kunnen verwerken. Er zijn ongeveer 25.600 entiteiten die in de selectie meelopen.

De selectie is gemaakt voor een aantal branches die actief zijn in de autohandel. Specifieke onderwerpen die in die branche fout zouden kunnen gaan zijn in de selectie betrokken, dat vergt dan soms ook weer specifieke kennis.
De criteria:

1	Aandachtscategorie in eerste aanleg richten op C en D (hoog risico) dan B (starters) en dan A (laag risico)	weging 1
2	Risicomodel Rivierenland, bovenste 10 %	weging 1
3	Materialiteitsbatch	weging 1
4	Veldtoetsinformatie en FIOD . Uitsluiten van onderzoeken die al in veldtoets / FIOD in beeld zijn (geweest)	
5	Omzet hoog x 4 %- saldo afdracht Ob; indien < - 1000 dan	weging 2
6	Taxgap auto (het aantal auto's zonder verklaring privé gebruik auto) indien .>= 3 auto's	weging 1
7	CLO weegscore (nog te ontvangen)	weging 2
8	Vies en aangifte Ob indien verschil >€ 5.000	weging 2
9	Balanspost OB indien > € 5.000	weging 2
10	Privé gebruik auto en verklaringhouders (afwijking + uzgb) indien >= 3 auto's	weging 2
11	CO 2 posten (specifiek probleem BPM) hoge weging om deze altijd in de selectie mee te laten nemen	weging 10
12	Campers hoge weging om deze altijd in de selectie mee te laten nemen	weging 10
13	Neg norm OB 5 en 6	weging 1
14	Loonbijtelling FLG (pga) vergelijken met omzet privé (ob aangifte) en geen suppletie	weging 2
15	Geen suppl. en geen OB privégebruik 4e kw of dec aangifte indien> €1.000 OB	weging 1
16	Arbeidsbeloning partner indien> € 30.000	weging 2
17	Beinvloedbare betalingsachterstand indien € 15.000	weging 2
18	Milieu inv.aftrek en desinvesteringen	weging 1

Wat hebben we niet gedaan
- theoretisch winstberekening = aantal auto's x opbrengst stel € 500
- selectie op onzakelijke kosten

Aanwezig op bijeenkomst 20 januari 2016 te Utrecht, project auto:
Persoonsgegevens

Persoonsgegevens

Je had van mij nog de lijst te goed met op en aanmerkingen/aanvullingen op de query Auto.

Ik neem ze hieronder op, soms wat kort maar mogelijk weet je wel wat er bedoeld wordt.

1. Teller ABD t.o.v. HSB
2. ABD : buitenland toevoegen en Sagitta
3. Btw auto wordt margeauto: beschrijving opvragen hoe dit onderdeel van de query tot stand is gekomen
4. Opvraag alle auto's op entiteitniveau, dus ook van kinderen, echtgenoot en digra enz
5. Invordering verder uitwerken
6. Ht wel of niet meenemen? Antw : voortaan wel meenemen in analyse, achteraf pas beslissen.
7. Nihilaangiften OB in beeld brengen
8. Vrijplaatsen en kamper: scoren hoger volgens deelnemers
9. Omzet V en W ook meenemen naast omzet OB i.v.m. margeregeling
10. Snelle starters in beeld brengen.
11. Hoge omzet en geen personeel
12. Aantal auto's in relatie tot aantal personeel
13. Entiteit met buitenlandse vestiging
14. Zwaarder wegen van ABD posten
15. Ongebruikelijk samenwerkingsverband man/vrouwfirma
16. Euro BV constructie met bijv CV , LTD enz
17. Bedrijven die leveren aan het buitenland.

Handboek Informatiebeveiliging B/CICT

(incl. maatregelen)

2009

(update HIB B/CICT 2007)

Inhoudsopgave

1 Opzet handboek 2
1.1 Inleiding 2
1.2 Doel 3
1.3 Relatie met klant-opdrachtgever 3
1.4 Werkwijze en verantwoording 4
2 Informatiebeveiliging 5
2.1 Algemene normen voor informatiebeveiliging 5
2.2 Specifieke informatiebeveiligingsnormen per hoofdproces 7
2.2.1 POO 7
2.2.2 Account management 12
2.2.3 Architectuur 14
2.2.4 O&B 15
2.2.5 Demand management 20
2.2.6 Exploitatie 23
2.2.7 Resource management 31
3 Bijlage 1: Begrippenlijst 37
4 Bijlage 2: Overzicht wijzigingen ten opzichte van het HIB B/CICT 2007 42

De in de tekst cursief gedrukte begrippen zijn opgenomen in de als bijlage bij dit document opgenomen begrippenlijst

1 Opzet handboek

1.1 Inleiding

De primaire en ondersteunende processen van de Belastingdienst zijn in hoge mate afhankelijk van adequate informatievoorziening en betrouwbare *(ICT-)services*. Het Handboek *Informatiebeveiliging* Belastingdienst (HIB) 1996 formuleert dat als volgt:

> "Uitval van computers/ netwerken, 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. Indien de Belastingdienst deze risico's onvoldoende beheerst, kan het vertrouwen van de belastingplichtigen in de Belastingdienst worden geschaad. Dit kan vervolgens de bereidheid van belastingplichtigen om aan hun verplichtingen te voldoen, nadelig beïnvloeden. Verstoringen van de continuïteit van de gegevensverwerking kunnen een directe invloed hebben op de kasstroom naar de overheid en bij de douane tevens op het (inter)nationale handelsverkeer."

Het informatiebeveiligingsbeleid van de Belastingdienst is er op gericht de *beschikbaarheid*, de *integriteit* en de *vertrouwelijkheid* van de (geautomatiseerde) informatievoorziening te waarborgen. Om dit te realiseren is het van belang een aantal gemeenschappelijke uitgangspunten te hanteren en deze uit te dragen. Vanuit het algemene informatiebeveiligingsbeleid worden de rol, de uitgangspunten, de verantwoordelijkheden en de borging van het beleid binnen de Belastingdienst aangegeven.

Het algemene informatiebeveiligingsbeleid van de Belastingdienst is verankerd in het HIB 1996 en verder uitgewerkt in het Handboek Informatiebeveiliging Belastingdienst – Basis BeveiligingsNiveau (HIB-BBN) Belastingdienst, versie 2007 en het Handboek *Informatiebeveiliging* van B/CICT. Dit laatste handboek is een uitwerking van het HIB 1996 voor B/CICT als ondersteunende dienst. B/CICT is, evenals alle andere eenheden, ook gehouden aan het naleven van de *informatiebeveiligingsmaatregelen* opgenomen in het HIB-BBN Belastingdienst.

In dit handboek zijn uitsluitend informatiebeveiligingsnormen opgenomen. Het is niet mogelijk een voldoende *beveiligingsniveau* te realiseren op basis van deze normen alleen. De organisatie en processen van B/CICT dienen aan hoge eisen te voldoen, waardoor er sprake is van voorspelbaarheid, structuur en kwaliteit van de activiteiten. Met opzet is er voor gekozen om deze voor een adequate informatiebeveiliging noodzakelijke kwalitatief hoogstaande procesinrichting niet in dit document op te nemen. De normering voor de algemene procesbeheersing is daarom opgenomen in een separaat document (Normen GPO versie 1.0). De uitwerking van deze normering is opgenomen in het Globaal Proces Ontwerp (GPO) en de Detail Proces Ontwerpen (DPO's) van B/CICT. De informatiebeveiligingsnormering kan nooit los worden gezien van de in deze documenten beschreven inrichtingscriteria voor proces- en organisatie. Een en ander betekent dat het basisbeveiligingsniveau van CICT wordt gevormd door de procesbeheersing in het kader van het GPO/DPO en de in de processen verankerde maatregelen als gevolg van de normering in dit document. Dit staat nog los van de specifieke inrichtingscriteria van de klant met betrekking tot applicaties (VBA) en infrastructuur (VBI).

Beschikbaarheid van gegevens in de zin van uitwijkvoorzieningen wordt in dit document niet behandeld. De normen die mogelijk hiervoor van toepassing zijn worden in een separaat document beschreven als gevolg van het Handboek Calamiteitenplan Belastingdienst (HCB).

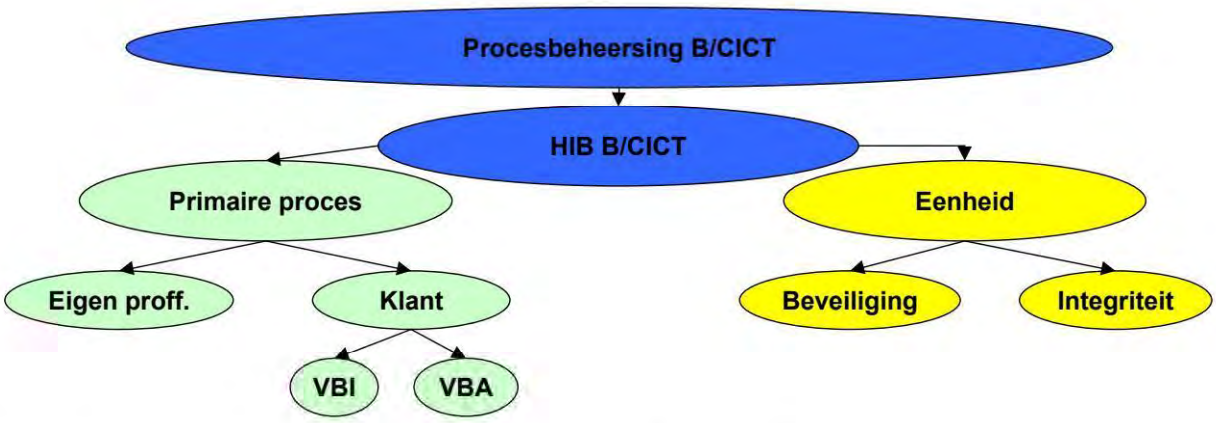
Om de lezing van dit document niet onnodig te bemoeilijken is de (theoretische) scheiding tussen informatiebeveiliging en *integriteit* niet aangebracht. Daar waar richtlijnen en normering ten aanzien van

personeel en organisatie worden beschreven, wordt *integriteit* als onderdeel van de informatiebeveiliging gezien.

1.2 Doel

In het Handboek *Informatiebeveiliging* B/CICT wordt het informatiebeveiligingsbeleid van de Belastingdienst vertaald naar informatiebeveiligingsnormen voor B/CICT. De normen zijn de basis voor de te treffen *informatiebeveiligingsmaatregelen*. De normen hebben een algemene werking en zijn onafhankelijk van de gebruikte informatietechnologie.

De processen van B/CICT moeten zodanig zijn ingericht dat de B/CICT-organisatie haar doelstellingen efficiënt en met een bepaalde kwaliteit en *beveiligingsniveau* kan realiseren. *Informatiebeveiliging* moet in deze processen zijn verankerd en afgestemd zijn op de feitelijke en actuele risico's. Het handboek dient als basis voor het uitwerken, implementeren en handhaven van *informatiebeveiligingsmaatregelen*. Dit handboek Informatiebeveiliging CICT geeft normen voor zowel B/CICT als eenheid (dienstonderdeel) van de Belastingdienst als voor het primaire proces van B/CICT:



Afbeelding 1: Samenhang procesbeheersing en normatiek beveiliging

De uitwerking van de normen in *informatiebeveiligingsmaatregelen* dient te geschieden in het kader van procesbeheersing door het verantwoordelijk management. Het management beheerst door de implementatie van de maatregelen en controles daarop de informatiebeveiligingsrisico's en legt hier verantwoording over af. Het management mag van de maatregelen in dit handboek afwijken mits de onderbouwing op basis van een risicoafweging en eventuele compenserende maatregelen is vastgelegd. Aanbevolen is het deze risicoafweging in samenspraak met de beveiligingscoördinator te doen.

Het handboek biedt door de weergave van zoveel mogelijk geobjectiveerde toetsingscriteria een basis voor de beoordeling en toetsing van de feitelijk getroffen maatregelen.

1.3 Relatie met klant-opdrachtgever

Het handboek vervult een belangrijke rol naar de klant-opdrachtgever van B/CICT. Met behulp van dit handboek geeft B/CICT concreet aan op welke wijze B/CICT de eisen en verwachtingen van de klant met betrekking tot *informatiebeveiliging* realiseert.

Ieder *beveiligingsniveau* kent zijn eigen specifieke inrichtings- en handhavingskosten. Deze dienen onderwerp te zijn van onderhandelingen tussen B/CICT en de opdrachtgever, waarbij een balans gevonden dient te worden tussen risico en kosten. Bij deze onderhandelingen zal B/CICT vanuit haar expertise als goede automatiseringsleverancier de opdrachtgever wijzen op de door haar eventueel te lopen risico's.

De klant-opdrachtgever is verantwoordelijk voor de te stellen informatiebeveiligingseisen aan de (*ICT-)service*. Diverse onderdelen binnen de Belastingdienst, zoals B/CPP, zijn klant-opdrachtgever voor de (*ICT-)service*s. De eisen die de klant-opdrachtgever stelt aan het *beveiligingsniveau* van (*ICT-)service*s worden gesteld door B/CPP. De door de klant-opdrachtgever gestelde informatiebeveiligingseisen aan de (*ICT-)service* dienen gedurende de gehele levenscyclus van de (*ICT-)service* te worden nageleefd en zijn uitgangspunt voor de met de klant overeengekomen SNO-afspraken.

1.4 Werkwijze en verantwoording

Dit document is tot stand gekomen door deskundigen van B/CICT allereerst de normen te laten formuleren zodat er van een voldoende *Basis Beveiligings Niveau* sprake is. Deze normen zijn toegewezen aan de verschillende B/CICT processen. Vervolgens zijn bij deze normen de richtlijnen en risicoafwegingen geplaatst. De normenset is gebaseerd op algemeen aanvaarde maatschappelijke criteria zoals onder andere zijn vastgelegd in de Code voor Informatiebeveiliging (ISO/IEC 17799-1) en de Basisnormen Beheer en Beveiliging Infrastructuur en een studie van het Platform *Informatiebeveiliging* Tenslotte heeft B/CPP dit document als een goede samenvatting van de klanteisen verklaard.

Bij de vaststelling van het handboek *Informatiebeveiliging* B/CICT heeft overleg plaatsgevonden met verantwoordelijke managers van B/CICT. Het handboek wordt na akkoord van het MT B/CICT ter vaststelling aangeboden aan de Groepsraad Belastingdienst.

In dit document zijn, behalve de richtlijnen en normering in relatie tot de positie van B/CICT als opdrachtnemer van de automatiseringsoplossingen van de Belastingdienst, ook de richtlijnen en normen opgenomen die gelden voor alle eenheden van de Belastingdienst. B/CICT als eenheid is door haar specifieke voortbrengingsproces en door het gebruik van een zeer uitgebreide normatiek voor haar processen, afwijkend van de reguliere eenheden van de Belastingdienst. Daarom is besloten de richtlijnen van de Belastingdienst te vertalen voor de specifieke situatie binnen B/CICT, waarbij de strekking van de richtlijnen en normen onverkort zijn gehandhaafd. Met name de hoofdstukken 2.1 en 2.2.1 (gedeeltelijk) en hoofdstuk 2.2.7 zijn hiervan een weerslag. Deze hoofdstukken zijn gemaakt in samenwerking met deskundigen van de RAD, B/CPP en B/CICT.

De veranderingen in de informatietechnologie en de steeds opnieuw optredende bedreigingen, vragen een alerte en anticiperende houding. Ook vanuit de klantorganisatie kunnen andere wensen/eisen ontstaan. De in dit handboek vastgestelde normen dienen dan ook periodiek op hun inhoud en op hun uitvoerbaarheid te worden getoetst. Deze activiteiten zijn ondergebracht in het proces Proces- en Organisatie Ontwikkeling (POO) van B/CICT. De normatiek in dit handboek is output van het proces POO.

2 Informatiebeveiliging

2.1 Algemene normen voor informatiebeveiliging

In deze paragraaf zijn de normen opgenomen waaraan, naast de normen voor de specifieke processen, in ieder geval voldaan dient te zijn.

Richtlijn

Alg B/CICT R-1	*Binnen B/CICT dienen specifieke functies op het gebied van informatiebeveiliging te worden onderscheiden.*

Risicoafweging

Het niet aanwezig zijn van specifieke functies op het gebied van informatiebeveiliging kan negatieve gevolgen hebben voor de *integriteit* van het personeel, de informatiebeveiliging van gegevens en (*ICT-) service*s.

Norm

Alg B/CICT N-1-1	Er bestaan afzonderlijke functies voor het adviseren en toetsen op het gebied van informatiebeveiliging.

Maatregelen

1. Op centraal niveau binnen B/CICT wordt binnen het proces POO de samenhang van informatiebeveiligingsbeleid en -maatregelen in organisatie, processen, personeel en techniek geregeld.
2. Binnen het Architectuurproces fungeren beveiligingsarchitecten voor het ontwerpen en het geven van voorschriften over informatiebeveiligingsmaatregelen in ICT-services.
3. In het Architectuurproces zijn de informatiebeveiligingseisen voor de technische infrastructuur (VBI) die te maken hebben met de in dit document vervatte normen van B/CPP, nader in een generiek kader uitgewerkt. Dit kader kent een tweetal aspecten: een richtinggevend kader voor Architecten en een normerend kader voor Ontwerpers en Bouwers.
4. Binnen het Exploitatieproces houdt het subproces managen beveiliging toezicht op informatiebeveiligingsaspecten in *TIS-componenten*.

Richtlijn

Alg B/CICT R-2	*Informatiebeveiligingsincidenten worden zodanig geregistreerd, dat ze apart te identificeren zijn.*

Risicoafweging

Door het niet onderkennen van informatiebeveiligingsincidenten kunnen risico's bij het leveren van ICT-services en het beheren van gegevens niet voldoende worden beheerst.

Norm

Alg N-2-1 B/CICT	*Integriteitsincidenten, Informatiebeveiligingsincident*en en *Informatiebeveiligings-verstoringen* worden geregistreerd, geanalyseerd, op afhandeling bewaakt en aan betrokkenen gerapporteerd.

Maatregelen

1. *Informatiebeveiligingsincidenten en –verstoringen* worden als aparte categorie behandeld en vastgelegd binnen het call-afhandelings- en incidentproces.
2. Naast deze categorie wordt door het subproces monitoren beveiliging van het proces Exploitatie tevens (*mogelijke) informatiebeveiligingsverstoringen* vastgelegd en behandeld.
3. *Integriteitsincidenten* worden geregistreerd binnen het proces POO.
4. De *informatiebeveiligingsincidenten* worden, behalve aan de beheersprocessen binnen O&B, ook periodiek gerapporteerd aan het proces POO.
5. Alles wat kan dienen als bewijsmateriaal van de gemelde incidenten (werkopdrachten, kopie-bestanden, logging) wordt veiliggesteld.

2.2 Specifieke informatiebeveiligingsnormen per hoofdproces

2.2.1 POO

Richtlijn

POO R-1 B/CICT	*De opzet van de processen en de organisatie, die leiden tot een beheerste bedrijfsvoering, zijn beschreven en het bestaan en de werking kan worden aangetoond.*

Risicoafweging

Het niet uitvoeren van de ICT-dienstverlening volgens een standaardaanpak die voldoet aan eisen, die daaraan kunnen worden gesteld, kan negatieve gevolgen hebben voor de *informatiebeveiliging*. Zie ook hetgeen in de inleiding is opgenomen over de samenhang tussen normen voor organisatie en processen en informatiebeveiligingsnormen.

Norm

POO N-1-1 B/CICT	Om tot een beheerste bedrijfsvoering te komen, is er een beheersingsmechanisme om opzet, bestaan en werking van organisatie en processen, afzonderlijk en in samenhang met elkaar te borgen.

Maatregelen

1. Er zijn uitgangspunten voor het ontwerp en de werking van proces en organisatie vastgesteld in de normen procesbeheersing, het Globaal Proces (GPO), de Detail Proces Ontwerpen (DPO's) en het Organisatieontwerp; deze uitgangspunten zijn getoetst aan maatschappelijk aanvaarde kaders.
2. Jaarlijks wordt het GPO en de DPO's geëvalueerd en eventueel aangepast.
3. Jaarlijks zal B/CICT het niveau voor beheersing van processen en organisatie in het MT B/CICT vaststellen.
4. De opzet en werking van organisatie en processen worden door internen en externen op hun werking beoordeeld en geaudit en zonodig bijgesteld.

Norm

POO N-1-2 B/CICT	*Risico's* op het gebied van informatiebeveiliging worden permanent bewaakt en maatregelen om risico's te beheersen worden genomen.

Maatregelen

1. Voor het beheersen van de risico's op het gebied van informatiebeveiliging is een regiegroep Beveiliging binnen B/CICT ingericht die minimaal 1 x per kwartaal bij elkaar komt.
2. Bij het inschatten van risico's op het gebied van informatiebeveiliging wordt o.a. rekening gehouden met incidentrapportages vanuit de processen POO, Dienstverlening, het subproces managen beveiliging van het proces Exploitatie. Ook wordt rekening gehouden met de uitkomsten van audits en onderzoeken door de proceseigenaar en de RAD. Ook wordt rekening gehouden met de vanuit het proces RM opgeleverde uitkomsten van de SNR-overleggen met partijen die B/CICT opdracht heeft gegeven om werkzaamheden uit te voeren mede ter dekking van bepaalde beveiligingsrisico's. Ook worden veranderende omgevingsfactoren in de analyse meegenomen.
3. Incidenten worden geanalyseerd en gecategoriseerd in:
   3.1. technische en organisatorische incidenten en
   3.2. incidenten die hun oorzaak vinden in het gedrag van mensen.
   Incidenten worden uitgezet bij de verantwoordelijke leidinggevende. Het verloop van de voortgang van afhandeling van deze incidenten wordt in het proces POO bewaakt en vastgelegd.

4. Het management zorgt voor de implementatie van de normen en/of maatregelen zoals in dit document beschreven of de maatregelen zoals deze door de regiegroep zijn bepaald. De maatregelen zijn gebaseerd op de normatiek zoals beschreven in dit document, het VBI/VBA en de resultaten en bevindingen van:
   - de regiegroep Beveiliging;
   - de analyse van de *beveiligings- en integriteitsincidenten*;
   - uitgevoerde interne procescontroles en TPM onderzoeken,
   - uitgevoerde interne controles op beveiligingsinstellingen van de *(ICT-)service*;
   - uitgevoerde onafhankelijke technical audits en certificeringsonderzoeken.

Norm

POO N-1-3 B/CICT	Om tot een beheerste afhandeling van *calamiteiten* te komen, is een crisisteam opgesteld.

Maatregelen

1. Het crisisteam is samengesteld uit leden van het managementteam van B/CICT
2. De werking van het crisisteam wordt geregeld in het crisismanagementplan.
3. Het crisismanagementplan wordt actueel gehouden.

Norm

POO N-1-4 B/CICT	Niet eerder onderkende risico's op het gebied van informatiebeveiliging en *integriteit* en opgetreden buitengewone voorvallen moeten worden gemeld. Daarna worden, afhankelijk van de aard en omvang daarvan, passende maatregelen ter voorkoming c.q. beperking genomen.

Maatregelen

1. *Risico's* voor zover deze niet adequaat worden bestreden en buitengewone voorvallen op het gebied van informatiebeveiliging en *integriteit* worden gemeld aan het verantwoordelijk management en de Beveiligingscoördinator. Deze risico's worden, eventueel met advies door de beveiligingscoördinator, door de verantwoordelijke manager afgehandeld.
2. Alle medewerkers worden door middel van publicaties op de hoogte gesteld van de opgestelde en afgesproken regels over hoe medewerkers om moeten gaan met buitengewone voorvallen zowel binnen de organisatie als (eventueel) buiten B/CICT.

Norm

POO N-1-5 B/CICT	In het proces POO wordt de eenheid van beleid op het gebied van *integriteit* en beveiliging bewaakt.

Maatregelen

1. Jaarlijks wordt aan het managementteam B/CICT (en/of daartoe in het leven geroepen regiegroepen) door de beveiligingscoördinator gerapporteerd over de voortgang en aard van de beheersing van de processen en de beveiligingsnormen en maatregelen en afhandeling van de eventueel geconstateerde bevindingen.
2. In deze rapportage zal tevens over de voortgang, aard en afhandeling van gemelde incidenten worden bericht.
3. Tevens zal, aan de hand van mogelijke bijstellingen van het Belastingdienstbeleid en genoemde rapportage, het B/CICT beleid worden afgestemd.

Richtlijn

POO R-2 B/CICT	*Binnen B/CICT dient op het gebied van informatiebeveiliging aan een aantal normen op het gebied van primaire functiescheidingen te worden voldaan.*

Risicoafweging

Het niet voldoen aan primaire functiescheidingen kan negatieve gevolgen hebben voor de informatiebeveiliging van gegevens en *ICT-Service*s .

Norm

POO N-2-1 B/CICT	De organisatie is ingericht zodanig dat functies, taken, bevoegdheden en verantwoordelijkheden transparant zijn belegd en bekendgemaakt.

Maatregelen

1. Per proces worden per *procesrol* de taken, bevoegdheden en verantwoordelijkheden, inclusief bijbehorende autorisatieprofielen en benodigde middelen, beschreven en actueel gehouden.
2. Bij het ontwerp van de organisatie wordt rekening gehouden met de vereiste controletechnische functiescheiding. Hierbij is het ‘‘need-to-know’’-principe gehanteerd.
3. Jaarlijks worden de per *procesrol* gedefinieerde autorisatierollen geëvalueerd en eventueel aangepast.
4. Er wordt een systeem voor de logische toegangsbeveiliging van de door B/CICT gebruikte software, applicaties en informatiesystemen gebruikt.
5. Ontheffingen van het gebruik van standaard bedrijfsmiddelen (onversleuteld lezen/schrijven, toestemming voor het gebruik van USB etc.) worden door de verantwoordelijke proceseigenaar inbegrepen in een verbijzonderd autorisatieprofiel, wat gekoppeld is aan een *procesrol*.
6. Medewerkers die uit hoofde van hun functie toegang hebben tot vertrouwelijke gegevens en/of privacy gevoelige informatie worden op regelmatige basis geïnformeerd over hun geheimhoudingsplicht.

Norm

POO N-2-2 B/CICT	Werkzaamheden die in een bepaalde combinatie leiden tot ongewenste risico’s, worden vermeden.

Maatregelen

1. In het proces PFC wordt bij het samenstellen van rolbeschrijvingen en de daaraan gekoppelde autorisatieprofielen een scheiding gemaakt tussen de uitvoerende-, beherende en beschikkende functie;
2. In het proces O&B wordt bij het samenstellen van autorisatieprofielen rekening gehouden met de scheiding tussen de logische omgevingen. Hierbij wordt ervoor zorggedragen dat de autorisatieprofielen van risicovolle *ICT-componenten*, in de ene logische omgeving geen invloed kunnen uitoefenen in de andere logische omgevingen;
3. In het proces EP wordt bij het autorisatieprofiel van medewerkers die door het management zijn aangewezen om privacy-gevoelige informatie te verwerken of in te zien rekening gehouden met het vertrouwelijke karakter van de aard van de werkzaamheden.
4. In het proces RM wordt er op toegezien dat er geen conflicterende rollen c.q. autorisatieprofielen bij dezelfde medewerker zijn/worden toegekend.
5. In het proces RM wordt bij het samenstellen van rolbeschrijvingen en de daaraan gekoppelde autorisatieprofielen een scheiding gemaakt tussen de uitvoerende- beherende en beschikkende functie m.b.t. salarismutaties en daaruit voortvloeiende betalingen.

6. In het proces POO wordt, bij het opstellen van de rolbeschrijvingen en de daaraan gekoppelde autorisatieprofielen voor de fysieke toegang tot ruimten rekening gehouden met de volgende uitgangspunten:
   6.1. toegang tot ruimten wordt gekoppeld aan de rol van een medewerker;
   6.2. medewerkers met een rol waarin bepaald is dat hun hoofdactiviteiten in één fysieke omgeving uitvoeren worden uitsluitend voor deze omgeving geautoriseerd;
   6.3. voor rollen waarbij toegang nodig is tot de *acceptatietest-* of *productieomgeving*, worden werkstations ter beschikking gesteld die zijn opgesteld in een ruimte afgescheiden van ontwikkelen/onderhouden van applicaties;
   6.4. rollen voor operationele beheertaken, worden in een afgescheiden ruimte uitgevoerd.

Richtlijn

POO R-3 B/CICT	*Indien, ondanks alle risicobeheersingsmaatregelen genoemd in het basis-beveiligingsniveau, er onverhoopt toch calamiteiten optreden dienen deze beheerst te worden afgehandeld.*

Risicoafweging

Het is belangrijk om de voortgang van de bedrijfsvoering onder vrijwel alle omstandigheden te waarborgen. In het basisbeveiligingsniveau is een groot aantal maatregelen genoemd om te anticiperen op mogelijke risico's. Er kunnen zich toch *calamiteiten* voordoen die grote inbreuk kunnen hebben op de bedrijfsvoering. Om de bedrijfsvoering zo veel mogelijk toch doorgang te laten vinden worden hieronder een aantal bijzondere maatregelen genoemd. Voor de maatregelen op het gebied van calamiteiten met gebouwen en personeel wordt ook verwezen naar RM R-3.

Norm

POO N-3-1 B/CICT	De continuïteit van de bedrijfsvoering van B/CICT is gewaarborgd.

Maatregelen

1. De voor de continuïteit van de bedrijfsvoering relevante tooling is inzichtelijk en met de leverancier zijn afspraken gemaakt over de continuïteit.
2. In het SNO met B/CA afspraken gemaakt over continuïteit van het systeem voor de primaire bedrijfsvoering van B/CICT.
3. De in de SNO's vastgelegde afspraken voldoen minimaal aan de voorschriften en richtlijnen die zijn vastgelegd in het Handboek Calamiteitenplan Belastingdienst (HCB).
4. Er is een continuïteitsplan waarin wordt geregeld hoe de continuïteit van de bedrijfsvoering wordt gewaarborgd na een optredende *calamiteit*.

Richtlijn

POO R-4 B/CICT	*Het gebruik van software en informatiesystemen is alleen toegestaan binnen kaders.*

Risicoafweging

Werkzaam bij het automatiseringsbedrijf van de Belastingdienst zijn de medewerkers van B/CICT de hele dag in de weer met voor de Belastingdienst ontwikkelde applicaties die worden samengesteld uit zelf samengestelde programmatuur en ingekochte software van derden. Door de normering vermeld in dit handboek is het gebruik van software en informatiesystemen gebonden aan zeer strikte regels. Zie hiervoor o.m. de uitgangspunten voor het procesontwerp in de normen procesbeheersing en in dit handboek de normering voor O&B en exploitatie. Het proces RM zorgt, gekoppeld aan de *procesrollen*, voor de uitgifte

van de middelen waarmee de medewerker van B/CICT werkt en spreekt de medewerkers aan op het moment dat zij zich niet houden aan de kaders die hierover zijn afgesproken. Een aparte categorie wordt gevormd door de informatiesystemen die B/CICT gebruikt voor haar eigen bedrijfsvoering. De *integriteit* van de bestanden binnen deze informatiesystemen zijn belegd bij het management onder wiens verantwoordelijkheid de mutaties in bestanden veroorzaken. Hieronder worden de norm beschreven voor zover deze van toepassing zijn op de uitgegeven software aan medewerkers van B/CICT en het gebruik van de informatiesystemen ter ondersteuning van de bedrijfsvoering van B/CICT.

Norm

POO N-4-1 B/CICT	Informatiesystemen worden geïmplementeerd en gebruikt conform de voorschriften.

Maatregelen

1. Voor het toezien op het gebruik van de ondersteunende systemen voor de bedrijfsvoering, de Beheer infrastructuur en de Systeemontwikkelingsinfrastructuur zijn regiegroepen ingericht. Deze bestaan uit voor deze gebieden verantwoordelijke managers en deskundigen.
2. Regiegroepen zorgen voor de opdrachtverstrekking voor het aanpassen en het implementeren van aangepaste informatiesystemen.
3. De lijst met software en/of applicaties waarvoor medewerkers van B/CICT geautoriseerd kunnen worden, wordt jaarlijks vastgesteld door de proceseigenaar POO.
4. Gebruik van software en/of applicaties buiten de vastgestelde lijst van software en/of applicaties is niet toegestaan.
5. Gebruik van illegale software wordt gezien als een *integriteitsincident*, passende maatregelen worden getroffen aan medewerkers die zich hieraan schuldig maken.

2.2.2 Account management

Richtlijn

AM R-1 B/CICT	*Afspraken t.a.v. informatiebeveiliging met betrekking tot het ontwikkelen, beheren en exploiteren van ICT-Services dienen integraal onderdeel te zijn van opdrachten en overeenkomsten.*

Risicoafweging

Indien geen afspraken t.a.v. *informatiebeveiliging* met opdrachtgevers worden gemaakt, bestaat het risico dat de opdrachtgever impliciet aanneemt dat eventuele risico's op het gebied van *informatiebeveiliging* zijn afgedekt, terwijl dit niet het geval hoeft te zijn.

Norm

AM N-1-1 B/CICT	In het Programma van eisen (PvE) worden de informatiebeveiligingseisen opgenomen die de klant-opdrachtgever stelt aan de te realiseren *ICT-Service*.

Maatregelen

1. De informatiebeveiligingseisen die in het algemeen gesteld worden aan *ICT-Service*s, zijn afgestemd met B/CPP. Totdat de opdrachtgever anders bepaalt worden als uitgangspunt voor de beveiliging van te bouwen infrastructuur en applicaties de voorschriften beveiliging infrastructuur (VBI) en de voorschriften beveiliging applicaties (VBA) gehanteerd.
2. Bij het accepteren van het PvE wordt er op toegezien dat in het PvE eisen op het gebied van informatiebeveiliging zijn opgenomen.
3. In het PvE wordt beschreven welke gebruikershandelingen moeten worden gelogd gedurende welke bewaartermijn in verband met eventuele toekomstige integriteitsonderzoeken.

Norm

AM N-1-2 B/CICT	Over door B/CICT geconstateerde risico's met betrekking tot te realiseren of gerealiseerde *ICT-Services* worden met de opdrachtgever afspraken gemaakt .

Maatregelen

1. CICT beoordeelt de ICT-services op mogelijke beveiligingsrisico's.
2. Geconstateerde beveiligingsrisico's met betrekking tot ICT-services worden geregistreerd inclusief de afspraken, die worden gemaakt om risico's op te heffen dan wel te accepteren.
3. In het Plan van Aanpak worden de gemaakte afspraken over de beveiligingsrisico's opgenomen.
4. Afspraken om (in een later stadium) maatregelen te treffen worden bewaakt op naleving.
5. Als de opdrachtgever geen specifieke aanvullende wensen heeft op het VBI/VBA t.a.v. beveiliging wordt hiervan separaat een aantekening in de opdracht gemaakt.

Norm

AM N-1-3 B/CICT	In de SNO met de klant-opdrachtgever wordt als onderdeel van de afspraken opgenomen: 1. Het overeengekomen *beveiligingsniveau* betreffende de (ICT-) *Service*; 2. De wijze van rapportage over de handhaving van het overeengekomen *beveiligingsniveau*.

Maatregelen

1. In de SNO wordt expliciet een gewenst beveiligingsniveau opgenomen en de wijze en frequentie waarop hierover wordt gerapporteerd.
2. Eventueel extra gewenste maatregelen specifiek gericht op de dienstverlening behorend bij een (ICT-) *Service* worden expliciet overeengekomen en in de SNO beschreven.
3. Indien door B/CICT geconstateerd wordt dan wel een vermoeden bestaat dat er sprake is van schending van vertrouwelijkheid en/of *integriteit* van gegevens en/of gegevensverwerking behorend bij de desbetreffende *ICT-Service* wordt hiervan door B/CICT onmiddellijk melding gedaan bij de opdrachtgever. B/CICT zal hierover tevens apart schriftelijk rapportage uitbrengen aan opdrachtgever.
4. B/CICT zal de resultaten over het afgesproken beveiligingsniveau conform SNO afspraken rapporteren.

2.2.3 Architectuur

Richtlijn

AR R-1 B/CICT	*De aspecten vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid dienen integraal onderdeel uit te maken van de architectuurproducten.*

Risicoafweging

Zonder grondige voorbereiding bestaat het risico dat *ICT-Service*s onjuist werken of dat medewerkers er niet goed mee om gaan. Als gevolg daarvan kan de informatievoorziening fouten bevatten, het operationele proces ernstig worden verstoord , de privacy van individuele Belastingplichtigen worden geschonden en/of het imago van de Belastingdienst worden aangetast.

Norm

AR N-1-1 B/CICT	In het architectuurproces zijn waarborgen aanwezig dat de aspecten vertrouwelijkheid, *integriteit*, beschikbaarheid en controleerbaarheid een integraal onderdeel uitmaken van de (*ICT-)Services* die worden beschreven in de architectuurproducten.

Maatregelen

1. De met B/CPP overeengekomen informatiebeveiligingseisen (zoals b.v. de Voorschriften Beveiliging Infrastructuur, de Voorschriften Beveiliging Applicaties, voorschriften op het gebied van *integriteit*, beschikbaarheid en controleerbaarheid) zijn verder uitgewerkt in een generiek kader, de domeinarchitectuur Beveiliging.
2. Bij het uitwerken van de domeinarchitecturen per *(ICT-) Service* is rekening gehouden met de kaders die in de domeinarchitectuur Beveiliging worden gesteld.
3. Er is geanalyseerd welke *(ICT-)services* een bijzonder belang voor de logische toegang tot belastingdienstgegevens vertegenwoordigen. Op grond hiervan is in de betreffende domeinarchtectuur aangegeven voor welke *TIS-componenten* in de technische documentatie instructies opgenomen moeten worden voor het controleren van beveiligingsinstellingen en het signaleren van afwijkend gebruik (Beveiligingsrisico's).
4. Autorisaties voor functies in ICT-services worden zoveel mogelijk gegroepeerd zodat de dynamiek in *(ICT-)service*s, processen, functies en organisaties niet tot onaanvaardbare, extra onderhoudswerkzaamheden leidt.

AR N-1-2 B/CICT	In het architectuurproces zijn waarborgen aanwezig om de architectuurproducten en de hiervan afgeleide producten te controleren op de realisatie van de afgesproken beveiligingskaders.

Maatregelen

1. Bij het opstellen van het basis- en technische ontwerp wordt er op toegezien dat de beveiligingsmaatregelen zoals beschreven in de domeinarchitecturen worden verwerkt.
2. In de regiegroep architectuurcontrol wordt er op toegezien dat de kaders en maatregelen op het gebied van beveiliging in de domeinarchitecturen en basis- en technische ontwerpen (inclusief teststrategie) worden nageleefd.

2.2.4 O&B

Richtlijn

O&B R-1 B/CICT	*Er dient voorkomen te worden dat in het O&B proces oneigenlijk gebruik wordt gemaakt van vertrouwelijke data.*

Risicoafweging

Het risico bestaat dat door oneigenlijk gebruik van gegevens tijdens het ontwikkelen en beheren van (ICT-) *Services*, de Belastingdienst wordt geschaad.

Norm

O&B N-1-1 B/CICT	Het is niet toegestaan productiegegevens te gebruiken die herleidbaar zijn naar *vertrouwelijke gegevens*.

Maatregelen

Ingeval er met kopieën van productiegegevens (b.v. in de *acceptatie- of testomgeving)* wordt gewerkt, zijn de volgende maatregelen getroffen:

1. De privacybepalende gegevens in de kopieën van de productiedata worden volgens een onvoorspelbaar patroon verschoven en als testgegevens herkenbaar gemaakt

of

2. Als desondanks aan de *gegevenseigenaar* schriftelijke toestemming wordt gevraagd een kopie van productiegegevens te mogen gebruiken voor test- of beheerdoeleinden (het oplossen van incidenten, database beheer etc.) dient met de *gegevenseigenaar* te worden besproken welke speciale aanvullende maatregelen er voor risicobeperking worden genomen. De *beveiligingscoördinator* van B/CICT toetst vooraf of deze maatregelen afdoende zijn en of de maatregelen juist worden toegepast.

Richtlijn

O&B R-2 B/CICT	*(ICT-)services die worden voortgebracht, dienen te voldoen aan generieke informatiebeveiligingskaders en daarvan afgeleide specifieke basisontwerpen voor informatiebeveiliging.*

Risicoafweging

Als bij de voortbrenging van *(ICT-)service*s onvoldoende rekening wordt gehouden met informatiebeveiligingseisen zoals verwoord in de voorschriften beveiliging applicaties (VBA) en voorschriften beveiliging infrastructuur (VBI), dan kunnen er tijdens het gebruik en de exploitatie van de *(ICT-)services* informatiebeveiligingsrisico's ontstaan die onvoldoende worden beheerst. Onderstaande normen zijn aanvullend op het VBA / VBI, en worden uiteindelijk hierin opgenomen.

Norm

O&B N-2-1 B/CICT	*(ICT-)services* worden ontworpen conform de informatiebeveiligingskaders.

Maatregelen

1. Bij het basis- en technisch ontwerp van de *(ICT-)service* worden de beveiligingskaders zoals beschreven in de domeinarchitectuur voor de *(ICT-)service* gehanteerd.
2. In het ontwerp zijn maatregelen m.b.t. de aspecten vertrouwelijkheid, *integriteit*, beschikbaarheid en controleerbaarheid opgenomen.

3. Voor ICT-services die van invloed zijn op de geldstroom dient in het ontwerp en de testspecifiaties zichtbaar rekening te worden gehouden met het beperken van het risico dat oneigenlijke programmatuurregels (i.v.m. afrondingen) worden toegevoegd.
4. De testspecificaties en testplan voor de *(ICT-)services* zijn in het ontwerp uitgewerkt in een samenhangende testtrategie (b.v. aan de hand van het Kwaliteitseisenmodel (KEM))
5. In het ontwerp dienen aanwijzingen te zijn opgenomen hoe eventuele handmatige bestands- en *gegevensmanipulaties* tijdens productie worden voorkomen. In het geval dat bestands- en/of *gegevensmanipulaties* door een optredend incident noodzakelijk zijn, dienen hiervoor aanwijzingen in de *(ICT-)service* te worden opgenomen.
6. In het ontwerp is beschreven welke directe en indirecte licenties van ingekochte software worden gebruikt in de *(ICT-)service* en hoe het verbruik hiervan wordt geregistreerd.

Norm

O&B N-2-2 B/CICT	In het ontwerp is rekening gehouden met de eisen m.b.t. het monitoren van de *(ICT-)services* in de productieomgeving.

1. In de aanwijzingen geleverd bij de *(ICT-)service* wordt beschreven op welke wijze, met welke frequentie, binnen welke grenzen en met welke tooling in de productieomgeving monitoring op beveiligingsrisico's moet plaatsvinden. Deze aanwijzingen hebben onder andere betrekking op door geautomatiseerde systemen gesignaleerde:
   1.1.1. *type* beveiligingsrisico's;
   1.1.2. afwijkingen van gewenst gebruik van functies zoals dit is vastgelegd in de bij de *(ICT-)service* behorende documentatie zoals meldingen op grond van intrusion detection, verkeerd gebruik van autorisaties, licentiegebruik en/of contentscanning;
   1.1.3. meldingen van gebruik van gevoelige functies of data.

Norm

O&B N-2-3 B/CICT	In het ontwerp is rekening gehouden met de eisen m.b.t. het aanbrengen van autorisaties en autorisatiegroepen in de *(ICT-)services* in de productieomgeving.

1. Het ontwerp van de groepsstructuur houdt rekening met het opvoeren van groepen in de exploitatieomgeving.
2. Per autorisatiegroep wordt een logische omschrijving gegeven van de aard van de erin opgenomen autorisaties, waarvan een actuele documentatie kan worden bijgehouden.

Norm

O&B N-2-4 B/CICT	In het acceptatieproces worden de risico's op het gebied van beveiliging van de (ICT-) service getoetst.

Maatregelen

1. De teststrategie zoals beschreven bij het ontwerp wordt aantoonbaar uitgevoerd tijdens het Acceptatieproces, verslagen hiervan zijn ter inzage voor belanghebbenden.
2. De aspecten vertrouwelijkheid, *integriteit*, beschikbaarheid en controleerbaarheid zijn, ook als ze geen onderdeel uitmaken van de testspecificaties, getoetst voor de (ICT-) service in exploitatie wordt genomen.

Richtlijn

O&B R-3 B/CICT	*De overdracht van ontwikkelde ICT-services naar uiteindelijke productieomgeving vindt beheerst plaats.*

Risicoafweging

De overdracht van ontwikkelde programmatuur tussen verschillende omgevingen dient beheerst plaats te vinden omdat anders het risico wordt gelopen dat er ongecontroleerd aanpassingen mogelijk zijn.

Norm

O&B N-3-1 B/CICT	Het *programmatuurbeheersysteem* voorziet in een gescheiden *ontwikkel-*, *acceptatie-, test-* en *productieomgeving*. De overdracht tussen deze omgevingen wordt gecontroleerd en geregistreerd.

Maatregelen

1. Er zijn voor de verschillende *platformen* beheersystemen, die o.m. de volgende registraties verzorgen:
   - de status (ontwikkeling, test, acceptatie, productie) van de release en release-attributen;
   - de versieaanduiding van de release en release-attributen;
   - de ICT-release aanduiding van de doelsystemen waarop de toepassingsprogrammatuur van een release draait;
   - de samenstelling van een release naar release-attributen;
   - de releases, waarin een attribuut voorkomt;
   – logging van wijzigingen in releases incl. uitvoerder daarvan.
2. Naar de *acceptatie-, test en productieomgeving* overgedragen programmatuur kan niet meer gewijzigd worden. Het is uitsluitend mogelijk deze programmatuur door nieuwe versies te vervangen als deze in de *ontwikkel*omgeving zijn vervaardigd.
3. Bij het proces ICI wordt voor de aan dit proces aangeboden *(ICT-)services* vastgesteld dat geen ontwikkeltools, compilers of broncode worden aangeboden voor implementatie in de *productie- acceptatie- en testomgeving*, zodat in deze omgevingen geen aanpassingen van de programmatuur kan plaats vinden.
4. Het beheersysteem beperkt de bevoegdheden om operationele programmabibliotheken bij te werken tot bevoegde medewerkers.
5. Oude versies van bronprogramma's worden gearchiveerd met duidelijke vermelding van de exacte datum en tijd waarop zij operationeel waren en inclusief alle ondersteunende programmatuur, taakbesturing, gegevensdefinities en procedures.
6. Overdrachten van programmatuurversies tussen de verschillende omgevingen worden geregistreerd.
7. De omgeving die wordt gebruikt voor het onderzoeken van nieuwe ontwikkelingen op het gebied van informatietechnologie ("laboratorium") is op geen enkele wijze verbonden met de *ontwikkel-, acceptatietest- en productieomgeving.*

Richtlijn

O&B R-4 B/CICT	*(ICT-)services die worden beheerd dienen te voldoen aan de maatregelen afkomstig uit generieke informatiebeveiligingskaders en daarvan afgeleide specifieke basisontwerpen voor informatiebeveiliging.*

Risicoafweging

Tijdens het beheer van de (ICT-)services dienen de aanwijzingen bij de (ICT-)services te worden opgevolgd. Deze aanwijzingen leiden tot acties rond monitoring. Als onvoldoende continue gemonitord wordt op beveiligingsinstellingen kunnen er tijdens het gebruik en de exploitatie informatiebeveiligingsrisico's ontstaan die onvoldoende worden beheerst. Als gedurende de werking van *(ICT-)service*s inbreuk dreigt te ontstaan op het gewenste niveau van beveiligingmoeten maatregelen op korte en/of langere termijn leiden tot een herstel van het niveau van beveiliging.

O&B N-4-1 B/CICT	De ICT-servicebeheerder bewaakt het niveau van beveiliging gedurende de exploitatie van de ICT-service

Maatregelen

1. Beveiligingsincidenten en/of optredende events worden door de ICT-servicebeheerder geregistreerd, afgewogen en opgelost.
2. Beveiligingsincidenten en voorvallen worden gerapporteerd aan het proces accountmanagement m.b.v de *Service* niveau rapportage.

Norm

O&B N-4-2 B/CICT	(ICT-)services worden gemonitord volgens de gestelde normen. Afwijkingen van deze norm worden door de ICT service beheerder op correcte wijze afgedaan.

Maatregelen

1. Monitoring vindt plaats op basis van de aanwijzingen die bij de oplevering van de geaccepteerde (ICT-) service zijn geleverd.
2. In de bij de (ICT-)service behorende technische documentatie is vastgelegd:
   2.1. Hoe de beveiligingsinstellingen moeten worden ingesteld en met welke frequentie en welke tooling deze instellingen voor toetsing moeten worden aangeboden, dan wel automatisch wordt gecontroleerd.
   2.2. Hoe het licentiegebruik wordt vastgesteld c.q. gevolgd en tot welke grenzen er gebruik mag worden gemaakt van de directe- of indirecte licenties.
3. Bij het monitoren wordt onderscheid gemaakt naar bevindingen, die in de gebruikersorganisatie moeten worden afgehandeld (functioneel beheer) en de bevindingen die betrekking hebben op B/CICT zelf (product- en/of servicebeheer).

O&B N-4-3 B/CICT	De mate waarin risico's worden gelopen, is bepalend voor de frequentie van de controle op beveiligingsinstellingen van de *(ICT-)services.*

Maatregelen

1. De ICT service beheerder verandert de frequentie van de controle op beveiligingsinstellingen (en/of licenties) van de *(ICT-)services* indien aard en omvang van de afwijkingen dit rechtvaardigt.
2. De ICT service beheerder vraagt in voorkomende gevallen om advies van de *Security Officer*. Deze kan tevens ongevraagd advies op dit punt geven op grond van de toezichthoudende functie die hij in dit kader vervult.

Norm

O&B N-4-4 B/CICT	Het oplossen van problemen mag het beveiligingsniveau zoals geformuleerd in dit document of aanvullende informatiebeveiligingseisen per afzonderlijke (ICT-) service niet aantasten.

Maatregelen

1. Als problemen alleen opgelost kunnen worden door het tijdelijk opheffen of versoepelen van *informatiebeveiligingsmaatregelen*, wordt dit altijd goedgekeurd door het verantwoordelijke management.
2. Aanvullend getroffen maatregelen worden na toestemming (vooraf of achteraf) met de klant inclusief de hieraan voorafgaande risicoanalyse vastgelegd. Door het management wordt toegezien op naleving van deze maatregelen.

O&B N-4-5 B/CICT	Het handmatig wijzigen van gegevens en/of bestandsmanipulaties is niet toegestaan tenzij hier expliciet toestemming voor is gegeven.

Maatregelen

1. De (ICT-)servicebeheerder wordt, indien onverhoopt noodzakelijk, altijd vooraf op de hoogte gebracht van voorgenomen wijzigingen die met de hand moeten worden aangebracht.
2. De (ICT-)servicebeheerder bepaalt per situatie de risico's en impact van de voorgenomen wijzigingen en bespreekt deze met het management.
3. De (ICT-)servicebeheerder zal zo veel mogelijk de optredende incidenten op het gebied van bestands- en *gegevensmanipulaties* herstellen en voorkomen door hiervoor in het probleembeheer proces maatregelen te treffen.

2.2.5 Demand management

Richtlijn

DM R-1 B/CICT	*Bij inkoop van (onderdelen van) (ICT-)services dienen met de leverancier zodanige afspraken t.a.v. informatiebeveiliging te worden gemaakt dat het Basis Beveiligings Niveau niet wordt aangetast.*

Risicoafweging

Het niet maken en vastleggen van afspraken op het gebied van *informatiebeveiliging* bij de inkoop van (onderdelen van) *ICT-Services*, waarbij het HIB B/CICT uitgangspunt is, kan leiden tot ongewenste negatieve gevolgen voor het *Basis Beveiligings Niveau*.

Norm

DM N-1-1 B/CICT	De inkopende organisatie dient te borgen dat de aan te schaffen *(ICT-)services* met een bijzonder belang voor het logisch toegangspad tot klantgegevens geen andere functies bevat dan beschreven staat in de bijgevoegde documentatie.

Maatregelen

1. In de Request for Proposals en Publicaties wordt op aanwijzing van O&B (volgens voorschrift van architectuur) het afgeven van een *integriteit*sverklaring als vraag opgenomen.
2. Door middel van een *integriteitsverklaring* borgt de leverancier dat de aan te schaffen *(ICT-)services* , met een bijzonder belang voor het logisch toegangspad tot klantgegevens, geen andere functies bevatten dan beschreven staan in de bijgevoegde documentatie.

Norm

DM N-1-2 B/CICT	Indien één van de *diensten* of activiteiten van B/CICT wordt uitbesteed dienen de leveranciers van de uitbestede *diensten* of activiteiten te voldoen aan de normen zoals deze in het HIB B/CICT zijn opgenomen.

Maatregelen

1. In de Request for Proposal en Publicaties wordt bij het uitbesteden van exploitatiediensten standaard een eis opgenomen inzake het controlerecht, waarbij:
   1.1. leverancier eenmaal per jaar zal zorgen voor een mededeling van een onafhankelijke deskundige, waaruit blijkt dat leverancier zowel in opzet, bestaan als werking gedurende het jaar voldoet aan de afspraken die worden overeengekomen op het gebied van vertrouwelijkheid, *integriteit* en beschikbaarheid. Deze afspraken mogen geen afbreuk doen aan het Basis Beveiligings Niveau, zoals in dit document is verwoord.
   1.2. B/CICT gerechtigd is de hiervoor bedoelde mededelingen te laten reviewen.
   1.3. B/CICT gerechtigd is tussentijds een kwaliteitstoetsing ten aanzien van de verlening van *Services* door leverancier op basis van de overeenkomst alsmede ten aanzien van vertrouwelijkheid, *integriteit* en beschikbaarheid van de door leverancier ter beschikking gestelde *Services* door een onafhankelijke deskundige te laten uitvoeren;
   1.4. leverancier zich bereid verklaart mee te werken aan een dergelijke voorgenomen toetsing en de door de deskundige aangegeven aanbevelingen ter verbeteringen, voor zover redelijkerwijze mogelijk, uit te voeren.
2. In de Request for Proposal en Publicaties bij ontwikkel en onderhoudsdiensten wordt standaard een eis opgenomen inzake geheimhouding en informatiebeveiliging, waarbij:

2.1. leverancier alle informatie en/of data van B/CICT op welk medium dan ook aan geen ander beschikbaar zal stellen of openbaar maken dan aan de door B/CICT aangewezen personen of organisaties;
2.2. leverancier zich verbindt ten aanzien van de data van B/CICT die onder hem berusten, waaronder ook begrepen transporten, het overeengekomen niveau van informatiebeveiliging in acht te nemen ter voorkoming van diefstal of onbevoegde wijziging en/of kennisneming daarvan;
2.3. leverancier alle kennis omtrent toegangsregels en –codes welke in verband met de uitvoering van de *Services* worden gehanteerd, geheim zullen houden en alle benodigde voorzieningen zullen treffen teneinde te voorkomen dat deze kennis in handen van onbevoegden raakt;
2.4. broncode kan alleen na schriftelijke toestemming door de beveiligingscoördinator van B/CICT ter beschikking worden gesteld aan derden. De beveiligingscoördinator zal eisen stellen aan de manier waarop de broncode aan de leverancier ter beschikking wordt gesteld en de wijze waarop deze broncode wordt geretourneerd c.q. vernietigd na beëindiging van het doel waarvoor deze broncode ter beschikking is gesteld. Ook zal de beveiligingscoördinator er op toezien dat gebruik door derden van data en/of programmaregels uitsluitend conform het beveiligingsbeleid van de Belastingdienst gebeurt.
2.5. leverancier ervoor zorgt dat haar personeel en door haar ingeschakelde derden schriftelijk tot geheimhouding zijn verplicht;
2.6. leverancier toezegt dat indien geconstateerd wordt dan wel een vermoeden bestaat dat er sprake is van schending van vertrouwelijkheid, *integriteit* en beschikbaarheid, hiervan door leverancier onmiddellijk melding wordt gedaan bij B/CICT en leverancier hierover tevens apart schriftelijk rapportage zal uitbrengen aan B/CICT.
2.7. In alle overige gevallen houdt de leverancier zich aan de beveiligingseisen zoals in dit document zijn opgenomen.

3. Bovengenoemde eisen dienen uiteindelijk hun weerslag te vinden in het af te sluiten contract.
4. In geval van remote onderhoud/beheer worden met leveranciers contractuele afspraken gemaakt inzake:
   4.1. het bijhouden van een logboek waaruit blijkt wanneer, hoe lang, waarom en door wie; beheerhandelingen zijn verricht;
   4.2. de regels bij het inloggen en het usermanagement;
   4.3. de regels omtrent fysieke toegang, ook en met name buiten kantoortijden
   4.4. het vernietigen van gegevens indien leveranciers opslagmedia ter beschikking krijgen bij het afstoten van *(ICT-)services.* .
5. In de mantelovereenkomst met leveranciers van extern personeel worden de volgende regelingen m.b.t. het te werkstellen personeel vastgelegd:
   5.1. de geheimhoudingsverplichting
   5.2. de identificatieplicht
   5.3. verklaring omtrent gedrag
   5.4. door B/CICT of door een door B/CICT aangestelde onafhankelijke, derde partij kan controle worden uitgevoerd op de naleving van bovenstaande regelingen door de leverancier.

Norm

DM N-1-3 B/CICT	Indien contracten worden afgesloten met leveranciers dienen waarborgen opgenomen te worden m.b.t. data van de Belastingdienst.

Maatregelen

1. Bij het buiten gebruik stellen van ICT-apparatuur, wordt geregeld dat het onherstelbaar wissen van vaste schijven conform de regeling materieel beheer Rijksoverheid 2006, wordt uitgevoerd.