

DE COMPLIANCEFUNCTIE: MEER BLAUW OP STRAAT?

mr. F.M.A. 't Hart

1. Inleiding

Een integere en beheerste bedrijfsvoering is voor financiële ondernemingen een belangrijke voorwaarde om in aanmerking te komen en te blijven voor een vergunning om de bedrijfsactiviteiten uit te mogen oefenen. De compliancefunctie is samen met onder andere de risicobeheerfunctie en de interne controlefunctie, een belangrijk (voorgeschreven) instrument om een integere en beheerste bedrijfsvoering te waarborgen. Ondanks de importantie van de compliancefunctie kent de wettelijke regeling van deze functie – die per type financiële onderneming kan verschillen – een aantal oneffenheden. In dit artikel een schets van de belangrijkste wettelijke inrichtingseisen, in het bijzonder de voorschriften die voor de compliancefunctie gelden, waarbij de nadruk zal worden gelegd op banken, verzekeraars en beleggingsondernemingen.¹

2. Korte historische schets

De wettelijke regeling van de compliancefunctie of van de compliance officer kent geen noemenswaardige historie. Eén van de eerste regelingen waarin gerefereerd wordt aan de positie van de compliance officer is de op 1 april 1994 door De Nederlandsche Bank (DNB) uitgevaardigde Regeling privé-beleggingstransacties.² Deze regeling bevatte onder andere het voorschrift dat een compliance officer dient te worden belast met het toezicht op de naleving van de door de bank in het leven te roepen regels ten aanzien van privé-beleggingstransacties door of namens bestuurders, commissarissen en medewerkers. De positie van de compliance officer als zodanig was echter niet gereguleerd.

De verplichting om een compliancefunctie in te bedden in de bedrijfsvoering werd voor het eerst verplicht gesteld in de op 1 april 2001 door DNB uitgevaardigde

1 Dit artikel kan beschouwd worden als een geactualiseerde versie van mijn bijdrage aan de eerste druk van deze bundel.

2 Regeling van DNB ingevolge artikel 22 Wet toezicht kredietwezen met betrekking tot privé-beleggingstransacties van insiders, door leden van de Raden van Commissarissen of daarmee vergelijkbare organen en door bankmedewerkers niet zijnde insiders. Zie ook brief van DNB aan onder toezicht staande banken d.d. 11 januari 1994.

Regeling Organisatie en Beheersing (ROB).³ Deze regeling legt aan banken de verplichting op om te beschikken over een compliancefunctie. Artikel 69 ROB luidde:

‘De instelling beschikt over een onafhankelijke ‘compliance’ functie voor het toezicht op de naleving van de interne normen, voorschriften en gedragsregels alsmede voor het toezicht op de realisatie van bijstellingen naar aanleiding van signaleerde tekortkomingen en gebreken.’

Deze bepaling vormde destijds een onderdeel van in totaal vijf voorschriften die DNB aan banken oplegde, ter beheersing van hun integriteitsrisico's. Deze voorschriften kunnen worden beschouwd als de voorloper van de regels omtrent een integere en beheerste bedrijfsuitvoering zoals die thans zijn opgenomen in de Wet op het financieel toezicht (Wft).

Verzekeraars en beleggingsondernemingen volgden later. Voor verzekeraars trad op 1 januari 2014 de Regeling integriteitsrisico's verzekeraars in werking.⁴ Deze regeling kan beschouwd worden als het equivalent van de ROB voor banken. De implementatie van MiFID 1 in de Wft per 1 november 2007 bracht met zich dat beleggingsondernemingen eveneens onderworpen werden aan de verplichting om – kort gezegd – een compliancefunctie in hun organisatie in te bedden. De invloed van Europese regelgeving ten aanzien van de compliancefunctie was hiermee voor het eerst herkenbaar in de Nederlandse wet- en regelgeving. Overigens zijn niet alleen banken, verzekeraars en beleggingsondernemingen onderworpen aan de verplichtingen om een compliancefunctie in te bedden. In toenemende mate worden aanvullende eisen gesteld ten aanzien van de compliancefunctie van financiële ondernemingen en in toenemende mate worden steeds meer soorten financiële ondernemingen onderworpen aan de verplichting om een compliancefunctie in te stellen en in stand te houden. Een voorbeeld van dit laatste blijkt uit de ontwerpversie van de toekomstige Regeling integere bedrijfsvoering voor trustkantoren die voor het eerst aan trustkantoren de verplichting oplegt om niet alleen een compliancefunctie maar ook een auditfunctie in te stellen.⁵

3. Inrichtingseisen ter naleving integriteit

Financiële ondernemingen dienen te voldoen aan steeds meer wettelijke voorschriften omtrent de inrichting van hun bedrijfsvoering. In feite beperkt de wetgever de vrijheid van een financiële onderneming om haar bedrijfsvoering naar eigen inzicht in te richten door een aantal functies voor te schrijven en de wijze waarop die functies moeten worden uitgeoefend. De wettelijke inrichtingseisen drukken hierdoor een steeds grotere stempel op wie wat hoe moet doen. In de praktijk worden

3 De Regeling Organisatie en Beheersing is per 1 januari 2007 komen te vervallen in verband met de inwerkingtreding van de Wet op het financieel toezicht (Wft).

4 Regeling tegengaan van belangenverstremming en beheersing van integriteitsrisico's verzekeraars uitgevaardigd op 18 december 2003 door de Pensioen- en Verzekeringskamer ter uitvoering van de artikelen 2 lid 2 en 3 lid 3 van het Besluit integere bedrijfsvoering kredietinstellingen en verzekeraars.

5 Ontwerpversie Regeling integere bedrijfsvoering Wet toezicht trustkantoren van 1 oktober 2013.

deze functies veelal belichaamd door afdelingen waarvan de medewerkers zorg dragen voor het realiseren van de door de wetgever beoogde doelen. Hierna zal eerst worden ingegaan op de belangrijkste door de wetgever beoogde doelen om vervolgens in te gaan op de wettelijk voorgeschreven inrichtingseisen.

4. Open normen: integere en beheerste bedrijfsuitoefening

De compliancefunctie is tezamen met een aantal andere functies voor banken, verzekeraars en beleggingsondernemingen instrumenteel om aan twee belangrijke vergunningsvoorschriften te voldoen. Ten eerste, om te kunnen voldoen aan de eisen die worden gesteld omtrent een integere bedrijfsuitoefening. Ten tweede, om te kunnen voldoen aan de voorschriften omtrent een beheerste en integere bedrijfsvoering. Dit zijn de twee belangrijkste door de wetgever beoogde doelen. De inrichting van een compliancefunctie is instrumenteel in het realiseren van deze doelen.

4.1. Integere bedrijfsuitoefening

Het vergunningsvoorschrift dat betrekking heeft op het voeren van een integere bedrijfsuitoefening behelst de plicht voor banken en verzekeraars om een *adequaate beleid* te voeren dat een integere uitoefening van hun bedrijf waarborgt.⁶ Voor banken en verzekeraars dient dit beleid vier aangelegenheden 'tegen te gaan':

1. dat sprake is van belangenverstrengeling;
2. dat de bank of verzekeraar als financiële onderneming of haar werknemer strafbare feiten of andere wetsovertredingen begaan, die het vertrouwen in de financiële onderneming of in de financiële markten kunnen schaden;
3. dat wegens haar cliënten het vertrouwen in de financiële onderneming of in de financiële markten kan worden geschaad; en
4. dat handelingen door de financiële onderneming of door haar werknemers worden verricht die ingaan tegen hetgeen volgens ongeschreven rechten in het maatschappelijk verkeer betaamt en dat hierdoor het vertrouwen in de financiële onderneming of de financiële markten ernstig kan worden geschaad.

4.2. Beheerste en integere bedrijfsvoering

De voorschriften omtrent een integere bedrijfsuitoefening moeten niet verward worden met de voorschriften omtrent beheerste en integere bedrijfsvoering. Deze voorschriften bepalen dat banken en verzekeraars hun bedrijfsvoering zodanig dienen in te richten dat een beheerste en integere bedrijfsuitoefening gewaarborgd is.⁷ Bij deze voorschriften gaat het in belangrijke mate om de wijze waarop het bedrijf van de desbetreffende financiële onderneming wordt ingericht. Bij algemene maatregel van bestuur zijn aan de bedrijfsinrichting nadere regels gesteld.⁸ Deze regels hebben betrekking op drie aangelegenheden, te weten:

6 Art. 3:10 lid 1 Wft.

7 Zie art. 3:17 lid 1 Wft.

1. het beheersen van bedrijfsprocessen en bedrijfsrisico's,
2. integriteit; en
3. de soliditeit van de financiële onderneming.

Dergelijke voorschriften gelden ook voor beleggingsondernemingen met dien verstande dat geen regels worden gesteld ten aanzien van de soliditeit van de beleggingsonderneming. Wel worden aan beleggingsondernemingen voorschriften gesteld met betrekking tot de ordelijke en transparante financiële marktprocessen, zuivere verhoudingen tussen marktpartijen en zorgvuldige behandeling van cliënten en deelnemers. Onder dit laatste dienen zes aangelegenheden verstaan te worden:⁹

1. het waarborgen van de informatieverstrekking aan cliënten of deelnemers;
2. het waarborgen van de vastlegging van de relatie met cliënten of deelnemers;
3. het waarborgen van de zorgvuldige behandeling van cliënten of deelnemers;
4. het tegengaan van belangenconflicten tussen de financiële onderneming en cliënten maar ook tussen cliënten onderling;
5. het waarborgen van de rechten van cliënten of deelnemers; en
6. andere bij algemene maatregel van bestuur te bepalen onderwerpen.

Het bovenstaande maakt duidelijk met het oog op welke twee belangrijke open normen de wetgever inrichtingseisen heeft gesteld. Het voert te ver om in het kader van deze bijdrage een uitputtend overzicht te geven van de verschillende regels die gelden ten aanzien van een integere bedrijfsvoering en een beheerste en integere bedrijfsvoering. Hierna volgen enkele belangrijke nadere voorschriften die voor de compliancefunctie van belang zijn.

4.3. Analyse integriteitsrisico en integriteitsbeleid

Eén van de belangrijkste voorschriften waaraan een bank en verzekeraar moet voldoen, is om zorg te dragen voor een 'systematische analyse van integriteitsrisico's'.¹⁰ Een dergelijke verplichting geldt niet voor beleggingsondernemingen maar wel voor beheerders, beleggingsinstellingen en bewaarders.¹¹ Het begrip integriteitsrisico is overigens als volgt in het Bpr gedefinieerd:

'gevaar voor aantasting van de reputatie of bestaande of toekomstige bedreiging van vermogen of resultaat van de financiële onderneming als gevolg van een ontoereikende naleving van hetgeen bij of krachtens enig wettelijk voorschrift is voorgeschreven'.¹²

De hiervoor bedoelde systematische analyse van integriteitsrisico's strekt derhalve tot het hele speelveld van de betreffende financiële onderneming. De verplichting brengt niet louter en alleen met zich om de integriteitsrisico's in kaart te brengen

⁸ Zie art. 3:17 lid 2 Wft.

⁹ Zie art. 4:14 lid 2, onderdeel c Wft.

¹⁰ Zie art. 10 lid 1 Besluit prudentiële regels (Bpr).

¹¹ Zie art. 17 lid 1 Besluit Gedragstoezicht financiële ondernemingen (Bgf) en art. 23 lid 1 BCfo.

¹² Zie art. 1 Bpr.

maar tevens ook om zorg te dragen dat een integriteitsbeleid wordt opgesteld dat tot doel heeft deze integriteitsrisico's te beheersen. Dit integriteitsbeleid dient vervolgens haar neerslag te vinden in procedures en maatregelen. Zowel beleid als de getroffen procedures en maatregelen dienen vervolgens systematisch getoetst te worden.

4.4. Belangenverstrengeling

Een andere belangrijke verplichting waaraan banken en verzekeraars dienen te voldoen is het beschikken over procedures en maatregelen met betrekking tot het tegengaan van verstrengeling van privébelangen. De wet maakt daarbij onderscheid tussen vier groepen van personen:

1. personen die het beleid van de financiële onderneming bepalen;
2. groepsbestuurders;
3. commissarissen; en
4. andere werknemers of personen die in opdracht van de financiële onderneming op structurele basis werkzaamheden voor haar verrichten.

4.5. Customer due diligence

Banken en verzekeraars dienen met het oog op hun zogenaamde relationele integriteit te beschikken over procedures en maatregelen met betrekking tot de acceptatie van klanten: het zogenoemde customer due diligence-beleid. Een adequaat acceptatiebeleid en het identificeren en verifiëren van klanten vormt een belangrijk onderdeel van het waarborgen van de relationele integriteit van de financiële onderneming. Overigens zijn de specifieke nadere regels rondom customer due diligence, evenals de Wet ter voorkoming van witwassen en financiering van terrorisme, sinds de implementatie van de derde anti-witwasrichtlijn niet van toepassing op schadeverzekeraars.¹³

4.6. Soliditeit

De verplichting om de bedrijfsvoering zodanig in te richten dat deze een beheerste en integere bedrijfsuitoefening waarborgt, dient onder andere gericht te zijn op de waarborging van de soliditeit van de financiële onderneming. Deze verplichting is nader uitgewerkt in paragraaf 4.2 Bpr. De essentie van deze specifieke voorschriften is neergelegd in het eerste lid van artikel 23 lid 1 Bpr dat aan banken, verzekeraars en beleggingsondernemingen de verplichting oplegt een beleid te voeren, gericht op de beheersing van relevante risico's. Onder relevante risico's worden verstaan het concentratierisico, kredieten en tegenpartijrisico, liquiditeitsrisico, marktrisico, operationeel risico, renterisico voortvloeiend uit niet handelsactiviteiten, restrisico, securitisatierisico en tenslotte het verzekeringsrisico. De meeste van deze benoemde risico's zijn wettelijk gedefinieerd. Banken dienen tevens rekening te houden met

¹³ Zie *Kamerstukken II 2007/08*, 31 238, nr. 3, p. 12.

risico's die voortvloeien uit de macro economische omgeving waarin de onderneming actief is of die verband houden met de stand van de conjunctuurcyclus. Het aldus op te stellen beleid moet worden vastgelegd in procedures en maatregelen ter beheersing van de relevante risico's en dient geïntegreerd te zijn in de bedrijfsprocessen. De hier bedoelde procedures dienen onder meer te bestaan uit de autorisatieprocedures, limietstellingen, limietbewakingen en procedures en maatregelen voor noodsituaties.

Tot zover deze korte toelichting op enkele nadere voorschriften met betrekking tot de verplichting om een integrale en beheerste bedrijfsuitoefening te waarborgen. Welke inrichtingseisen heeft de wetgever nu gesteld?

5. Algemene inrichtingseisen

De Wft kent algemene en specifieke inrichtingseisen. Allereerst een korte uiteenzetting van de algemene inrichtingseisen.

5.1. Organisatiestructuur

De Wft stelt diverse eisen aan de wijze waarop banken en verzekeraars zijn georganiseerd. De meest bekende eisen hebben betrekking op het voorschrift om een statutaire directie te hebben die uit ten minste twee leden bestaat alsmede het voorschrift om een Raad van Commissarissen (RvC) te hebben die uit ten minste drie leden bestaat.¹⁴ De Wft kent daarnaast enkele algemene voorschriften omtrent de wijze waarop de organisatie is gestructureerd. Zo bepaalt artikel 17 Bpr dat de bedrijfsvoering van een bank en verzekeraar aldus moet worden ingericht dat deze mede omvat:

1. een duidelijke en adequate organisatiestructuur;
2. een duidelijke en adequate verdeling van taken, bevoegdheden en verantwoordelijkheden;
3. een adequate vastlegging van rechten en verplichtingen;
4. eenduidige rapportagelijnen; en
5. een adequaat systeem van informatievoorziening en communicatie.

Verder kent de Wft een aantal specifieke inrichtingseisen waarvan enkele belangrijke hierna worden vermeld.

Functiescheiding

Banken en verzekeraars dienen te beschikken over een adequate functiescheiding met het oog op een beheerste bedrijfsvoering.¹⁵ Deze verplichting kent geen nadere uitwerking. Beleggingsondernemingen zijn overigens niet aan een dergelijk voorschrift onderworpen.

¹⁴ Zie art. 3:19 Wft.

¹⁵ Zie art. 18 Bpr.

Administratie rechten en verplichtingen

Banken en verzekeraars dienen te voorzien in een juiste tijdige en volledige vastlegging van alle rechten en verplichtingen in de daartoe bestemde administratie.¹⁶ Dit voorschrift geldt overigens niet voor beleggingsondernemingen. Beleggingsondernemingen zijn daarentegen verplicht zorg te dragen voor procedures en maatregelen om de integriteit, voortdurende beschikbaarheid en beveiliging van geautomatiseerde gegevensverwerking te waarborgen.¹⁷

Informatievoorzieningen

Banken en verzekeraars dienen te beschikken over een informatiesysteem dat een effectieve beheersing van de bedrijfsprocessen en -risico's mogelijk maakt en dat voorts voorziet in interne en externe informatiebehoeften.¹⁸

Vakbekwaamheidseisen

Naast de wettelijke vakbekwaamheidseisen, die gelden voor bepaalde medewerkers,¹⁹ heeft de komst van het BGfo 3 met zich gebracht dat een financiële dienstverlener – waaronder banken en verzekeraars – ‘door middel van zijn bedrijfsvoering er tevens zorg voor draagt dat alle medewerkers te allen tijde vakbekwaam en op de hoogte zijn van de laatste actuele ontwikkelingen. Dat betekent dat het bedrijfsvoeringsmodel van de financiële dienstverlener erop moet zijn ingericht dat nieuwe kennis snel en adequaat binnen de onderneming wordt verspreid.’²⁰

Diverse functies

Banken, verzekeraars en beleggingsondernemingen dienen te beschikken over drie afzonderlijke functies die tot doel hebben een integere en beheerste bedrijfsvoering te waarborgen. Ten eerste, de interne auditfunctie. Ten tweede, de riskmanagementfunctie en ten derde, de compliancefunctie. Deze drie functies zullen hierna worden toegelicht.

5.2. Interne controlefunctie (audit)

De effectiviteit van (i) de organisatie-inrichting en (ii) de procedures en maatregelen dient ten minste één keer per jaar op onafhankelijke wijze te worden getoetst.²¹ Dit dient te geschieden door een organisatieonderdeel dat de *interne controlefunctie* uitoefent. Verreweg de meeste financiële ondernemingen laten in de praktijk deze functie uitoefenen door de interne accountantsdienst. Het Bpr stelt geen nadere voorschriften ten aanzien van deze interne controlefunctie, tenzij de desbetreffende bank beleggings-

16 Zie art. 19 Bpr.

17 Zie art. 31b BGfo.

18 Zie art. 20 Bpr.

19 Zie art. 22a Bpr.

20 Zie Nota van toelichting BGfo 3, *Stb.* 2012, 695, p. 64.

21 Zie art. 17 lid 4 Bpr.

diensten verleent of beleggingsactiviteiten verricht. Artikel 17a Bpr (en art. 31a BGfo) bepaalt dat in dat geval de interne controlefunctie tot taak heeft:

1. het vaststellen en uitvoeren van een controleplan om de deugdelijkheid en effectiviteit van de systemen, interne controleprocedures en regels van de bank te onderzoeken en te beoordelen;
2. het doen van aanbevelingen op basis van de onderzoeksresultaten;
3. het controleren of aan de aanbevelingen gevolg wordt gegeven; en
4. het ten minste één maal per jaar rapporteren aan de raad van commissarissen inzake aangelegenheden met betrekking tot de interne controle en de genomen maatregelen ingeval van gesignaleerde tekortkomingen.

Externe accountant

De interne controlefunctie wordt deels 'aangevuld' door wettelijk voorgeschreven werkzaamheden van de externe accountant. Artikel 22 Bpr verplicht banken en verzekeraars om bij het onderzoek van hun jaarrekening aan de externe accountant te verzoeken om op hoofdlijnen de toereikendheid van de organisatie-inrichting en risicobeheersing te toetsen en te beoordelen.

5.3. Risicobeheerfunctie (risk management)

Het zesde lid van artikel 23 Bpr bepaalt onder andere dat een bank en verzekeraar dienen te beschikken over een onafhankelijke risicobeheerfunctie die op systematische wijze een onafhankelijk risicobeheer uitvoert dat gericht is op het identificeren, meten en evalueren van die risico's waaraan de financiële onderneming is of kan worden blootgesteld. Het risicobeheer wordt zowel uitgevoerd ten aanzien van de financiële onderneming als geheel als ten aanzien van de verscheidene bedrijfsonderdelen.

Indien de bank tevens beleggingsdiensten verleent of beleggingsactiviteiten verricht, dient de afdeling die belast is met het risicobeheer tevens controle uit te oefenen op:

1. de deugdelijkheid en effectiviteit van de vastgestelde procedures en maatregelen;
2. de mate waarin de financiële ondernemingen en haar werknemers de procedures en maatregelen naleven; en
3. de deugdelijkheid en effectiviteit van de maatregelen die genomen zijn om de gesignaleerde tekortkomingen of gebreken op te heffen.²²

Evenals de interne controlefunctie en de compliancefunctie (hierover later meer) dient ook de risicobeheerfunctie ten minste één keer per jaar te rapporteren aan de RvC.²³ Er worden, anders dan ingeval van de interne controlefunctie en de compliancefunctie, geen nadere eisen gesteld ten aanzien van de inhoud of de in de rapportage te behandelen onderwerpen. Wél schrijft de wet voor dat in een jaarlijkse rapportage met name moet worden aangegeven of maatregelen zijn genomen

²² Zie art. 24b Bpr.

²³ Zie art. 24b lid 2 Bpr.

in geval van gesignaleerde onvolkomenheden. Paragraaf 4.2 Bpr bevat voorts een keur aan specifieke voorschriften op het gebied van risicomanagement. Daartoe behoort onder andere de verplichting om procedures vast te leggen voor de acceptatie, aanpassing, vernieuwing en herfinanciering van kredieten, het in stand houden van procedures en maatregelen die gericht zijn op het beheersen van het operationeel risico en het beschikken over solide, doeltreffende en alomvattende strategieën en procedures aan de hand waarvan doorlopend kan worden nagegaan of ervoor zorg wordt gedragen dat de hoogte, samenstelling en verdeling van haar eigen vermogen aansluit op de omvang en aard van haar huidige en mogelijk toekomstige risico's.

6. De compliancefunctie

De compliancefunctie is voor banken en verzekeraars voorgeschreven in artikel 21 lid 1 Bpr en voor beleggingsondernemingen in artikel 31c BGfo. De wettelijke regulering van de compliance officer is relatief summier. Voor zover de positie is gereguleerd, houdt de regulering nauw verband met de voorschriften waaraan een financiële onderneming moet voldoen om een beheerste en integere bedrijfsuitoefening te waarborgen, in het bijzonder om te beschikken over een compliancefunctie. De vereisten die de Wft ten aanzien van de compliance officer stelt zijn onder te verdelen in twee groepen. Ten eerste, kwalitatieve eisen ten aanzien van de compliance officer zelf en ten tweede, eisen ten aanzien van de door de compliance officer te verrichten taken.

6.1. Kwalitatieve vereisten compliance officer

De kwalitatieve vereisten die aan een compliance officer gesteld worden zijn op hun beurt te verdelen in twee categorieën. Ten eerste, een categorie die betrekking heeft op de positie van een compliance officer binnen de onderneming en ten tweede, de eigenschappen waarover een compliance officer dient te beschikken.

Positie compliance officer

De eisen die ten aanzien van de positie van de compliance officer binnen de financiële onderneming worden gesteld zijn neergelegd in het eerste lid van artikel 21 Bpr voor banken en verzekeraars en in artikel 31c BGfo voor beleggingsondernemingen. Deze wettelijke bepalingen schrijven voor dat de financiële onderneming dient te beschikken over een organisatieonderdeel dat op een onafhankelijke en effectieve wijze de compliancefunctie uitoefent.

Het eerste vereiste houdt in dat sprake is van een *organisatieonderdeel*. Hoewel de toelichting op deze wettelijke bepaling erg summier is, mag aangenomen worden dat de wetgever daarmee heeft beoogd voor te schrijven dat de compliancefunctie uitgeoefend moet worden door een managerial (niet juridisch afgescheiden) apart aangestuurde afdeling. Dit houdt mijns inziens een (verkapt) voorschrift van functiescheiding in. Dit betekent dat de compliancefunctie moet worden uitgeoefend door personen die als zodanig daarvoor zijn aangesteld en organisatorisch niet

verweven zijn met andere activiteiten of taken die binnen de onderneming worden verricht. Voorts is aannemelijk – hoewel dit niet met zoveel woorden uit dit voorschrift blijkt – dat de compliancefunctie moet worden uitgeoefend door een afdeling of door personen die als zodanig binnen de onderneming herkenbaar zijn. Het voorschrift dat sprake moet zijn van een organisatieonderdeel hoeft geen beletsel te vormen om de compliancefunctie te laten uitoefenen door personen (of een persoon) die ook andere werkzaamheden verricht, mits de aard van deze werkzaamheden zich niet verzet tegen het tweede vereiste dat de wetgever aan de compliance officer stelt, te weten dat deze onafhankelijk is.

Het tweede vereiste is dat de compliancefunctie op *onafhankelijke wijze* wordt uitgeoefend. Dit vereiste is niet nieuw en was reeds opgenomen in de ROB.²⁴ Van een daadwerkelijke onafhankelijke uitoefening van de compliancefunctie in de strikte zin des woords kan geen sprake zijn. De woordkeuze ‘onafhankelijk’ is ongelukkig omdat deze naar mijn mening niet anders geïnterpreteerd moet worden dan ‘zelfstandig’. Immers, de uiteindelijke verantwoordelijkheid voor het functioneren en het waarborgen van de compliancefunctie ligt bij de statutaire directie van de financiële onderneming. In de verhouding tussen de compliance officer en de bestuurder heeft de bestuurder het laatste woord. Dit is inherent aan één van de wezenlijke kenmerken van de arbeidsovereenkomst, te weten dat sprake is van een (hiërarchische) zeggenschapsrelatie. Van ‘onafhankelijk’ in de zin van artikel 31c BGfo is sprake indien zorg is gedragen voor een functiescheiding als hiervoor bedoeld. Dit houdt niet alleen in dat sprake is van uitoefening van een als zodanig herkenbare compliancefunctie door personen die geen daarmee tegenstrijdige werkzaamheden verrichten, maar ook dat deze personen rechtstreeks rapporteren aan de statutaire directie van de financiële onderneming. Indien niet rechtstreeks aan het bestuur van de financiële onderneming gerapporteerd zou worden, dan zou zulks afbreuk kunnen doen aan de mogelijkheid om zelfstandig werkzaamheden te kunnen verrichten zonder dat daarop invloed wordt uitgeoefend door andere afdelingen en personen (anders dan het bestuur zelf). Het Bazels Comité beschrijft vier kenmerken van onafhankelijkheid die de compliancefunctie zou dienen te hebben.²⁵ In de eerste plaats dient de compliancefunctie een formele status te hebben. In de tweede plaats dient een compliance officer aangesteld te worden die verantwoordelijk is voor de coördinatie van ‘the management of the compliance-risk’. In de derde plaats dient de compliance officer niet zodanig gepositioneerd te worden dat hij een conflict of interest heeft. In de vierde plaats dient de compliance officer toegang te hebben tot alle relevante informatie.

Het derde en laatste vereiste is dat de compliancefunctie op *effectieve wijze* wordt uitgeoefend. Het effectiviteitsvereiste betekent dat de personen die belast zijn met de uitoefening van de compliancefunctie door (het bestuur van) de financiële onderneming in staat moeten worden gesteld om hun werkzaamheden effectief

²⁴ Zie art. 69 ROB.

²⁵ Zie principle 5 en articles 20-32 van het Basel Committee on Banking Supervision ‘Compliance and the compliance function in banks’ d.d. april 2005.

uit te oefenen. Dit betekent dat de compliance officer in staat moet worden gesteld om ten minste de wettelijk aan de compliancefunctie voorgeschreven taken te kunnen verrichten. Een financiële onderneming heeft de compliancefunctie niet adequaat ingericht indien de compliance officer een 'papieren bestaan' leidt.

Vaardigheden compliance officer

Het Bpr (en het BGfo) schrijft voor dat de compliance officer, althans het organisatieonderdeel dat de compliancefunctie uitoefent, dient te beschikken over de nodige autoriteit, middelen, deskundigheid en toegang tot alle noodzakelijke informatie om de taken onafhankelijk en effectief te kunnen uitoefenen.²⁶ Het lijkt erop dat dit *eigenschappen* zijn waaraan de compliance officer moet voldoen. Mijns inziens zijn dit voorschriften die aan de financiële onderneming de verplichting opleggen een kwalitatief toereikende en goed functionerende compliancefunctie in stand te houden. Zo moet het vereiste dat de compliance officer beschikt over de nodige autoriteit en deskundigheid niet anders geïnterpreteerd worden dan een inrichtingsvereiste (autoriteit) en een opleidingsvereiste waaraan de financiële onderneming moet voldoen (zorg ervoor dat de persoon die de compliancefunctie uitoefent deskundig is en zijn vakbekwaamheid kan onderhouden).

Overigens stelt de Wft geen nadere eisen ten aanzien van de deskundigheid. In de praktijk is een aantal initiatieven ontplooid teneinde compliance officers een herkenbare status als vakbekwame professional te geven waarvan het meest bekende initiatief afkomstig is van de Vereniging van Compliance Officers om in samenwerking met het Dutch Securities Institute compliance officers in een openbaar register op te nemen. Deze registratie kan alleen plaatsvinden indien aan bepaalde voorwaarden is voldaan.²⁷

6.2. Wettelijke taken compliance officer

De Wft draagt aan het organisatieonderdeel dat de compliancefunctie uitoefent een aantal wettelijke taken op. De belangrijkste taken staan omschreven in het tweede lid van artikel 21 Bpr (voor banken en verzekeraars) en in artikel 31c BGfo (voor beleggingsondernemingen). Het gaat daarbij in totaal om vijf uit te voeren taken.

Taak I: controle naleving wetgeving

De eerste taak is om de naleving van wettelijke regels en interne regels te controleren.

Uit de toelichting is niet op te maken wat de reikwijdte is van het begrip 'wettelijke en interne regels'. Een restrictieve interpretatie van dit begrip zou kunnen inhouden dat de compliance officer tot taak heeft om de naleving van wettelijke voorschriften te controleren die betrekking hebben op de integere en beheerste bedrijfsuitoefening, inclusief de daarop betrekking hebbende en de uit wettelijke voorschriften voortvloeiende interne regels. Een extensieve uitleg zou inhouden dat de compliance officer alle

²⁶ Zie art. 21 lid 3 Bpr en art. 31c lid 3 BGfo.

²⁷ Zie http://www.dsi.nl/index.php?sid=306&mod_id=1300&l=ned (2 juni 2014).

– dus zonder enige vorm van beperking – wettelijke en interne regels dient te controleren. De restrictieve interpretatie verdient de voorkeur. Dit houdt overigens niet in dat de compliance officer slechts hoeft toe te zien dat de bepalingen die betrekking hebben op de beheerste en integere uitoefening worden nageleefd, maar dat de compliance officer zorg draagt voor controle op de naleving van alle wettelijke en interne regels die voor een beheerste en integere bedrijfsuitoefening van belang zijn. Er zal derhalve een materieel verband dienen te zijn tussen de te controleren regels en de door de Wft vereiste beheerste en integere bedrijfsuitoefening. Mijns inziens dient de compliance officer zich daarbij primair te richten op wetgeving die bij een gebrekkige naleving kan leiden tot een integriteitsrisico.

Taak II: adviseren beleggingsmedewerkers

De tweede taak die de compliance officer dient te vervullen is het adviseren van de personen die verantwoordelijk zijn voor het verlenen van beleggingsdiensten bij de naleving van wettelijke regels en interne regels. Aangezien deze taak niet eerder in de Wft of in de ROB was opgenomen en zijn bestaan dankt aan de MiFID Richtlijn, kan de reikwijdte van het begrip 'wettelijke regels en interne regels' niet meer behelzen dan de publiekrechtelijke voorschriften die als gevolg van de implementatie van de MiFID Richtlijn in de Wft zijn opgenomen.

Taak III: toezien deugdelijkheid en effectiviteit

De derde taak die de compliance officer moet vervullen is het toezien op de deugdelijkheid en effectiviteit van de interne regels en procedures.

Taak IV: beoordelen maatregelen ter opheffing van gebreken

De vierde taak die de compliance officer dient uit te oefenen is het beoordelen van de effectiviteit van de procedures die zijn opgesteld en maatregelen die zijn genomen om de gesignaleerde onvolkomenheden bij de naleving van wettelijke regels en interne regels op te heffen. Deze taak moet gezien worden in het licht van het wettelijk voorschrift dat tekortkomingen in de integere bedrijfsuitoefening door de compliance officer gesignaleerd dienen te worden en dat de compliance officer toezicht dient te houden op de benodigde bijstellingen.²⁸ Frappant is dat het wettelijk voorschrift niet inhoudt dat compliance officer er op toe dient te zien dat de gesignaleerde onvolkomenheden daadwerkelijk opgeheven worden.

Taak V: rapporteren

Ten slotte dient de compliance officer ten minste jaarlijks aan bestuurders en RvC te rapporteren over aangelegenheden met betrekking tot de naleving van wettelijke en interne regels. Daarbij dient de compliance officer te vermelden of maatregelen zijn genomen in het geval van gesignaleerde tekortkomingen. Hoewel niet met zoveel woorden tot uitdrukking gebracht, is het aannemelijk dat de wetgever heeft beoogd dat de door de compliance officer te verstrekken rapportage is gericht aan de statutaire directie en aan de RvC. Hierbij zal worden bedoeld op de statutaire directie en de RvC als vennootschapsrechtelijk orgaan en niet dat de rapportage

²⁸ Zie art. 10 leden 5 en 6 Bpr.

dient te zijn gericht aan een (willekeurig) lid van de Raad van Bestuur of van de RvC. Het ligt eveneens voor de hand dat de desbetreffende rapportage wordt geagendeerd, toegelicht en besproken in een reguliere bestuurs- of de commissarissenvergadering. Evenmin wordt het vereiste gesteld dat de rapportage *schriftelijk* wordt gedaan.²⁹

Deze rapportageplicht betekent de facto dat de wetgever het bestuur en de RvC heeft willen verplichten om kennis te nemen van de bevindingen van de compliance officer. Een soortgelijke rapportageplicht is ook opgenomen ten aanzien van de bevindingen van de riskmanager en de interne accountant. Het staat buiten kijf dat deze rapportageplicht in de praktijk tot spanningen kan leiden tussen de compliance officer en het bestuur. Menig bestuurders zal immers grip willen hebben en invloed willen uitoefenen op de rapportage die de compliance officer (mede) aan de RvC uitbrengt.

7. Verhouding compliance versus internal audit en risk management

Funcitiescheiding en vermenging

Het ligt niet voor de hand om de personen die belast zijn met de compliancefunctie tevens (deels) te belasten met de risicobeheerfunctie, laat staan de interne controlefunctie. De Wft verbiedt zulks niet maar vanuit een oogpunt van functiescheiding en deskundigheid zou zulks niet wenselijk zijn.

Versus internal audit

Zowel de interne controlefunctie als de compliancefunctie hebben een controlerende taak. De interne controlefunctie is gericht op het toetsen van de effectiviteit van (i) de organisatie-inrichting en (ii) procedures en maatregelen. In het feit dat de interne controlefunctie primair een *toetsende* rol heeft, is het verschil gelegen met de compliancefunctie. Een tweede belangrijk verschil is dat de compliancefunctie primair gericht is op de controle van naleving van *wet- en regelgeving*. Dit laatste betekent dat de compliance officer juridische affiniteit dient te hebben of het vermogen om in samenwerking met (interne dan wel externe) juristen zijn werkzaamheden te verrichten. Overigens behoort tot de controlerende taak van de interne controlefunctie ook het toetsen van de compliancefunctie.

Versus risk management

De risicobeheerfunctie is primair gericht op het identificeren, meten en evalueren van – met het oog op de aan financiële ondernemingen gestelde soliditeiteisen – relevante risico's, waaronder het krediet- of verzekeringsrisico. De vraag doet zich voor of de compliance officer gehouden is te controleren in welke mate een financiële onderneming de soliditeiteisen (kapitaalsvereisten) naleeft. In de praktijk wordt dit meestal aan de risicobeheerfunctie overgelaten. In het licht van de hierboven uiteengezette wettelijke systematiek en de wettelijke definitie van integriteitrisico zou de conclusie moeten zijn dat de compliance officer eveneens moet toezien op naleving van de gestelde soliditeiteisen.

²⁹ Art. 9 lid 2 MiFID Uitvoeringsrichtlijn bevat wel een schriftelijkheidsvereiste.

De interne controlefunctie dient de ter beheersing van de relevante risico's genomen maatregelen en procedures te toetsen, de compliancefunctie dient te controleren of de wettelijke en interne regels op dit punt worden nageleefd en de risicobeheerfunctie dient de risico's te identificeren en te meten.

8. Internationale standaarden

De regulering van de compliancefunctie in Nederland kan niet los gezien worden van de ontwikkelingen op Europees niveau. Hierna zal worden ingegaan op de belangrijkste internationale standaarden die door de Europese toezichthouders zijn vastgesteld voor verzekeraars, banken en beleggingsondernemingen. Alle drie daarvoor in aanmerking komende Europese toezichthouders hebben richtsnoeren uitgevaardigd met daarin nadere eisen ten aanzien van de inrichting van de bedrijfsvoering, waaronder de compliancefunctie.

8.1. Verzekeraars: Solvency II en EIOPA

Voor verzekeraars geldt dat deze naast een risicobeheerfunctie, een internal auditfunctie en een compliancefunctie tevens dienen te beschikken over een actuariële functie. De Solvency II Richtlijn alsmede de EIOPA richtsnoeren beschouwen deze functies als een onmisbaar onderdeel van het governance-systeem.³⁰ In de preambule van Solvency II Richtlijn wordt met zoveel woorden opgemerkt dat de functies die tot het governance-systeem behoren, beschouwd worden als sleutelfuncties en dus ook als belangrijke en kritieke functies. Aan die sleutelfuncties worden specifieke eisen gesteld, waaronder het vereiste dat alle personen die betrokken zijn bij de uitvoering van sleutelfuncties (waaronder mede begrepen de compliancefunctie) deskundig en betrouwbaar dienen te zijn. Behoudens de interne auditfunctie, kunnen in kleinere en minder complexe ondernemingen de sleutelfuncties door een persoon of een organisatorische eenheid worden vervuld. Daarbij maakt de Solvency II Richtlijn onderscheid tussen de interne controlefunctie waarvan de compliancefunctie onderdeel uitmaakt en de interne auditfunctie. Zo wordt voorgeschreven dat een doeltreffend systeem van interne controle in ieder geval de administratieve en financiële verslagleggingsprocedures, een interne controlekader, passende rapportageregelingen op alle niveaus en een compliancefunctie bevat.³¹ Blijkens Solvency II wordt van de compliancefunctie verwacht dat deze aan het bestuurlijk, beleidsbepalend of toezichthoudend orgaan (in Nederland veelal de statutaire directie en de RvC) advies uitbrengt over de naleving van de voorschriften ingevolge Solvency II. Tevens dienen de mogelijke gevolgen van de verrichtingen door de onderneming beoordeeld en de compliance risico's vastgesteld en beoordeeld te worden. De richtsnoeren voor het governance-systeem verwijst uitdrukkelijk naar Solvency II en de daarin opgenomen voorschriften. Hoewel de compliancefunctie als een sleutelfunctie wordt benoemd ontbreekt elk specifiek

³⁰ Zie preambule 30 Solvency II en Richtsnoer 5 (1.22) van de EIOPA richtsnoeren voor het governance-systeem 2013 (EIOPA-CP-13/08 NL).

³¹ Zie art. 46 lid 1 Solvency II Richtlijn.

richtsnoer voor de compliancefunctie terwijl specifieke richtsnoeren wel bestaan voor alle andere sleutelfuncties.

8.2. Banken: EBA richtsnoeren

Voor banken zijn naast het reeds in 2004 verschenen rapport van het Bazels Comité,³² met name de EBA richtsnoeren met betrekking tot de interne governance van belang.³³ De EBA benoemt één richtsnoer dat specifiek ziet op de compliancefunctie en dit richtsnoer bestaat uit zes onderdelen.

Het eerste onderdeel van de richtsnoer is evident, te weten dat een compliancefunctie ingesteld dient te worden ter beheersing van het compliancerisico. Dit risico wordt omschreven als het bestaand of verwacht financieel risico voor – kort gezegd – het niet-naleven van wet- en regelgeving, maar ook van overeenkomsten, voorgeschreven praktijken en ethische normen. Daarnaast behoren reputatierisico's tot het compliancerisico.

Het tweede onderdeel van het richtsnoer komt erop neer dat door de bank een compliancebeleid moet worden vastgesteld en goedgekeurd dat aan het voltallige personeel kenbaar moet worden gemaakt. Mijns inziens dient dit richtsnoer aldus te worden begrepen dat de statutaire directie verantwoordelijk is voor het compliancebeleid en dat het personeel ook onderworpen dient te worden aan dit beleid.

Het derde onderdeel houdt in dat een permanente en doeltreffende compliancefunctie moet worden ingesteld waarbij kennelijk wordt bedoeld op een organisatorische eenheid. Tevens dient een zogenaamde compliance officer te worden aangesteld belast met de leiding van deze eenheid. Het tweede richtsnoer voegt daaraan toe dat in kleinere en minder complexe banken de compliancefunctie gecombineerd of ondersteund kan worden door de risicobeheerfunctie of ondersteunende functies. Als concrete voorbeelden worden genoemd HR en Legal.

Het vierde onderdeel houdt in dat de compliance officer erop toe moet zien dat het compliancebeleid wordt nageleefd. Daarover dient de compliance officer verslag uit te brengen aan de statutaire directie en de RvC, inclusief de benodigde aanbevelingen. Overigens begrijp ik dit richtsnoer zo dat compliance officer erop moet toezien dat het compliancebeleid wordt nageleefd. De naleving van het compliancebeleid als zodanig is en blijft de verantwoordelijkheid van de statutaire directie.

Het vijfde onderdeel verplicht de compliance officer advies uit te brengen over de naleving van wet- en regelgeving. Tevens dient de compliance officer het mogelijk effect te beoordelen van veranderingen in wet- en regelgeving op de activiteiten van de bank.

32 Basel Committee on Banking Supervision, 'Compliance and the compliance function in banks', april 2005.

33 EBA-richtsnoeren inzake interne governance (GL 44) van 27 september 2011.

Ten slotte het zesde onderdeel van dit richtsnoer. Dit onderdeel van het richtsnoer houdt in dat de compliance officer dient te verifiëren of nieuwe producten en nieuwe procedures voldoen aan het geldende juridisch kader en aan bekende op handen zijnde wijzigingen in wet- en regelgeving.

8.3. *Beleggingsondernemingen: ESMA*

Beleggingsondernemingen en banken die beleggingsdiensten verlenen dienen rekening te houden met de richtsnoeren die door ESMA zijn uitgevaardigd.³⁴ ESMA heeft elf richtsnoeren opgesteld die betrekking hebben op de compliancefunctie, waarvan negen voor de praktijk het meest van belang zijn.

Deze richtsnoeren bevatten meer gedetailleerde aanbevelingen dan de richtsnoeren van EIOPA of EBA. Een kort overzicht:

- De compliancefunctie moet middels een op risico gebaseerde benadering doeltreffend opereren.³⁵
- De compliancefunctie moet aan de hand van een toezichtsprogramma alle 'beleggingsactiviteiten' monitoren, inclusief de bijbehorende prioriteiten.³⁶
- De compliance rapporteert haar bevindingen aan het hoogste management.³⁷
- Beleggingsondernemingen moeten de compliancefunctie in staat stellen effectief te opereren.³⁸
- De compliancefunctie moet voldoende capaciteiten en vakbekwaam zijn aan haar taken te kunnen vervullen.³⁹

³⁴ ESMA Richtsnoeren met betrekking tot bepaalde aspecten van de MiFID-eisen voor de compliancefunctie, 25 juni 2012.

³⁵ 'Investment firms should ensure that the compliance function takes a risk-based approach in order to allocate the function's resources efficiently. A compliance risk assessment should be used to determine the focus of the monitoring and advisory activities of the compliance function. The compliance risk assessment should be performed regularly to ensure that the focus and the scope of compliance monitoring and advisory activities remain valid.'

³⁶ 'Investment firms should ensure that the compliance function establishes a monitoring programme that takes into consideration all areas of the investment firm's investment services, activities and any relevant ancillary services. The monitoring programme should establish priorities determined by the compliance risk assessment ensuring that compliance risk is comprehensively monitored.'

³⁷ 'Investment firms should ensure that the regular written compliance reports are sent to senior management. The reports should contain a description of the implementation and effectiveness of the overall control environment for investment services and activities and a summary of the risks that have been identified as well as remedies undertaken or to be undertaken. Reports must be prepared at appropriate intervals and at least annually. Where the compliance function makes significant findings, the compliance officer should, in addition, report these promptly to senior management. The supervisory function, if any, should also receive the reports.'

³⁸ 'Investment firms should ensure that the compliance function fulfils its advisory responsibilities including: providing support for staff training; providing day-to-day assistance for staff and participating in the establishment of new policies and procedures within the investment firm.'

³⁹ 'When ensuring that appropriate human and other resources are allocated to the compliance function, investment firms should take into account the scale and types of investment services, activities and ancillary services undertaken by the investment firm. They should also provide

- De compliancefunctie moet permanent functioneren.⁴⁰
- De compliancefunctie moet onafhankelijk kunnen opereren.⁴¹
- De compliancefunctie moet niet worden vermengd met de interne auditfunctie. Wel met andere functies zolang dat de effectiviteit en onafhankelijkheid van de compliancefunctie niet aantast.⁴²
- De compliancefunctie mag (deels) worden uitbesteed mits adequaat gecontroleerd.⁴³

ESMA heeft op 22 mei 2014 een consultation paper gepubliceerd. Eén van de daarin door ESMA opgenomen voorstellen is om de essentie van de hierboven onder 1, 2, 3, 6 en 7 vermelde richtsnoeren te verankeren in de Uitvoeringsverordening MiFID II.⁴⁴ Tot zover deze korte uiteenzetting.

9. Slotbeschouwingen

Het bovenstaande laat zien dat de inrichtingseisen voor financiële ondernemingen verschillen en ook de eisen die aan de compliancefunctie worden gesteld. Of dat beschouwd dient te worden als een omissie of dat de geschetste oneffenheden voor de praktijk onoverkomelijk zijn, kan niet met zekerheid gesteld worden. Van groot belang is het besef dat de waarborging van een integere en beheerste bedrijfsvoering niet uitsluitend gerealiseerd kan worden door allerlei inrichtingseisen, waaronder een compliancefunctie, wettelijk verplicht te stellen. De wil en het streven naar een

compliance staff with the authority necessary to exercise their duties effectively, as well as access to all relevant information concerning the investment services and activities as well as ancillary services undertaken. The compliance officer should have sufficiently broad knowledge and experience and a sufficiently high level of expertise so as to be able to assume responsibility for the compliance function as a whole and ensure that it is effective. The compliance officer should have sufficiently broad knowledge and experience and a sufficiently high level of expertise so as to be able to assume responsibility for the compliance function as a whole and ensure that it is effective.'

40 'MiFID requires investment firms to ensure that the compliance function performs its tasks and responsibilities on a permanent basis. Investment firms should therefore establish adequate arrangements for ensuring the responsibilities of the compliance officer are fulfilled when the compliance officer is absent, and adequate arrangements to ensure that the responsibilities of the compliance function are performed on an ongoing basis. These arrangements should be in writing.'

41 'Investment firms should ensure that the compliance function holds a position in the organisational structure that ensures that the compliance officer and other compliance staff act independently when performing their tasks. The compliance officer should be appointed and replaced by senior management or by the supervisory function.'

42 'An investment firm should generally not combine the compliance function with the internal audit function. The combination of the compliance function with other control functions may be acceptable if this does not compromise the effectiveness and independence of the compliance function. Any such combination should be documented, including the reasons for the combination so that competent authorities are able to assess whether the combination of functions is appropriate in the circumstances.'

43 'Investment firms should ensure that all applicable compliance function requirements are fulfilled where all or part of the compliance function is outsourced.'

44 Zie ESMA 'Consultation paper MiFID II/MiFIR', 22 mei 2014, p. 18-22 (ESMA/2014/549).

integere en beheerste bedrijfsuitoefening zal in de eerste geplaatst getoond moeten worden door het hoogste management. Het is de intrinsieke integriteit van het hoogste management dat allesbepalend is voor een integere en beheerste bedrijfsuitoefening. Dat neemt niet weg dat het hoogste management ervoor dient te zorgen dat een compliancefunctie wordt ingesteld die voldoet aan de wettelijke inrichtingseisen en die tenminste zichtbaar gevolg heeft gegeven aan de belangrijkste open normen, waaronder het beschikken over een analyse van de integriteitsrisico's en een integriteitsbeleid. Illustratief voor het belang hiervan zijn de bevindingen van DNB omtrent de compliancefunctie bij het voormalige Bouwfonds:

'Parallel hieraan liep ook een onderzoek van De Nederlandsche Bank bij Bouwfonds.

De toezichthouder onderzocht de opzet van de compliance-organisatie en de opzet en werking van de CDD-beheersingsmaatregelen. De aanleiding voor dit onderzoek was de overname in 2004 door Bouwfonds van de vastgoedportefeuille van Staal Bankiers, het gegeven dat niet eerder een onderzoek naar compliance en customer due diligence had plaatsgevonden en door De Nederlandsche Bank onderkende hoge inherente risico's in het cliëntenbestand. Daarbij speelde de negatieve publiciteit rond Bouwfonds door haar relatie met Endstra een rol.

De uitkomsten van het onderzoek waren niet mals. Bij Bouwfonds ontbrak een onafhankelijke, centrale compliance-functie. Gedocumenteerde risicoanalyses waren niet voorhanden. Er was geen centraal geformuleerd beleid ter beheersing van integriteitsrisico's bij klanten. De wijze waarop gerapporteerd werd vertoonde tekortkomingen. De onderzoekers hadden een negatieve indruk van de projectmatige aansturing van customer due diligence.⁴⁵

Uiteraard kan het in de praktijk voorkomen dat een compliance officer zelf van goede wil is, maar zich geconfronteerd voelt met management dat onvoldoende prioriteiten toekent aan een integere en beheerste bedrijfsvoering. Deze compliance officer dient niet in zijn schulp te kruipen maar zijn ongenoegen (onderbouwd) te uiten jegens het management.

Een voor de praktijk illustratief voorbeeld zijn de uitlatingen van de voormalig compliance officer van het voorheen beursgenoteerde en inmiddels gefailleerde Van der Moolen. Zo citeerde de Ondernemingskamer van het Hof Amsterdam in zijn arrest waarin het verzochte enquêteverzoek werd toegewezen:

'E. Seinstra, compliance officer van Van der Moolen, heeft op 13 augustus 2008 aan Den Drijver een brief met onder meer de volgende inhoud geschreven:

je (hebt) mij gezegd dat je het er niet mee eens bent dat ik regelmatig laat weten wat ik van situaties vind en dat ik geen waardeoordelen mag geven. Daarop heb ik geantwoord dat het beoordelen van situaties, vooral situaties met integriteitaspecten, en het geven van een waardeoordeel over zo'n situatie,

⁴⁵ R.J. Hoekstra en J. Rijns, *Het rapport van de evaluatiecommissie nationalisatie SNS Reaal*, Amsterdam: Uitgeverij Balans 2014, p. 215.

behoort tot mijn taak als compliance officer en general counsel. (...) Ik heb ook laten weten dat ik de problemen, deels integriteitissues, die [Wolfswinkel] had gesignaleerd ook ken en zijn bezorgdheid daarover deel. Wat mij telkens opvalt is dat jij mijn signaleringen over integriteitissues meteen naast je neerlegt, omdat je ze gewoon niet serieus neemt of wilt nemen. (...)

Het is teleurstellend en bovenal onzorgvuldig dat jij mij (...) niet in de gelegenheid hebt gesteld ook mijn toedracht van het besprokene kenbaar te maken. Je wilde uitsluitend je eigen visie aan mij laten horen. (...) Ik constateer dat jij (...) ongefundeerde beschuldigingen aan mijn adres uit. Met dergelijke beschuldigingen op basis van horen zeggen, zonder dat ik zelf mijn mening heb kunnen geven, heb ik heel veel moeite. (...)

Het vorenstaande en de vele compliance- en integriteitissues die ik op talloze vergaderingen en bijeenkomsten aan de orde heb gesteld en die niet worden aangepakt maken dat ik mijn werkzaamheden niet kan verrichten. Wat de compliance- en integriteitissues betreft ben ik inmiddels zelfs in gewetensnood komen te verkeren (...).⁴⁶

Ook wil het in de praktijk voorkomen dat een compliance officer een beroep doet op AFM of DNB teneinde binnen de onderneming meer aandacht te krijgen voor de integere en beheerste bedrijfsvoering. De Commissie Scheltema:

‘Tegelijkertijd geeft DNB in een gesprek op 20 september 2006 aan een minder positief beeld te hebben ten aanzien van de compliance, het interne toezicht op de naleving van wet- en regelgeving. DSB scoort op 8 van de 10 principes ontwikkeld door het Bazel's Comité voor banktoezicht van de Bank Internationale Betalingen (BIB) een onvoldoende. Door de Compliance Officer van DSB wordt dit gewijd aan de bedrijfscultuur: dat DSB nog te veel een commercieel bedrijf is en te weinig een bank. Tegelijkertijd is naar de mening van de Compliance Officer de toezichthouder te geduldig, het helpt als DNB zegt dat iets moet gebeuren, want dan gebeurt het pas.’⁴⁷

De bovenstaande voorbeelden spreken voor zich. Een integere en beheerste bedrijfsvoering is bovenal een kwestie van ‘cultuur en gedrag’ en niet zozeer het naleven van allerlei compliance eisen. Mijns inziens moet er serieus rekening mee gehouden worden dat de effectiviteit van meer en meer nadere regelgeving op dit gebied gering is. Personen dienen zoveel mogelijk hun eigen verantwoordelijkheden te nemen en zo nodig te leren die te nemen. Het in het leven roepen van meer regelgeving of meer compliance officers is niet per definitie het juiste medicijn, zelfs als de patiënt (ernstig) ziek is. Niet altijd helpt een pleister.

⁴⁶ Zie uitspraak Hof Amsterdam 5 juli 2010, JOR 2010/305.

⁴⁷ Zie ‘Rapport van de commissie van Onderzoek DSB Bank’, Den Haag 23 juni 2010, p. 43.