Is functiescheiding AO of IB volgens ISA? En wat zijn de gevolgen voor de auditaanpak?

http://www.accountancyvanmorgen.nl/2016/05/09/is-functiescheiding-ao-ib-volgens-isa-en-gevolgen-auditaanpak/

9 MEI 2016 DOOR ACCOUNTANCY VANMORGEN

Dr Niels van Nieuw Amerongen RA is partner van opleidings- en adviesbureau V&A en is associate professor Auditing & Assurance bij Nyenrode Business Universiteit.

Drs Alex Boxum RA EMITA is directeur Opleidingen en Compliance van opleidings- en adviesbureau V&A.

Stel u bent als accountant betrokken bij de wettelijke controle van een hotel. Een casus die ondermeer staat beschreven in één van de recente AFM boetebesluiten[1]. Ten aanzien van deze wettelijke controle besteedt de accountant terecht aandacht aan de controle op de juistheid en volledigheid van de omzet uit verhuur van hotelkamers. Hij onderkent een significant risico ten aanzien van de volledigheid.

Wij kennen het dossier niet maar uit het boetebesluit blijkt dat de accountant hiertoe *'een combinatie van systeem- en gegevensgerichte werkzaamheden heeft uitgevoerd om de juistheid en volledigheid van de omzet vast te stellen. De systeemgerichte werkzaamheden bestaan uit de vaststelling van de effectieve werking van de functiescheidingen'.*
De AFM beschrijft vervolgens de werkzaamheden van de accountant ten aanzien van de controletechnische functiescheiding als volgt. '*Ter vaststelling van de effectieve werking van de functiescheidingen binnen [D] heeft de externe accountant de gebruikerslijsten van vier geautomatiseerde systemen in het controledossier opgenomen'.*
Maar de AFM concludeert dat de accountant meer systeemgerichte controlewerkzaamheden moest verrichten ten aanzien van de werking van de controletechnische functiescheiding. Een citaat: '*Daarmee heeft de externe accountant onvoldoende controlewerkzaamheden uitgevoerd om de effectieve werking van de functiescheidingen binnen [D] vast te stellen, terwijl hij daarop in zijn verdere controle ten aanzien van de ————- wel heeft gesteund.'.*

Interessant is de constatering dat de AFM vindt dat de effectieve werking van de functiescheiding vastgesteld moet worden.
In onze OKB en reviewpraktijk zien we nogal eens controledossiers waar de werkzaamheden ten aanzien van de functiescheiding beperkt is tot het vaststellen welke functiescheidingen bestaan en in hoeverre deze in opzet toereikend zijn. In dergelijke gevallen rijst de vraag of het inderdaad, zoals de AFM stelt, noodzakelijk is om ook de effectieve werking van functiescheiding gedurende de controleperiode vast te stellen.
Dit onderwerp is relevant mede doordat in het rapport 'In het Publiek Belang – Het kan echt beter!'[2] in maatregel 4.4 wordt opgeroepen tot een bredere focus op het ontdekken en adequaat 'omgaan met' fraude, onder meer om beter aan te sluiten op de verwachtingen van de stakeholders. De aloude discrepantie tussen de verantwoordelijkheden van de accountant enerzijds en anderzijds de verwachtingen van het

maatschappelijk verkeer dat accountants fraudes voorkomen en signaleren maakt de stap naar controletechnische functiescheiding klein. Immers: juist de tegengestelde belangen binnen de cliëntomgeving dienen ter voorkoming van fraude. Hoe diepgaand dient de aandacht van de accountant te zijn voor de werking van de controletechnische functiescheiding?
Deze vraag is tenslotte ook relevant omdat in de AFM rapporten 2013 (next nine-, NBA-, en SRA accountantsorganisaties) en 2014 (Big 4 accountantsorganisaties) relatief veel aandacht wordt besteed aan het onderwerp functiescheiding in het kader van het vaststellen van de volledigheid van de opbrengstverantwoording. Een tekortkoming in het controledossier op het punt van onvoldoende gedocumenteerde functiescheiding leidt daarmee al snel tot een onvoldoende dossier. In dit artikel bekijken we deze vraag vooral vanuit de Controlestandaarden. Die zijn immers primair de norm waaraan controledossiers moeten voldoen.

COS 315 Inzicht in de entiteit

We nemen ons vertrekpunt in COS 315 omdat dit binnen de Controlestandaarden de plaats is waar je het onderwerp Functiescheiding zou verwachten, want deze Standaard gaat over het verwerven van inzicht in de entiteit. Een eerste ‘dingetje’ dat opvalt is dat de term Functiescheiding niet voorkomt onder de kopjes Doelstellingen, Definities, respectievelijk Vereisten. De term Functiescheiding komt in totaal negen keer voor in COS 315. De eerste keer in toelichting A56.

Functiescheiding en kleinere entiteiten

Deze A56-paragraaf bevat overwegingen specifiek voor de controle van kleinere entiteiten. Het is op zich niet verrassend dat het juist bij dit onderwerp over functiescheiding gaat. Immers, bij kleinere entiteiten heeft de ondernemingsleiding – praktisch gezien – minder mogelijkheden om functiescheiding te creëren. Wel enigszins verrassend is hier de opmerking dat het toezicht door de eigenaar-bestuurder de beperkte mogelijkheden van functiescheiding kan compenseren. Hier staat dan wel weer in A57 tegenover dat de eigenaar-bestuurder in een dergelijke situatie meer mogelijkheden heeft voor het doorbreken van de interne beheersing. Enerzijds dus een verlaagd frauderisico, anderzijds dus een verhoogd frauderisico in deze setting. Deze overwegingen worden in A84 nog eens herhaald, alsof de standard setter wil zeggen: ‘houdt u er alstublieft wel voldoende rekening mee…’. We schieten nog niet echt op.

Relevante interne beheersing en informatietechnologie

We scrollen door naar A62. Deze A-paragraaf staat in het kader van handmatige en geautomatiseerde elementen van interne beheersing. Uit A62 kun je afleiden dat geautomatiseerde interne beheersing doorgaans sterker is dan handmatige interne beheersing. In totaal worden voor deze stelling zes redenen gegeven. De zesde reden is: een verbeterde mogelijkheid om effectieve functiescheiding te bereiken door beveiligingsmaatregelen te implementeren in toepassingen, databanken en besturingssystemen. Hieruit kunnen we alvast twee conclusies trekken:

- Functiescheiding is een element van interne beheersing;
- Functiescheiding kan bestaan uit handmatige (hier bedoeld als ‘fysieke’) respectievelijk geautomatiseerde functiescheiding. Dit laatste wordt ook wel logische toegangsbeveiliging genoemd.

Tot zover kun je nog zeggen dat functiescheiding in COS 315 vooral gezien wordt als *aanknopingspunt* om bij de controle op te kunnen steunen, en daarmee controlerisico’s te beperken. Echter, als we doorlezen in A63 zien we al snel dat ook sprake kan zijn van *extra risico’s* voor de accountant, namelijk wanneer IT medewerkers toegangsrechten krijgen die verder gaan dan die ze voor hun taken nodig hebben. Hierdoor wordt functiescheiding feitelijk tenietgedaan.

Interne beheersingsactiviteiten

Wanneer we nog weer verder speuren in COS 315 komen we uiteindelijk uit in een gedeelte dat gaat over de componenten van interne beheersing (COSO-componenten). A96 start eerst met een definitie van interne beheersingsactiviteiten: 'Interne beheersingsactiviteiten zijn de beleidslijnen en -procedures die ervoor helpen te zorgen dat de instructies van het management worden uitgevoerd. Interne beheersingsactiviteiten, hetzij in IT-systemen, hetzij in handmatige systemen, hebben verschillende doelstellingen en worden op verschillende organisatie- en functieniveaus uitgevoerd.' Beleidslijnen en beleidsprocedures. Dat klinkt als AO, als randvoorwaarden voor het effectief doen functioneren van het stelsel van interne beheersing. Maar, diezelfde A96 noemt dan vijf voorbeelden van interne beheersingsactiviteiten:

- Autorisatie
- Prestatiebeoordelingen
- Informatieverwerking
- Fysieke interne beheersingsmaatregelen
- Functiescheiding

OK, dus: Functiescheiding is een interne beheersingsactiviteit, en geen interne beheersingsmaatregel, want deze laatste wordt onderscheiden van functiescheiding in de opsomming.

Nogmaals IB componenten

Het lijkt allemaal nogal verwarrend. Toch valt dat wel mee. COS 315 bevat een bijlage 1 die op deze problematiek nog wat verheldering verschaft:

- Fysieke interne beheersingsmaatregelen bestaan uit:
  - Fysieke beveiliging van activa
  - Autorisatie voor de toegang tot computerprogramma's en gegevensbestanden
  - Periodieke tellingen en vergelijkingen met bedragen in controlebestanden
- Functiescheiding is 'De toewijzing aan verschillende personen van de verantwoordelijkheden voor het autoriseren van transacties, het vastleggen van transacties en het bewaren van activa. Functiescheiding is bedoeld om beperkingen aan te brengen in de mogelijkheden voor wie dan ook om bij de uitvoering van zijn normale taken fouten te maken en te verhullen of fraude te plegen en te verhullen'.

Zo gepresenteerd is het allemaal niet zo ingewikkeld: logische toegangsbeveiliging (als digitaal equivalent van fysieke functiescheiding) is een IB maatregel, en (fysieke) functiescheiding is een IB activiteit. Maakt dit onderscheid dan nog wat uit?

IB en COS vereisten

Om deze vraag te beantwoorden moeten we terug naar de COS vereisten. Vereiste 12 stelt dat de accountant inzicht dient te verwerven in de IB maatregelen die relevant zijn voor de controle. Het verwerven van inzicht kan worden opgevat als controleactiviteit om de toereikendheid van de *opzet* van de IB maatregelen te beoordelen alsmede het *bestaan* er van vast te stellen. Dat moet de accountant bij elke controle doen, zoals ook vermeld in Vereiste 13.
De accountant moet ook inzicht verwerven in het informatiesysteem met inbegrip van de daarmee verband houdende bedrijfsprocessen (Vereiste 18). Dit vereiste laat zien dat de accountant goed zicht moet zien te krijgen op hoe de stromen van gegevensverwerking lopen; welke IB maatregelen daarop in geautomatiseerde dan wel handmatige vorm daarin zijn opgenomen. Dan hebben we het nog steeds over inzicht in de opzet, en niet de effectieve werking.
Vereiste 26 gaat in op de risico-inschattingen door de accountant. Bij deze risico-inschattingen houdt de accountant rekening met de *IB maatregelen* die de accountant van plan is om te gaan toetsen (onderdeel

c). Volgens dit vereiste zijn het dus maatregelen die op effectieve werking worden getoetst. In Vereiste 29 vindt vervolgens een soort omschakeling plaats. Zodra sprake is van een significant risico, moet de accountant ook inzicht krijgen in de *IB activiteiten*. Aan dit vereiste zijn drie A-paragrafen verbonden: A137-139. Het bijzondere bij deze A-paragrafen is dan dat het opeens weer gaat om IB maatregelen. Op grond van de hiervoor opgenomen uiteenzetting concluderen we dat het onderscheid tussen IB maatregelen en IB activiteiten niet goed wordt gemaakt[3]. Het vorenstaande biedt tenminste onvoldoende grond om te kunnen stellen dat je functiescheiding *niet* op effectieve werking behoeft te toetsen. Vereiste 30 kan hierbij relevant zijn: voor risico's waarvoor gegevensgerichte werkzaamheden alleen niet leiden tot voldoende en geschikte controle-informatie, zal de accountant de effectieve werking van de IB maatregelen en –activiteiten moeten toetsen (om te komen tot een goedkeurende controleverklaring).

Wat betekent dit?

We weten nu dat we IB maatregelen (of activiteiten) op effectieve werking moeten toetsen als gegevensgerichte werkzaamheden alleen niet leiden tot voldoende en geschikte controle-informatie[4] .
Betekent dit dan automatisch dat de accountant dan ook altijd de effectieve werking van functiescheiding toetst?
Dat zou je wel verwachten als je zo door de AFM rapporten 2013 en 2014[5] leest. Het onderwerp functiescheiding komt daar steevast terug als onderdeel van de controle op de volledige verantwoording van de omzet. De AFM beschrijft dit onderwerp zowel vanuit het perspectief van de geautomatiseerde als handmatige functiescheidingen, en steeds met het oog op de verdere gegevensverwerking. De accountant maakt immers bij de controle ook veel gebruik van lijstwerk uit het geautomatiseerd systeem. Dan moet je toch vaststellen hoe deze lijsten (in voldoende functiescheiding) tot stand zijn gekomen (COS 500.9)? In het algemeen is dit (generieke) uitgangspunt wel bruikbaar. Maar we zouden er toch voor willen pleiten om deze materie wat specifieker te beschouwen. Dat begint met de vraag in hoeverre de volledigheid van de opbrengstverantwoording wel altijd een risico is. Vanuit COS 240 is bekend dat terzake de opbrengstverantwoording een frauderisico verondersteld wordt aanwezig te zijn. Maar dat impliceert nog niet dat een frauderisico ten aanzien van de volledigheid in de opbrengstverantwoording altijd aan de orde is. Het kan ook goed zijn dat de juistheid van de omzetverantwoording de dominante bewering is, bijvoorbeeld in tijden van kredietcrisis. Maar je kunt ook denken aan vele (internationale) boekhoudschandalen waar de fraude met betrekking tot de omzet zat in het boeken van fictieve omzet of het te vroeg verantwoorden van omzet. Dus, helemaal geen volledigheid, maar juistheid.
Stel dat de accountant alleen een significant frauderisico met betrekking tot de juistheid heeft onderkend, dan zal de accountant nog steeds aandacht dienen te besteden aan de opzet van de digitale en handmatige functiescheiding, maar niet per definitie de effectieve werking behoeven vast te stellen. De juistheid van de omzetverantwoording kan immers in veel gevallen prima gegevensgericht middels een statistische steekproef (of andere aanvaardbare methode volgens COS 530) worden vastgesteld. Wanneer echter wel sprake is van een significant volledigheidsrisico, dan kun je feitelijk niet anders dan ook de functiescheidingen (bij voorkeur in de geautomatiseerde omgeving) op effectieve werking te toetsen. Vergelijkbaar met het eerder genoemde voorbeeld van de controle van het hotel .

We hebben je in dit artikel meegenomen in onze speurtocht naar het onderwerp Functiescheiding en welke werkzaamheden je daaraan moet verrichten in de praktijk. We zien in de praktijk veel verschillende zienswijzen. Daarom staan we open voor suggesties en andere denkrichtingen (info@vna-aa.nl), en op die manier bij te dragen aan een beter functionerend accountantsberoep.

[1] Deze casus is ontleend aan het besluit tot het opleggen van een bestuurlijke boete aan Deloitte vanaf pag. 64.

[2] Het Rapport 'In Publiek Belang – Het kan echt Beter!' is het antwoord vanuit het accountantsberoep op de benodigde hernieuwde focus op kwaliteit.

[3] Daardoor is het begrijpelijk dat de AFM rapporten in 2013 en 2014 niet de term IB activiteiten hanteren, maar de term IB maatregelen. Ook in de op 24 maart 2016 verschenen boetebesluiten noemt de AFM functiescheiding een maatregel.

[4] En de accountant is voornemens op de effectieve werking te steunen (315.26).

[5] Merkwaardig genoeg wordt het onderwerp functiescheiding als zodanig niet genoemd in het AFM rapport van 1 september 2010 (big 4), terwijl latere rapporten er relatief veel aandacht aan besteden. Ook in de op 24 maart 2016 verschenen boetebesluiten van de AFM inzake de onderzoeken bij de Big4 komt functiescheiding aan de orde, zoals in het eerder in dit artikel aangehaalde boetebesluit inzake Deloitte.