De compliancefunctie in banken '…en de rol van accountants'

Peter A.M. Diekman

SAMENVATTING De *compliancefunctie* is een relatief jonge functie die zich sinds begin van de jaren negentig van de vorige eeuw binnen financiële ondernemingen sterk heeft ontwikkeld. In dit artikel wordt ingegaan op de functie en taak van de compliancefunctie in een bank. Deze functie wordt hierbij gezien als onderdeel van het systeem van interne beheersing binnen de corporate governance van de bank. Vervolgens wordt ingegaan op het normenkader dat geldt voor de compliancefunctie. Hoewel er ten aanzien van verschillende financiële ondernemingen niet één normenkader is, kan een normenkader worden ontwikkeld voor iedere financiële onderneming met in acht name van de specifieke wet- en regelgeving. Vervolgens wordt een viertal kerntaken van de compliancefunctie beschreven. Deze taken zijn afgeleid uit een analyse van de wet- en regelgeving, de literatuur en waarnemingen bij enkele grote financiële instellingen. Tenslotte wordt de rol van de interne en externe accountant in het kader van de accountantscontrole op de compliancefunctie behandeld.

RELEVANTIE VOOR DE PRAKTIJK In dit artikel wordt geprobeerd een brug te slaan tussen corporate governance en interne beheersing enerzijds en de compliancefunctie anderzijds. De compliancefunctie in een bank wordt beschreven tegen de achtergrond van het in Nederland geldende recht, COSO-model en het zogenaamde Lines of Defence model.

Er wordt een poging gedaan te komen tot invulling van de compliancefunctie op basis van het wettelijk normenkader. Hierbij staat de vraag centraal welke taken tenminste aan de compliancefunctie kunnen worden toebedeeld. Daarnaast wordt op praktische wijze beschreven wat de rol is die externe en interne accountants spelen ten aanzien van de compliancefunctie.

1 Inleiding

Met name de invoering in het vorige decennium van nieuwe wet- en regelgeving gericht op de integriteit van de financiële markt heeft de aandacht binnen de financiële sector naar compliance doen gaan. Europese richtlijnen gericht op de bestrijding van witwassen en financiering van terrorisme vormen de basis voor de wet- en regelgeving in de Europese lidstaten. Amerikaanse wetgeving, zoals de USA Patriot Act 2001[1] en regelgeving vanwege het Amerikaanse ministerie van financiën, de US Treasury, en in het bijzonder de afdeling OFAC (Office of Foreign Assets Control) hebben een extraterritoriaal karakter en beïnvloeden daarmee ook de criteria waaraan compliance wordt getoetst in Europese banken. Hiermee wordt bedoeld dat de wet- en regelgeving van toepassing is op

- niet-Amerikaanse banken die vestigingen hebben in Amerika;
- het internationaal betalingsverkeer in US dollars;
- het bedienen van Amerikaanse staatsburgers door (niet-Amerikaanse) banken buiten Amerika.

In Europese en Nederlandse banken heeft de ontwikkeling van de compliancefunctie in het bijzonder na de aanslagen in september 2001 een vlucht genomen. De ontwikkeling is echter gestart in de jaren negentig van de vorige eeuw met een sterke focus op het bestrijden van inkomen uit drugsverkopen en het afromen van de winsten daarvan.

Het doel van dit artikel is te komen tot een beschrijving van de reikwijdte van de compliancefunctie bij banken. Daarnaast beoogt het artikel een aanzet te geven voor het normenkader waaraan de compliancefunctie zou kunnen worden getoetst. De reikwijdte van de compliancefunctie wordt in hoge mate bepaald door hetgeen heeft te gelden als recht. In dit artikel wordt de compliancefunctie gezien als een onderdeel van corporate governance, meer in het bijzonder: de compliancefunctie vormt een onderdeel van het systeem van interne beheersing binnen de onderneming. Compliance moet in het gedrag van de medewerkers zijn ingebed. De procedures, de werkwijze en de cultuur van de onderneming moeten compliance uitstralen, met andere woorden: compliance moet onderdeel zijn van het DNA van de onderneming (Kaptein, 2008).

In het artikel wordt het begrip compliancefunctie gebruikt. Met dit begrip wordt bedoeld de functie binnen een organisatie die tot taak heeft het toezicht houden op gedrag binnen de onderneming en het geven van advies aan het bestuur ten aanzien van de interpretatie van vigerende

wet- en regelgeving op het terrein van gedrag. De functie staat onder leiding van een compliance officer.

Het artikel gaat in paragraaf 2 in de op de vraag wat is compliance en wat is de reikwijdte van compliance bij een bank. In paragraaf 3 wordt de compliancefunctie in relatie tot corporate governance beschreven, waarna in paragraaf 4 wordt toegespitst op de compliancefunctie in het kader van interne beheersing. Paragraaf 5 gaat vervolgens in op het normenkader voor de compliancefunctie. Hier staat de vraag centraal welke taken aan de compliancefunctie kunnen worden toegekend op grond van de wet- en regelgeving alsmede wat deze taken dan inhouden. In paragraaf 6 wordt de rol van de accountant beschreven. Er wordt zowel ingegaan op de rol van de externe als de interne accountant bij de controle op de compliancefunctie. In paragraaf 7 wordt tenslotte een samenvatting gegeven en worden enkele conclusies getrokken.

2 Wat is compliance en wat is de reikwijdte ervan?

Compliance betekent letterlijk naleving. De vraag hierbij is *wat* wordt er nageleefd? *Compliance is kort gezegd de functie binnen de organisatie die de naleving van wet- en regelgeving borgt* (Paape en Hoff, 2009). Deze korte en bondige omschrijving zegt veel over de rol en positie van de compliancefunctie in een organisatie, maar is het een juiste omschrijving?
De compliancefunctie is een functie die onder andere tot doel heeft te komen tot beheersing van het risico dat wet- en regelgeving worden overtreden. Het is een onderdeel van het interne risicobeheersings- en controlesysteem van de organisatie. In dat kader kan de compliancefunctie worden gepositioneerd in de zogenaamde tweede lijn ofwel de *second line of defence* in een organisatie (Pike, 2009; Hattenbach en Zwikker, 2009).

Een organisatie - en dus ook een bank - moet niet alleen wet- en regelgeving naleven, maar al hetgeen geldt als recht. Dit is ruimer dan wet- en regelgeving. Met wet- en regelgeving wordt bedoeld het geheel van formele en materiële regels die van toepassing zijn op een bank. Daaronder vallen ook de door de bank zelf opgestelde regels zoals statuten, procedures en interne controlemaatregelen. Banken worden aangesproken op de naleving van de zelf opgestelde regels door toezichthouders, aandeelhouders en andere stakeholders. Dat de zelf opgestelde regels behoren tot het recht volgt ook logisch voort uit het feit dat het Nederlandse Burgerlijk Wetboek een zogenaamde open norm kent. De wetgever heeft ten aanzien van de regels omtrent het verkeer tussen personen (zowel natuurlijke als rechtspersonen) veel ruimte gelaten voor eigen invulling. Het gevolg is dat hetgeen we met elkaar afspreken in statuten, overeenkomsten, procedures dan ook als recht geldt en dient te worden nageleefd.

Met hetgeen geldt als recht wordt bedoeld het geheel van wet- en regelgeving, de jurisprudentie, gezaghebbende wetenschappelijke literatuur en cultuur, gewoonte en gebruik.
Onder jurisprudentie wordt verstaan het samenstel van rechterlijke uitspraken, in casu de wijze waarop de rechter de formele en materiële regels interpreteert. Belangrijke jurisprudentie komt van de Hoge Raad, die een rol speelt in het bevorderen van de eenheid in de rechtsvorming. De uitspraken van gerechtshoven en lagere rechters zijn onderdeel van de jurisprudentie, zij het dat lagere rechters de jurisprudentie van hogere rechters meestal in hun uitspraken meewegen.
In de derde plaats kan tot recht in Nederland worden gerekend hetgeen gezaghebbende wetenschappers schrijven. Wetenschappelijke literatuur levert een bijdrage aan de inhoud van het recht. De literatuur draagt bij aan een kritisch debat over het recht en kan aanleiding zijn voor de wetgever om wetten te wijzigen of in te voeren. Het zijn mede de wetenschappelijke artikelen en promotieonderzoeken die bijdragen aan de kennis en die stimulerend kunnen werken ten aanzien van veranderingen. Zij staan daarmee mede aan de basis van de ontwikkeling van het recht.
Tenslotte de vierde component van het recht, namelijk de cultuur, gewoonte en gedrag van mensen. De wijze waarop een samenleving het recht beleeft en het als recht aanneemt (accepteert) evolueert door de tijd. Wat vroeger als heel normaal werd beschouwd kan vandaag als onaanvaardbaar gelden. Wat de samenleving als recht ervaart, de wijze waarop wij interacteren en wat wij als norm wensen aan te nemen is het gevolg van publiek debat, scholing, beïnvloeding van buitenaf, literatuur en ervaring. De cultuur en meningsvorming in een samenleving is uiteindelijk medebepalend voor het recht. De menselijke interactie heeft ook gevolgen voor de wijze waarop wij denken over interne risicobeheersing- en controlesystemen in organisaties. De laatste jaren is het menselijke gedrag meer in de spotlights gekomen en wordt aandacht geschonken aan zaken als soft controls. De opkomst van soft controls, dit zijn controls die zijn gericht op aspecten van menselijk gedrag in een organisatie, is indicatief voor het belang dat gedrag tegenwoordig speelt in organisaties. Een kernpunt ten aanzien van menselijk gedrag in organisaties is het handhaven van een hoge graad van integriteit van de organisatie. Kaptein en Wallage (2010) geven aan dat gedrag thans zo belangrijk is dat er een toenemende behoefte is aan het verstrekken van zekerheid over dit onderwerp en zien daarbij een rol weggelegd voor de accountant. Vink en Kaptein (2008) geven aan dat de

aandacht voor gedrag zich niet beperkt tot het bedrijfsleven, maar zich ook uitstrekt tot de overheid.
Eén van universele doelstellingen van het COSO ERM model (COSO, 2004) is compliance. Deze universele doelstelling beoogt dat in de onderneming alle activiteiten op alle niveaus en te allen tijde voldoen aan het recht. Het is deze universele COSO-doelstelling die met de compliancefunctie wordt nagestreefd. Het compliancerisico is dat deze doelstelling niet wordt gehaald en dat de onderneming daardoor bloot staat aan kritiek van toezichthouders, cliënten of het brede publiek. Deze kritiek kan uiteindelijk leiden tot reputatieverlies en verdere financiële schade. Op grond van het bovenstaande kan de compliancefunctie als volgt worden gedefinieerd:
De compliancefunctie is een interne beheersingsfunctie gericht op het bewerkstelligen en onderhouden van een hoge graad van integriteit in de onderneming als geheel, leidend tot naleving van het recht bij gebreke waarvan de onderneming bloot staat aan een verhoogd risico op sancties, financiële schade en reputatieschade
De compliancefunctie is een interne beheersingsfunctie gericht op de borging van hetgeen als recht heeft te gelden. Daarmee heeft de compliancefunctie een ruimere reikwijdte dan door Paape en Hoff (2009) beschreven. In het kader van compliance wordt ook gesproken over compliancerisico. Het compliancerisico wordt door de Basel Committee on Banking Supervision (verder: BCBS) als volgt gedefinieerd (BCBS, 2005a):
The expression 'compliance risk' is defined in this paper as the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct applicable to its banking activities (together 'compliance laws, rules and standards').

Niet-naleving van het recht leidt mogelijk tot extra kosten of verliezen en kan uiteindelijk zelfs leiden tot faillissement. Dat is ondermeer aangetoond na de schandalen rond Enron, Parmalat, Ahold en andere grote ondernemingen. Deze schandalen hebben er zeker toe bijgedragen dat de compliancefunctie verder tot ontwikkeling is gekomen. De onafhankelijke compliancefunctie wordt genoemd in art. 21 Besluit prudentiële regels Wft (verder: BPR).[2] De reikwijdte van de compliancefunctie wordt in dit artikel omschreven als het toezicht op de naleving van wettelijke regels en van interne regels die de financiële onderneming of bijkantoor zelf heeft opgesteld. In de nota van toelichting bij het BPR wordt de reikwijdte van de compliancefunctie nader omschreven. Hieruit blijkt dat deze functie ook ziet op het monitoren van nieuwe wetgeving en de beoordeling of (nieuwe) producten of diensten aan de (nieuwe) wetgeving voldoen.
Het woord compliance komt als zodanig niet voor in de Wet op het financieel toezicht[3] (verder: Wft) noch in het 'Besluit gedragstoezicht financiële ondernemingen Wft' (verder: BGFo).[4] De wettelijke bepalingen, vooral ex art 3:10 Wft, zijn evenwel gericht op de compliancefunctie. Zoals in de nota van toelichting bij het BPR (p. 104) wordt gesteld is de financiële onderneming primair verantwoordelijk voor de bevordering en handhaving van het integer handelen. De financiële onderneming dient voorts toe te zien op de realisatie van het geformuleerde beleid en de naleving van interne richtlijnen en gedragscodes door haar medewerkers.

3 De compliancefunctie, een onderdeel van corporate governance

Corporate governance komt in het burgerlijk wetboek als term voor in artikel 2:391, lid 5, dat luidt als volgt: '*[...]Bij algemene maatregel van bestuur kunnen nadere voorschriften worden gesteld omtrent de inhoud van het jaarverslag. Deze voorschriften kunnen in het bijzonder betrekking hebben op naleving van een in de algemene maatregel van bestuur aan te wijzen gedragscode en op de inhoud, de openbaarmaking en het accountantsonderzoek van een verklaring inzake corporate governance.*'
Op dit moment zijn twee codes onder dit artikel gebracht, in de eerste plaats De Nederlandse corporate governance code. In de tweede plaats is de Code Banken (NVB, 2009), die met ingang van 1 januari 2010 van kracht is, ook onder dit wetsartikel gebracht.
Beide codes bevatten regels met betrekking tot corporate governance van specifieke groepen van ondernemingen. De Nederlandse corporate governance code noch de Code Banken vormen dwingend recht. Naleving van deze codes door ondernemingen is gemodelleerd naar het beginsel *comply or explain*. Dat wil zeggen: indien een onderneming een bepaling in de code niet naleeft, moet dit worden uitgelegd. Er is echter geen wet die eist dat de codes *moeten* worden nageleefd. Zoals hiervoor al is gesteld: het burgerlijk wetboek kent een open norm. De wetgever heeft er bewust voor gekozen de norm niet in te vullen. Natuurlijke en rechtspersonen hebben een vrijheid om de omgang met elkaar zelf te regelen. Het feit dat er corporate governance codes zijn opgesteld kan worden gezien als een uiting van de burger om de open norm zelf in te vullen. De vraag kan worden gesteld of de corporate governance code en de code banken harde gedragsnormen inhouden. Dit vloeit niet duidelijk voort uit de wet wegens het feit dat sprake is van de modellering volgens het principe van comply or explain. Afwijken mag dus al moet het wel worden uitgelegd. Wel kan worden gesteld dat sprake is van een onderlinge afspraak omtrent het gedrag dat in de codes is vastgelegd. Er wordt een maatschappelijk belang aan toegekend hetgeen ook blijkt uit de verplichting om over de corporate governance melding te doen in het jaarverslag. Daar waar de wetgever de norm heeft open gehouden vult de maatschappij die norm zelf

in. Dit betekent dat naleving van de codes zeker niet vrijblijvend is hoewel er geen sprake is van een dwingend wettelijk voorschrift. Naleving van de code is een verantwoordelijkheid van het bestuur van de vennootschap. De raad van commissarissen dient hierop toe te zien in het kader van diens toezichthoudende taak. Tenslotte kan worden gesteld dat de corporate governance codes kunnen worden gezien als in Nederland algemeen erkende rechtsbeginselen en rechtsovertuigingen als bedoeld in art. 3:12 BW. Dit artikel geeft een nadere invulling van wat onder redelijkheid en billijkheid moet worden verstaan. De tekst van dit artikel luidt:

'Bij de vaststelling van wat redelijkheid en billijkheid eisen, moet rekening worden gehouden met algemeen erkende rechtsbeginselen, met de in Nederland levende rechtsovertuigingen en met de maatschappelijke en persoonlijke belangen, die bij het gegeven geval zijn betrokken.'

Hoewel naleving van de corporate governance code is gemodelleerd volgens het principe comply or explain betekent dit niet dat organisaties de code ongefundeerd naast zich zouden kunnen neerleggen. Met andere woorden: comply or explain is niet hetzelfde als vrijheid-blijheid, hetgeen met zich meebrengt dat organisaties zich wel degelijk moeten richten op de naleving van de code.

De Organisation for Economic Co-operation and Development (OECD) definieert corporate governance als volgt: *'[...] a set of relationships between a company's management, its board, its shareholders, and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined. Good corporate governance should provide proper incentives for the board and management to pursue objectives that are in the interests of the company and its shareholders and should facilitate effective monitoring. The presence of an effective corporate governance system, within an individual company and across an economy as a whole, helps to provide a degree of confidence that is necessary for the proper functioning of a market economy.'*

Uit deze definitie blijkt dat het gaat om de relatie tussen de ondernemingsdoelen die door het bestuur worden vastgesteld en het beheersingsysteem dat ertoe moet bijdragen dat deze doelen ook bereikt worden.

Zoals reeds gesteld is het doel van de compliancefunctie de borging van het naleven van het recht. En, zoals in de OECD definitie gesteld, *"...the means of attaining those objectives and monitoring performance..."* kan mede worden gezien als een onderdeel van de compliancefunctie. Met de definitie van de OECD is een link gelegd tussen corporate governance en compliance. Het hebben van een compliancefunctie als onderdeel van de corporate governance is een conditie voor diens kwaliteit. De BCBS (2005b) stelt dat het hebben van een compliancefunctie een verplicht onderdeel is van de organisatie van een bank. De compliancefunctie maakt daarmee onderdeel uit van corporate governance en niet omgekeerd (Diekman en Kersten, 2008). Paape en Hoff (2009) leggen eveneens een verband tussen corporate governance en compliance met name waar het gaat om het bereiken van doelen. Zij zien het bereiken van specifieke doelen (naleving van wet- en regelgeving en integer handelen) als de aansluiting tussen corporate governance en compliance.

Volgens het BCBS is corporate governance bij banken van groter belang dan bij andere ondernemingen (BCBS, 2005b). Dit heeft te maken met de rol die banken spelen in de economie als belangrijke schakel in het betalingsverkeer en als hoeder van spaargelden en deposito's van cliënten. Dit geldt in nog sterker mate voor banken die als systeemrelevant worden aangemerkt. Systeemrelevante banken kunnen worden omschreven als banken waarvan het goed functioneren van existentieel belang is voor de economie. Een faillissement van een systeemrelevante bank zal een belangrijk en algemeen voelbaar negatief effect hebben op het fungeren van de economie. Tijdens de kredietcrisis die in de tweede helft van 2007 begon zijn enkele systeemrelevante banken in verschillende landen met behulp van belastinggeld overeind gehouden en is daarmee een faillissement van deze ondernemingen afgewend. Het is opvallend dat in het rapport van de commissie Maas (Adviescommissie toezicht banken, 2009) noch in de Code Banken (NVB, 2009) wordt ingegaan op de compliancefunctie. De titel van het rapport van de commissie Maas luidt: *Naar herstel van vertrouwen* en is geschreven tijdens het dieptepunt van de kredietcrisis. Deze periode wordt gekenmerkt door verlies van publiek vertrouwen in banken. Wellicht het belangrijkste ankerpunt voor vertrouwen van de markt voor een bank is de integriteit van de mensen die in die onderneming werken en dit behoort tot de focus van compliance. Juist een goed functionerende compliancefunctie draagt bij aan het herstel van vertrouwen en ondersteunt het bestuur van de financiële onderneming om dat vertrouwen waar te maken en te bestendigen. Overigens laat niet alleen de commissie Maas na om het belang van de compliancefunctie voor herstel van vertrouwen te belichten. Ook het Walker report (Walker, 2009) gaat niet in op de compliancefunctie. Evenals het rapport van de commissie Maas zet Walker het zoeklicht op de riskfunctie naast de functie van het bestuur en de toezichthoudende organen. Toegegeven, de kredietwaardigheid van een bank en de kwaliteit van het risicomanagement zijn belangrijke ankerpunten voor het publieke vertrouwen. Maar het komt toch wat vreemd over wanneer op het dieptepunt van de financiële crisis het zoeklicht in het geheel niet wordt gericht op de compliancefunctie, maar uitsluitend op de riskmanagementfunctie.

4 De compliancefunctie, een onderdeel van de interne beheersing

4.1 Risicobeheersing

Hoewel compliance een relatief nieuwe verbijzonderde functie is in ondernemingen bestaat het eigenlijk al heel lang. Het voldoen aan het recht is niet iets van de laatste tijd; het is altijd één van de doelen geweest van interne beheersing binnen een onderneming. Gesteld kan worden dat voldoen aan het recht helemaal geen doel op zich is. Hooguit is het een middel om doelen te bereiken. Toch wordt in het COSO-model (2004) compliance gezien als een universeel doel van de organisatie. De reden is gelegen in het feit dat naleving van het recht in veel organisaties geen vanzelfsprekendheid is. Naleving van het recht zit als het ware nog niet in het DNA van de organisatie en dus moeten er specifieke maatregelen worden getroffen om naleving wel te bereiken.
Het is anders gesteld in de cockpit van een vliegtuig waar niet-naleving van regels vrijwel ondenkbaar is. Maar waarom houdt een piloot zich beter aan de regels dan een bankier? Omdat hij misschien ook zijn eigen leven in gevaar brengt als hij de regels negeert? In ieder geval kan worden gesteld dat werken conform de regels bij een piloot meer in het DNA zit dan bij medewerkers van veel andere bedrijven, waaronder banken. Dit is de reden dat compliance als een doel (en natuurlijk ook als een middel) in organisaties kan worden gezien.
In toenemende mate bestaat bij veel ondernemingen het besef dat het niet voldoen aan het recht tot ernstige gevolgen kan leiden die uiteindelijk ook het voortbestaan van de onderneming als geheel in gevaar kan brengen. Er zijn talloze voorbeelden van ondernemingen die publiekelijk aan de schandpaal worden genageld, waarbij geen middel wordt ontzien om normafwijkend gedrag van ondernemingen ter discussie te stellen.[5] Tillema (2008) geeft aan dat non-compliance met name in de financiële sector grote gevolgen kan hebben voor ondernemingen. Een kort onderzoek naar de handhaving van wet- en regelgeving maakt duidelijk dat de boetes tot zeer hoge bedragen kunnen oplopen en bevestigen hetgeen Tillema in 2008 schreef. In de gevallen dat het Amerikaanse ministerie van justitie (DOJ) een strafrechtelijk vooronderzoek instelt leidt dit in de meeste gevallen tot het afkopen van de strafzaak. Tegen soms extreem hoge bedragen wordt dan een zogenaamd *deferred prosecution agreement* gesloten met justitie. Het onderzoek leidt ook tot de conclusie dat toezichthouders torenhoge boetes kunnen opleggen aan banken wegens onvoldoende compliancemaatregelen.

De ontwikkeling van de compliancefunctie is mede tot stand gekomen door de steeds meer complexe wet- en regelgeving waaraan banken moeten voldoen. Daar komt bij dat deze wet- en regelgeving in veel gevallen extraterritoriale dimensies heeft waarmee de complexiteit alleen maar toeneemt. Het risico waaraan banken blootstaan is ook toegenomen als gevolg van het feit dat sprake is van een toenemende kritische blik vanuit allerlei maartschappelijke geledingen. In de eerste plaats staat de financiële dienstverlening op de agenda van de politiek. In de tweede plaats hebben de voornaamste toezichthouders in de financiële sector (De Nederlandsche Bank NV (DNB) en de Autoriteit Financiële Markten, (AFM)), mede door de financiële crisis, aan ervaring en daarmee aan daadkracht gewonnen. In de derde plaats is er toenemende aandacht voor financiële dienstverlening, met name gericht op naleving van de zorgplicht, bij populaire televisieprogramma's, waardoor deze dienstverlening op een begrijpelijke wijze onder de aandacht van het grote publiek wordt gebracht.
Banken staan bloot aan complexe risico's, waaronder het risico van normafwijkend gedrag van eigen mensen alsmede cliënten. De compliancefunctie is in het bijzonder gericht op het beheersen van het gedragsrisico, zowel voortvloeiend uit het gedrag van de eigen medewerkers van de onderneming als van de cliënten.

4.2 Plaats in de organisatie

Er wordt tegenwoordig wel gesproken over het zogenaamde *Three lines of defence model* (Pike, 2009; Hattenbach en Zwikker, 2009). Dit model is niet meer dan een denkmodel dat inzicht probeert te geven in de manier waarop ondernemingen zich trachten te wapenen tegen gevaren van buitenaf en excessieve risico's. Pike (2009) beschrijft in dit verband dat er drie verdedigingslinies bestaan te weten: 1) het bestuur 2) de interne beheersingsfuncties risk management en compliance en tenslotte 3) de interne accountantsdienst.
De drie verdedigingslinies van Pike (2009) hebben ieder een eigen taak en verantwoordelijkheid. De eerste verdedigingslinie wordt gevormd door het bestuur en lijnmanagement in de organisatie. De taak van het bestuur is de vaststelling en uitvoering van de strategie van de ondermening. Het bestuur is beleidsbepalend en vormt daarmee de eerste verdedigingslinie. De gedachte hierachter is dat het bestuur zich oriënteert op het belang van de vennootschap en de daarin verbonden onderneming. In dat kader zal het bestuur zich ook moeten oriënteren op het maximaal aanvaardbare risico dat de onderneming kan en wil lopen. Dit is de bepaling van een in het kader van de onderneming gezonde *risk appetite*. Met andere woorden: het bestuur zal trachten de juiste balans te vinden tussen het accepteren van risico's en de prijs die daarvoor op de markt kan worden gerealiseerd en dit alles binnen de grenzen van de risicotolerantie (de risk appetite).
In toevoeging aan Pike's beschrijving, ben ik van oordeel dat er meer verdedigingslinies zijn dan die drie die hij benoemt. In de eerste plaats is de raad van commissarissen een belangrijke verdedigingslinie in de taak om toezicht uit toe oefenen op de raad van bestuur van een onderneming. In de

Tabel 1 Recente boetes in de financiële sector

Datum	Bank	Boete of Settlement	Handhaving instantie(s)	Korte reden
Februari 2011	Zions First National Bank	US $ 8 mln	FinCen	Onvoldoende compliancemaatregelen
Augustus 2010	RBS	£ 5,6 mln	FSA	Onvoldoende screening van cliënttransacties
Juni 2010	JP Morgan	£ 33,3 mln	FSA	Onvoldoende compliancemaatregelen
Augustus 2010	Barclays	US$ 298 mln	DOJ, OFAC	Illegale currency transacties met landen die onder embargo vallen
Mei 2010	ABN AMRO / RBS	US $ 500 mln	DOJ	Afkoop juridische vervolging wegens vermeende overtreding van US embargo wetgeving inzake betalingsverkeer
December 2009	Credit Suisse	US $ 536 mln	DOJ, OFAC	Handel in securities met entiteiten die onder embargo vallen
Augustus 2009	Australia and New Zealand Banking Group	US $ 5,75 mln	OFAC	Transacties met entiteiten die onder embargo vallen
Januari 2009	Llyods TSB	US $ 350 mln	DOJ	Afkoop juridische vervolging wegens vermeende overtreding van US wetgeving inzake betalingsverkeer
Juni 2007	- AMEX Bank Int'l - AMEX travel related services company	US $ 65 mln	DOJ, FinCen	- Onvoldoende compliancemaatregelen - Onvoldoende interne controles - Onvoldoende monitoring - Onvoldoende management oversight
December 2005	ABN AMRO	US $ 80 mln	FED, NY State, Illinois State en De Nederlandsche Bank	Onvoldoende compliance inzake US anti money laundering wetgeving
Mei 2004	Citi Group	US $ 70 mln	FED	Verschillende wetsovertredingen
Mei 2004	UBS	US $ 100 mln	FED	Onvoldoende compliance met US anti money laundering wetgeving
Mei 2004	Riggs Bank	US $ 25 mln	OCC, FinCen	Onvoldoende compliance met US anti money laundering wetgeving
December 2003	Credit Lyonnais	US$ 100 mln	FED	Verschillende wetsovertredingen

Legenda: FED – Federal Reserve Bank - Stelsel van centrale banken in de Verenigde Staten
DOJ – Department of justice – Amerikaanse ministerie van justitie
FinCen – Financial crimes enforcement network – vergelijkbaar met meldpunt voor ongebruikelijke transacties
OFAC – Office of foreign assets control – onderdeel van het Amerikaanse ministerie van financiën
FSA – Financial services authority – toezichthouder in Engeland
State Authorities – Toezichthouders in verschillende Amerikaanse staten

tweede plaats geldt dat waar ondernemingen werkzaam zijn in een gereguleerde sector met een door de wet aangestelde toezichthouder, die bij de uitoefening van de toezichttaak ook een verdedigingslinie vormt voor de onderneming. Tenslotte wordt wel betoogd dat de externe accountant (en wellicht ook andere externe controleurs) een soort zesde verdedigingslinie vormt voor de onderneming.

De compliancefunctie kan worden gepositioneerd in de tweede verdedigingslijn van de organisatie. Deze lijn bestaat uit vakspecialisten (subject matter experts) die een adviserende taak hebben naar de raad van bestuur. De tweede lijn omvat naar mijn oordeel tenminste de volgende afdelingen:

- juridische zaken;
- finance;
- risk management;
- human resources; en
- compliance.

De primaire taak is het adviseren van het bestuur op de bovengenoemde onderdelen om daarmee bij te dragen dat de onderneming op koers blijft.

Een essentieel punt is dat de tweede verdedigingslinie zou moeten kunnen interveniëren in de eerste lijn. Walker (2009, paragraaf 6.17) stelt ten aanzien van de risk managementfunctie dat deze '*[...] should be able to exercise a power of veto where necessary.*' Er is mijns inziens geen reden om dit anders te zien voor de compliancefunctie. Ten aanzien van die functie komt dit er concreet op neer dat deze een transactie die door het lijnmanagement wordt geïnitieerd kan stoppen met als argument dat de transactie tot te grote compliancerisico's leidt. Een dergelijk besluit van de compliancefunctie kan worden overruled door de eerste lijn, in casu het bestuur en lijnmanagement die immers de eindverantwoordelijk hebben, maar het overrulen zal wel tot een belangrijk dispuut leiden tussen het bestuur en de controlfuncties. Escalatie van dit dispuut naar de raad van commissarissen (veelal de audit committee) is dan een uitweg. Het confronteert commissarissen met essentiële beslispunten en geeft inhoud aan hun toezichthoudende taak. Uiteindelijk is het wel het bestuur dat de beslissing neemt onder toezicht van commissarissen.

5 Normenkader

Is er een normenkader voor de compliancefunctie en welke taken vloeien daar dan uit voort?

Het normenkader voor de compliancefunctie is af te leiden uit de definitie van compliance en vloeit mede voort uit het recht. In de Nederlandse omgeving kan de normstelling voor compliance in belangrijke mate worden ontleend aan de Wet ter voorkoming van witwassen en financiering van terrorisme (Wwft)[6], de Wft en het BPR. Daarnaast gelden voor veel banken ook internationale normen. Een belangrijke norm kan ondermeer worden ontleend aan art. 352 van de USA Patriot Act 2001. Dit artikel geeft kortweg aan dat een bank een compliancefunctie moet hebben die tenminste de volgende vier aspecten moet omvatten:

- adviseren over specifieke interne controles gericht op naleving van de Amerikaanse wet- en regelgeving;
- het in dienst hebben van een functionaris belast met het toezicht op anti-money laundering en terrorist financing;
- permanente educatie op het terrein van compliance ten behoeve van bankmedewerkers; en
- onafhankelijke controle op de compliancefunctie.

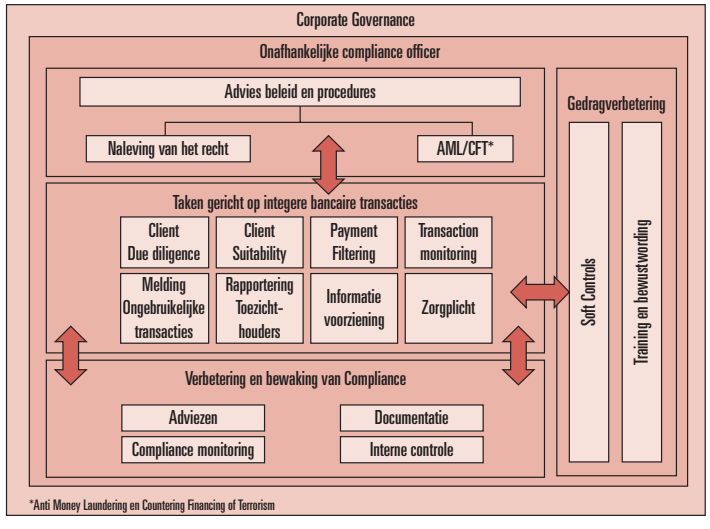
Uitgaande van de bovengenoemde (Nederlandse) wetten en uitvoeringsbesluiten kunnen voor de compliancefunctie een viertal kerntaken worden onderscheiden, te weten:

- adviseren omtrent beleid en procedures;
- taken gericht op integere bancaire transacties;
- verbetering en bewaking van compliance;
- gedragverbetering.

5.1 Advies over beleid en procedures

Om de compliancefunctie op een goede manier gestalte te geven binnen de bank zal een beleid moeten worden geformuleerd dat is gericht op het bevorderen van integer gedrag van de eigen mensen alsmede op het zaken doen met betrouwbare en integere cliënten. Dit uitgangspunt zou moeten worden opgenomen in het statuut van de compliancefunctie binnen de bank. Een belangrijk doel van de compliancefunctie is het verankeren van integer gedrag van de bank en erop toezien dat cliënten integere financiële transacties uitvoeren. Dit is de basis voor de licence-to-operate van de bank.

Figuur 1 Elementen van de compliancefunctie



De compliance officer is daarmee als het ware een poortwachter voor het integer handelen van de bank. Vanuit deze rol adviseert de compliance officer de raad van bestuur over het beleid en de procedures op het terrein van compliance.

5.2 Taken gericht op integere bancaire transacties

Er wordt een achttal taken onderscheiden die allemaal zijn gericht op het integer zaken doen. Deze taken vloeien voor een belangrijk deel voort uit Nederlandse en buitenlandse wet- en regelgeving. De taken die kunnen worden onderscheiden zijn:

- client due diligence;
- client suitability;
- payment filtering;
- transaction monitoring;
- melding ongebruikelijke transacties;
- rapportering aan toezichthouders;
- informatievoorziening;
- zorgplicht.

Client due diligence (CDD) is de risicobeoordeling ten aanzien van cliënten en erop gericht om bij voortduring vast te stellen dat de cliënten zich in financieel opzicht blijven gedragen op een integere wijze. CDD is niet alleen van belang bij het aannemen van nieuwe cliënten, maar dient zich bij voortduring te voltrekken. De Wwft stelt eisen aan de CDD. Bij hoogrisico cliënten dient de CDD uitgebreider te worden uitgevoerd dan bij laagrisico cliënten. Wanneer de bank indicaties krijgt dat het financiële gedrag van een cliënt vraagtekens oproept zal moeten worden besloten of de cliënt bediend kan blijven of dat afscheid moet worden genomen.

Client suitability is een beoordeling van de aard van de cliënt tegen de achtergrond van de marktsegmentering die de bank heeft gekozen. Hierbij is de vraag aan de orde of de cliënt past bij de bank en of de dienstverlening die de bank aanbiedt aansluit bij de behoefte die een cliënt heeft.

De financiële transacties die cliënten via de bank laten uitvoeren moeten voortdurend worden beoordeeld op integriteit van de transacties. Dit gebeurt op basis *van transaction monitoring* en *payment filtering*. De monitoring van transacties kan een indicatie aan het licht brengen van niet-integer handelen. Dit kan aanleiding zijn nader onderzoek te doen naar transacties met een eventueel karakter van witwassen en terrorisme financiering. Bij payment filtering ligt het accent meer op het voorkomen van transacties die vanwege de wetgever à priori zijn verboden. Hierbij is te denken aan het uitvoeren van transacties met personen die op een zwarte lijst staan (bijvoorbeeld terroristen, bepaalde politici of transacties met landen waarvoor een embargo geldt).

Een bank dient op grond van de wet onverwijld melding te doen van transacties waarvoor een verdenking van witwassen of financiering van terrorisme bestaat. Hierbij kunnen banken gebruik maken van de indicatorenlijst als bedoeld in art. 15 Wwft.[7] Meldingen moeten aan formele eisen voldoen. Het is de compliancefunctie die kan dienen als communicatiekanaal naar het meldpunt (in Nederland het Financial Intelligence Unit NL). De compliancefunctie dient de ongebruikelijkheid vast te stellen en te bewaken dat de meldingen aan de autoriteiten zowel tijdig als juist geschieden. Tegelijk leidt het onderzoek naar cliëntentransacties tot advisering aan de raad van bestuur ten aanzien van het al dan niet handhaven van bepaalde cliënten in het bestand.

De compliancefunctie is bij uitstek ook geschikt om te dienen als eerste communicatiekanaal naar de toezichthouders, te weten DNB en AFM. Dit geldt zeker waar het gaat om het toezicht op de integriteit van de bank en diens cliënten. Het feit dat de compliancefunctie het primaire communicatiekanaal is leidt ertoe dat de informatieverschaffing aan toezichthouders wordt geprofessionaliseerd en daarmee tot meer consistente informatieverschaffing naar de toezichthouders.

De compliancefunctie verschaft niet alleen informatie aan toezichthouders, maar ook naar andere afdelingen binnen de bank. Hierbij kan worden gedacht aan interpretatie van nieuwe wet- en regelgeving en het aangeven hoe de bank daarop zou kunnen reageren. Tenslotte heeft de compliancefunctie een belangrijke taak in het kader van de zorgplicht van de bank. Zeker na de financiële crisis van 2007-2009 is de zorgplicht meer onder de aandacht gekomen. Hierbij gaat het om de inhoud van de informatie die aan cliënten wordt verstrekt en de vraag of deze informatie in voldoende mate duidelijk is. Ook gaat het om de vraag of de bancaire producten/diensten die worden aangeboden passen binnen de wettelijke grenzen. Het is een taak van de compliancefunctie om de producten/diensten voortdurend aan de wettelijke normen te toetsen en indien nodig de raad van bestuur te adviseren daarin verandering aan te brengen of bepaalde producten/diensten niet meer aan te bieden.

Tenslotte gaat het bij de zorgplicht erom hoe de bankmedewerkers zich ervan hebben overtuigd en hebben gedocumenteerd dat de cliënt daadwerkelijk de complexiteit van de bancaire producten/diensten begrijpt, het risico daarvan overziet, de eigen risicoacceptatie goed heeft bepaald en daarmee tot een weloverwogen beslissing kan komen om diensten van de bank af te nemen.

5.3 Verbetering en bewaking van compliance

De compliancefunctie heeft tot taak de compliance binnen de bank bij voortduring te bewaken en waar nodig te verbeteren. In dit kader kunnen een viertal taken worden onderscheiden, te weten:

- adviezen;
- documentatie;
- compliance monitoring;
- kwaliteitsbewaking.

De compliancefunctie heeft een belangrijke adviestaak binnen de bank. In het bijzonder richt zich dit op de interpretatie van wet- en regelgeving. Daarnaast adviseert de compliancefunctie ook ten aanzien van de positie die de bank inneemt bij de cliëntacceptatie, het afscheid nemen van cliënten en conflicten met toezichthouders en eigen medewerkers.

In de huidige tijd is documentatie van activiteiten steeds belangrijker. Er wordt wel gesteld '*...if it is not documented, it is not done...*'. Dit betekent dat alle activiteiten die de bank uitvoert in het kader van compliance dienen te worden gedocumenteerd. Toezichthouders eisen dit en nemen geen genoegen met een mondelinge uitleg dat bepaalde controles of activiteiten zijn gedaan, maar niet zijn vastgelegd. Cliëntdossiers moeten up-to-date zijn en bepaalde informatie, zoals bijvoorbeeld cliëntidentificatiebewijzen, moeten aanwezig zijn. Bij cliëntacceptatie moet informatie worden ingewonnen over de herkomst van het geld dat nieuwe cliënten op de bankrekening storten. Hierbij is het van belang dat verder wordt gekeken dan alleen de herkomst van geld vanaf een rekening bij een andere bank, maar dat wordt gevraagd naar de uiteindelijke bron van de welvaart, ofwel de *source of wealth*. Dit is van belang om te voorkomen dat de bank ongewild toch verzeild raakt in een procedure om geld met een criminele herkomst wit te wassen en terug te geleiden in de legale economie. Ook dit behoort deugdelijk te worden gedocumenteerd.

Tenslotte heeft de compliancefunctie tot taak de compliance binnen de bank bij voortduring te beoordelen (te monitoren) en waar nodig aan te zetten tot verbetering van de kwaliteit. Dit kan bijvoorbeeld leiden tot inspectie (monitoring) van cliëntdossiers, vastleggingen van medewerkers, toezicht op verplichte educatie (inclusief de educatie die verplicht is voor bestuurders en commissarissen op grond van de Code Banken).

5.4 Gedragverbetering

Tenslotte heeft de compliancefunctie een taak in het bevorderen van compliant gedrag van medewerkers. Daarbij staan twee aspecten centraal, te weten:

- soft controls;
- training en bewustwording.

Soft controls zijn sturings- en beheersingsmaatregelen die erop gericht zijn om gewenst, integer, gedrag bij medewerkers en management te bevorderen. In tegenstelling tot hard controls zijn deze beheersingsmaatregelen minder goed te meten of te sturen, omdat softcontrols vooral betrekking hebben op (gedeelde) normen en waarden. Van belang is daarbij dat bepaalde normen en waarden en/of gewenst gedrag voor eenieder helder moeten zijn en onderschreven moeten worden (Lückerath-Rovers, 2010). De Kiewit (2011a) geeft aan dat om sturing te geven aan de integriteit van de organisatie soft controls van belang zijn. De financiële crisis heeft de aandacht voor cultuur binnen banken doen aanwakkeren en daarmee ook de aandacht voor soft controls (De Kiewit, 2011b), hetgeen ook wordt aangetoond door onderzoek van KPMG (KPMG, 2010). Hiervoor is al aangegeven dat cultuur, gewoonte en gedrag een component is van hetgeen heeft te gelden als recht. Toezicht op de handhaving van cultuur, gewoonte en gedrag is daarmee ook een logisch aandachtspunt voor de compliancefunctie.

Dit komt mede tot uitdrukking in de taak die deze functie heeft ten aanzien van het bevorderen van training en bewustwording onder de medewerkers van de bank. Uitleg van de regels en het aangeven hoe deze regels van invloed zijn op gedrag leiden tot meer bewustwording en tot gedrag dat de basis vormt voor integer handelen door de bank.

6 De rol en verantwoordelijkheid van de accountant

6.1 Algemeen

Enkele specifieke taken en verantwoordelijkheden voor de externe accountant belast met de controle van de jaarrekening van een bank vloeien voort uit de wet, in dit kader de Wft. In artikel 3:88 en 4:27 Wft wordt aan de accountant die is belast met de controle van de financiële verantwoording een meldplicht aan toezichthouders opgelegd. De accountant heeft een meldplicht aan DNB en AFM indien hij kennis heeft gekregen van feiten bij de bank die in strijd zijn met de bepalingen in hoofdstuk 3 respectievelijk hoofdstuk 4 van de Wft, die duiden op een bedreiging van het voortbestaan van de bank of indien er situaties bestaan die ertoe leiden dat de accountant niet langer een ongeclausuleerde controleverklaring kan afgeven. De communicatie tussen de accountant en toezichthouder is verder uitgewerkt in het BPR en BGFo. De communicatie tussen de accountant en de AFM wordt in detail geregeld in de artikelen 107 en 108 van het BGFo. Daaruit kan worden afgeleid dat naast de hiervoor genoemde formele meldplicht op grond van de wet, de accountant ook de belangrijkste communicatie met het management met betrekking tot de accountantscontrole en de controleverklaring alsmede de management letter deelt met de AFM.

Ten aanzien van de communicatie tussen de accountant en DNB kan worden gesteld dat deze inhoudelijk vrijwel gelijk is aan de communicatie met de AFM. Dit is geregeld in de artikelen 136 en 137 BPR. In afwijking van het bepaalde ten aanzien van de communicatie met de AFM staat het BPR toe dat DNB aanvullende informatie kan vragen aan de accountant. Sinds vele jaren is het gebruikelijk dat DNB dit doet tijdens een jaargesprek met de accountant die is belast met de controle van de jaarrekening. Onderwerpen die tijdens dit gesprek aan de orde

komen zijn de belangrijkste bevindingen van de accountant tijdens de controle die relevant zijn voor de toezichttaak van DNB. De externe accountant heeft de focus primair op de jaarrekening gericht. Gesteld kan daarom ook worden dat een inhoudelijke controle of beoordeling van de compliancefunctie hooguit een marginale toetsing inhoudt. De inhoudelijke toetsing van de compliancefunctie wordt om die reden dan ook in de meeste gevallen door de interne accountant van de bank uitgevoerd.

6.2 De audit van de compliancefunctie

De compliancefunctie in een bank is onderworpen aan (interne) accountantscontrole. Op grond van artikel 17, lid 4 BPR kan worden gesteld dat de primaire taak voor de controle op de compliancefunctie rust op de interne auditor die daarover rapporteert aan de raad van bestuur en aan de audit committee van de raad van commissarissen. Steun hiervoor wordt ontleend aan het BCBS paper over de compliancefunctie (2005a, Principle 8) waarin wordt gesteld dat *'[...]The scope and breadth of the activities of the compliance function should be subject to periodic review by the internal audit function (...)'.*

Het doel van de interne accountantscontrole op de compliancefunctie is in de eerste plaats te controleren of alle taken die zouden moeten worden uitgevoerd ook daadwerkelijk tot het werkterrein van de compliancefunctie behoren. In de tweede plaats moet worden gecontroleerd of de taken naar behoren worden uitgevoerd. In de derde plaats zal de interne accountant aanbevelingen doen tot verbetering van de taakinvulling waar dat blijkens de resultaten van de controle noodzakelijk is.

Toch lijkt het eenvoudiger dan het is om de compliancefunctie te controleren. In de eerste plaats moet voor een audit een duidelijke norm worden bepaald anders is een audit niet mogelijk. In de tweede plaats is een audit pas zinvol indien de auditor beschikt over voldoende kennis ter zake van het controleobject. Dit betekent dat de interne auditor over voldoende kennis moet beschikken over de compliancefunctie alvorens een zinvolle controle kan worden uitgevoerd. De interne auditor kan de noodzakelijke kennis ter zake van compliance op verschillende manieren verwerven, waarbij te denken is aan:

- het volgen van op compliance gerichte opleidingen, zowel intern als extern;
- het nastreven van een sterke focus op complianceaudits in de jaarplanning van de uitvoerende auditor;
- het participeren in vaktechnische discussies over compliance gerelateerde onderwerpen;
- het participeren in projecten die worden opgezet rond compliancethema's.

De noodzakelijke training voor een interne auditor om een compliance audit te kunnen uitvoeren moet in de eerste plaats ingaan op kennisoverdracht ter zake van wet- en regelgeving. Sommige banken hebben met internationale wet- en regelgeving te maken, waardoor deze eis dus al vrij zwaar wordt. De interne auditor kan ervaring opdoen door in de jaarplanning een sterke focus op de compliancefunctie na te streven. Op de vraag wat een sterke focus is kan moeilijk een concreet antwoord worden gegeven, maar een minimum aantal uren[8] dat op jaarbasis wordt besteed aan complianceaudits zou hiervoor een basis moeten zijn.

7 Conclusies

De compliancefunctie is een relatief jonge functie in banken. 't Hart (2008) stelt dat een van de eerste regelingen waarin werd gerefereerd aan de positie van de compliance officer is de op 1 april 1994 door DNB uitgevaardigde Regeling Privé-beleggingstransacties. Toch kan ook worden gesteld dat de compliancefunctie juist in banken sterk tot ontwikkeling is gekomen. Dit heeft mede te maken met de sterke focus van de Europese en Nederlandse wetgevers op het voorkomen van misbruik van het financiële stelsel en de wetgeving die daarvan het gevolg is (Diekman, 2008).

Gesteld is dat de compliancefunctie onderdeel uitmaakt van de corporate governance van de onderneming. Op basis van hetgeen geldt als het recht is aangegeven dat een viertal taken kunnen worden toegekend aan de compliancefunctie te weten:

- adviseren omtrent beleid en procedures;
- taken gericht op integere bancaire transacties;
- verbetering en bewaking van compliance;
- gedragverbetering.

Indien deze taken niet naar behoren worden uitgevoerd en daarmee wordt afweken van hetgeen in de wet als eis ten aanzien van compliance is gesteld staan banken bloot aan soms extreem hoge financiële risico's als gevolg van boetes. Een overzicht van boetes die de afgelopen jaren aan banken zijn opgelegd laat zien dat deze gemakkelijk in de honderden miljoenen dollars kunnen lopen.

Zowel de wet als ook de papers van de BCBS kennen accountants een controlerol toe ten aanzien van de compliancefunctie. Gesteld is dat de externe accountant in dit verband meer een marginale toetsing uitvoert. De inhoudelijke controle op de kwaliteit van de compliancefunctie ligt meer op het werkterrein van de interne accountant. ■

Prof. dr. Peter A.M. Diekman RA is partner bij KPMG Advisory NV en hoogleraar Compliance & Risk Management aan de Erasmus Universiteit Rotterdam.

Noten

1 USA Patriot Act 2001 – Public law 107–56– October 26, 2001

2 Besluit van 12 oktober 2006, houdende prudentiële regels voor financiële ondernemingen die werkzaam zijn op de financiële markten (Besluit prudentiële regels Wft), Staatsblad 2006, 519.

3 Wet van 28 september 2006, houdende regels met betrekking tot de financiële markten en het toezicht daarop (Wet op het financieel toezicht).

4 Besluit van 12 oktober 2006, houdende regels met betrekking tot het gedragstoezicht op financiële ondernemingen (Besluit Gedragstoezicht financiële ondernemingen Wft).

5 Voorbeelden kunnen worden gevonden in verschillende televisieprogramma's waar voor een miljoenenpubliek gedrag van ondernemingen ter discussie wordt gesteld. Een bekend voorbeeld is DSB, maar ook de verzekeringsbranche die werd bekritiseerd wegens het verstrekken van woekerpolissen.

6 Wet van 15 juli 2008, houdende samenvoeging van de Wet identificatie bij dienstverlening en de Wet melding ongebruikelijke transacties (Wet ter voorkoming van witwassen en financieren van terrorisme), Staatsblad 2008, 302.

7 Voor de indicatorenlijst Wwft zie: http://www.afm.nl/~/media/Files/wetten-regels/wwft/Indicatorenlijst%20behorende%20bij%20de%20WWFT.ashx.

8 Mijn ervaring bij een grootbank leert dat een minimum van 650 uren auditwerk op de compliancefunctie een goede basis kan bieden om ervaring op te doen. Daarnaast kunnen auditors zich theoretisch bekwamen door opleidingen op het terrein van compliance.

Literatuur

- Adviescommissie Toekomst Banken (2009), *Naar herstel van vertrouwen*, Nederlandse Vereniging van Banken, 7 april 2009.
- BCBS (Basel Committee on Banking Basel Supervision) (2001), *Internal audit in banks and the supervisor's relationship with auditors*, August 2001; zie: http://www.bis.org/publ/bcbs84.htm
- BCBS (Basel Committee on Banking Basel Supervision) (2005a), *Compliance and the compliance function in banks*, April 2005"; zie: http://www.bis.org/publ/bcbs113.pdf
- BCBS (Basel Committee on Banking Supervision) (2005b), *Enhancing Corporate Governance for Banking Organisations* – consultative document, July 2005; zie: http://www.bis.org/publ/bcbs117.pdf p 4
- COSO (Committee of Sponsoring Organizations of the Treadway Committee) (2004), Risico management van de onderneming - Geïntegreerd raamwerk - *Enterprise Risk Management - Integrated Framework (ERM)*, september 2004; zie: http://www.coso.org/ERM-IntegratedFramework.htm.
- De Kiewit, M. (2011a), Auditen van integriteit vraagt om een juiste combinatie van hard en soft controls - , *Audit Magazine*, nr. 2, juni 2011, pp. 14-17
- De Kiewit, M. (2011b), Sturen op soft controls – *De kwaliteit van een organisatiecultuur –, Bank en Effectenbedrijf*, juni 2011, pp. 14-17
- Diekman, P.A.M. (2008), *Protecting financial market integrity – Roles and responsibilities of auditors*, Deventer: Kluwer.
- Diekman, P.A.M. en A.J.J.P.B.M. Kersten (2008), Whither compliance?, in: *Jaarboek Compliance 2009* (pp. 57-62), Nederlands Compliance Instituut.
- Diekman, P.A.M. (2010), Vertrouwen in banken, *Maandblad voor Accountancy en Bedrijfseconomie*, vol. 84, nr. 3 (maart), pp. 123-132.
- 't Hart, F.M.A. (2008), De compliancefunctie, in: M. Jurgens en R. Stijnen (red.), *Compliance in het financieel toezicht* (pp. 61-84), Deventer: Kluwer.
- Hattenbach L.C.M. en N.M. Zwikker (2009), Three lines of defence. Wat mag van een compliance functie worden verwacht?, in: *Jaarboek Compliance 2010* (pp. 97-110), Nederlands Compliance Instituut.
- Kaptein, M. (2008), *The living code – Embedding ethics into the corporate DNA*, Sheffield: Greenleave Publishing.
- Kaptein, M. en Ph. Wallage (2010), Assurance over gedrag en de rol van soft controls: een lonkend perspectief, *Maandblad voor Accountancy en Bedrijfseconomie*, vol. 84, no. 12 (december), pp. 623-632.
- KPMG (2010), Onderzoekresultaten soft controls bij interne accountantsdiensten, zie: http://www.kpmg.com/NL/nl/IssuesAndInsights/ArticlesPublications/Documents/PDF/Forensic/Onderzoeksres_soft_controls.pdf
- Lückerath-Rovers, M. (2010), Soft controls in corporate governance, in: *Jaarboek Compliance 2011* (pp 77-87), Nederlands Compliance Instituut.
- Monitoring Commissie Corporate Governance Code (2008), *De Nederlandse Corporate Governance Code*, 10 december 2008; zie: www.commissiecorporategovernance.nl/.
- NVB (Nederlandse Vereniging van Banken) (2009), *Code Banken*, 9 september 2009; zie: www.commissiecodebanken.nl/
- OECD –(Organisation or Economic Co-operation and Development) (2004), *Principles of Corporate Governance* – Preambule; zie: www.oecd.org/dataoecd/32/18/31557724.pdf
- Paape, L. en R.J. Hoff (2009), It's the behaviour, stupid! Over compliance en corporate governance, in: *Jaarboek Compliance 2010* (pp. 61-70), Nederlands Compliance Instituut.
- Pike, R. (2009), *Strengthening the three lines of defence*, CCH, Wolters Kluwer; zie: www.cch.com/press/news/CCHWhitePaper_3lines.pdf.
- Tillema, A.J.M., (2008), Enkele opmerkingen over falende compliance, in: M. Jurgens en R. Stijnen (red.), *Compliance in het financieel toezicht* (pp. 115-130), Deventer: Kluwer.
- Vink, H.J. en M. Kaptein (2008), Soft controls bij de rijksoverheid. De oorzaken van rechtmatigheidsfouten onderzocht, *Maandblad voor Accountancy en Bedrijfseconomie*, vol. 82, no. 6 (juni), pp. 256-263.
- Walker, D. (Chair) (2009), *A review of corporate governance in UK banks and other financial industry entities*, London, 16 July 2009; zie: www.lfhe.ac.uk/governance/aboutgovernance/walkerreportfinal.pdf