De Compliancefunctie

De circulaire van de NBB_2012_14 en van de FSMA – 2012-21 dd. 4 december 2012

Geert Maelfait

Compliance Officer

Delta Lloyd life NV

(deze bijdrage is in eigen naam geschreven en vertolkt geenszins standpunten van het bedrijf).

Inhoudstafel

1. Inleiding

Deze bijdrage behandelt de prudentiële controleaspecten van de Circulaire NBB_2012_14 en van de FSMA 2012-21, hierna genoemd "Circulaire Compliance". Worden in deze bijdrage evenwel niet behandeld:

- het Principe 7 inzake onafhankelijkheid (zie daarvoor de bijdrage van dhr. Dupont);
- de erkenningsprocedure bij de FSMA (zie de bijdrage van mevr. Decoster en dhr. Lannoy);
- detailanalyses van de belangrijkste werkdomeinen.

In hun brief van 5 juli 2012 aan de sectorverenigingen waarin een ontwerpcirculaire ter consultatie werd meegedeeld, gaven de Voorzitter van de FSMA en de Gouverneur van NBB de reden van de aanpassing aan:

> "*Het ontwerp is een aanpassing van de bestaande circulaires aangaande compliance en strekt ertoe rekening te houden met:*
>
> *- De nieuwe toezichtsarchitectuur en de behoeften van zowel de Bank als de FSMA;*
> *- De ontwikkelingen in de compliancefunctie gedurende de voorbije jaren;*
> *- De evolutie in het deugdelijk bestuur van de instellingen (bijvoorbeeld de respectieve rol van de raad van bestuur, de effectieve leiding en het auditcomité, de organisatie van de compliancefunctie op groepsniveau).*
>
> *In vergelijking met de bestaande circulaires, bevat het ontwerp een uitgebreidere omschrijving van de opdrachten en de governance van de compliancefunctie. Er wordt meer aandacht besteed aan de onafhankelijkheid van de compliancefunctie en er wordt nader ingegaan op de organisatie van de compliancefunctie in een groepscontext en bij kleinere instellingen."*

We stellen ook vast dat de internationale organismen veel aandacht aan de controlefuncties besteden en dat hun werk de Belgische Toezichthouders inspireerde. In dit verband kunen we verwijzen naar het rapport van ESMA (European Securities and Markets Authority) van 6 juli 2012, getiteld "Guidelines on certain aspects of the MiFID compliance requirements", en het consultatieve document van de Bank for International Settlements van December 2011 met als titel " The internal audit function in banks" (principe 7 – nrs. 37 tot 39, en principe 13 – nrs. 55 tot 59).

In de Circulaire Compliance wordt de Compliancefunctie meteen sterk geduid:

> " *De compliancefunctie is voor de financiële instellingen van fundamenteel belang voor de beheersing van hun integriteit en voor de bescherming van de financiële consument"*
> (Circulaire Compliance, Aanhef, blz 2)

> "*De Compliancefunctie is belast met het toezicht op de naleving van de wettelijke en/of reglementaire integriteits- en gedragsregels, die van toepassing zijn op de instellingen;"*
> (Circulaire Compliance, 1.2.1., blz 4).

Meteen wordt de functie als een sleutelfunctie voor het beheer van een verzekeringsonderneming aangemerkt, naast de (minimaal) 2 leden van de effectieve leiding of het Directiecomité, de Interne Auditor, de riskfunctie en de actuariële functie. Beide toezichthouders geven er de voorkeur aan dat er per onderneming slechts één leidende Compliancefunctie zou zijn (dhr. M. Pickeur, NBB, studiedag IFE, 6 december 2012).

De Circulaire Compliance werd op de website geplaatst op 18 december en vervangt met onmiddellijke datum de circulaire PPB/D.255 van 10 maart 2005, gericht aan de verzekeringsondernemingen.

In onderstaande bijdrage worden achtereenvolgens volgende onderwerpen behandeld, waarbij maximaal naar een pragmatische benadering gestreefd werd:

- de verschillen met de vorige circulaire,
- de wettelijke basis en de aanverwante circulaires,
- de domeinen,
- de definities en opdrachten (principe 1),
- governance van de compliancefunctie (principes 2 tot 7),
- organisatie van de compliancefunctie (principes 9 tot 11),
- de proportionaliteitsregels (principes 12 tot 14).

2. Vind de ? verschillen …

- Primeur: een gemeenschappelijke Circulaire Compliance van beide toezichthouders samen.
- Alle financiële instellingen worden aangesproken in de Circulaire Compliance (nr.1.1.), met uitzondering van de bijkantoren van de in de EER gevestigde instellingen en de pensioenfondsen. De bijkantoren van de in de EER gevestigde instellingen zijn omwille van het Europese paspoort in principe vrijgesteld, doch worden wel aangeschreven via de techniek van de “maatregel van algemeen belang”. De pensioenfondsen worden uitsluitend door de FSMA gecontroleerd, en voor hen geldt nog steeds de Circulaire CBFA CPP-2007-2 WIBP van 23 mei 2007.
- De vroegere Circulaire D.255 telde 10 bladzijden, de huidige 24.
- De vroegere Circulaire D.255 telde 10 principes, de huidige 14. Twee principes werden niet langer als dusdanig opgenomen:
    - het vroegere principe 6 over de prioritaire werkdomeinen viel weg en werd vervangen door de opsomming van deze domeinen in deel 1 betreffende het toepassingsgebied;
    - het vroegere principe 10 inzake het complianceoverleg werd niet als afzonderlijk principe weerhouden, maar gedeeltelijk in het nieuwe principe 7 geïncorporeerd.
- Drie nieuwe principes voeren heel duidelijk het COSO-model in met de drie “lines of defence”, meer bepaald:
    - opdracht en methodologie als tweedelijnsfunctie (principe 1);
    - rapportering (principe 6);
    - deel van transversale controlefuncties (principe7).

- Drie nieuwe principes definiëren de proportionaliteit:
    - werken binnen een groepsstructuur (principe 12);
    - een beroep doen op een externe deskundige (principe 13);
    - de regeling voor kleinere instellingen (principe 14).
- Sinds februari 2009 werd de wettelijke basis in art 14 bis van de Controlewet verduidelijkt, waarmee hierdoor op de Europese directieve van Solvency II vooruitgelopen werd.
- Het aantal werkdomeinen voor de Compliancefunctie in de verzekeringsonderneming is verhoogd van de "prioritaire" 5 domeinen, naar ten minste 15. De effectieve leiding kan er bovendien nog aan toevoegen …
- De werkdomeinen worden opgedeeld naargelang de financiële sector (de verzekeringsondernemingen komen aan bod op blz. 6 tot 8) en volgens de bevoegdheden van de respectievelijke toezichthouders.
- We lezen voor het eerst heldere definities van "Compliance", "Effectieve Compliance", "Compliancerisico", en de "Compliancefunctie". Hopelijk leidt dit ertoe dat zij voortaan in alle circulaires op een coherente wijze zullen worden gehanteerd.
- De adviezen van de Compliancefunctie krijgen een bijzondere kracht: "comply or explain". Ze zijn met andere woorden niet vrijblijvend, zonder daarbij bindend te worden. De effectieve leiding kan er bijgevolg wel van afwijken, maar enkel mits motivering en ze draagt de volle verantwoordelijkheid.
- De principes worden als norm gesteld en niet als aanbeveling. Ze worden veelal uitgebreid met good practices. De rechtsgrond en –kracht van deze "soft law" is ons evenwel niet altijd duidelijk.

3. Wettelijke basis en circulaires

De Circulaire D255 was gebaseerd op het oude artikel 14 bis van de Controlewet (wet van 9 juli 1975 betreffende de controle der verzekeringsondernemingen) en stelde:

> *"De verzekeringsondernemingen moeten beschikken over een beleidsstructuur, een administratieve en boekhoudkundige organisatie en interne controleprocedures die specifiek zijn afgestemd op de activiteiten die zij uitoefenen".*

Het gebruik van deze tekst als basis voor een verplichting tot het aanstellen van een onafhankelijke werknemer die binnen de onderneming ongebreideld kan rondkijken, onderzoeken, adviseren en er zowel intern als extern over rapporteren, komt ongetwijfeld neer op een wel zeer ruime interpretatie ervan.

De Wet van februari 2009 op de herverzekeringen en de aanpassing van de Controlewet, evenals het KB van 3 maart 2011 met betrekking tot het Twin Peaks-model, brachten een grondige herwerking van het artikel 14bis teweeg. Voortaan werden de Compliancefunctie, interne controlevereiste, interne audit enz. in de wet opgenomen. Getuige de nieuwe tekst:

Art. 14bis

§ 1. De verzekeringsonderneming beschikt over een voor haar activiteiten of voorgenomen activiteiten passende beleidsstructuur, administratieve en boekhoudkundige organisatie, controle- en beveiligingsmaatregelen met betrekking tot de elektronische informatieverwerking, en interne controle. Zij houdt daarbij rekening met de aard, de omvang en de complexiteit van deze activiteiten en de eraan verbonden risico's.

§ 2. De verzekeringsonderneming beschikt over een passende beleidsstructuur, waaronder inzonderheid dient te worden verstaan :
- een coherente en transparante organisatiestructuur, met inbegrip van een passende functiescheiding;
- een duidelijk omschreven, transparant en samenhangend geheel van verantwoordelijkheidstoewijzingen; en
- passende procedures voor de identificatie, de meting, het beheer en de opvolging van en de interne verslaggeving over de belangrijke risico's die de verzekeringsonderneming loopt ingevolge haar activiteiten of voorgenomen activiteiten.

§ 3. De verzekeringsonderneming organiseert een passende interne controle waarvan de werking minstens eenmaal per jaar wordt beoordeeld. Voor haar administratieve en boekhoudkundige organisatie organiseert zij een systeem van interne controle dat een redelijke mate van zekerheid verschaft over de betrouwbaarheid van het financiële verslaggevingsproces, zodat de jaarrekening in overeenstemming is met de geldende boekhoudreglementering.
De verzekeringsonderneming neemt de nodige maatregelen om permanent te beschikken over een passende onafhankelijke interneauditfunctie.
*De verzekeringsonderneming werkt een passend integriteitsbeleid uit dat geregeld wordt geactualiseerd. **[**Onverminderd artikel 87bis van de wet van 2 augustus 2002 neemt zij**]** de nodige maatregelen om blijvend te kunnen beschikken over een passende onafhankelijke compliancefunctie, om de naleving door de onderneming, haar bestuurders, effectieve leiding, werknemers en gevolmachtigden te verzekeren van de rechtsregels in verband met de integriteit van haar bedrijf.*
De verzekeringsonderneming beschikt over een passende onafhankelijke risicobeheerfunctie.

*§ 4. De **[**Bank**]** kan, onverminderd het bepaalde bij §§ 1, 2 en 3, nader bepalen wat moet worden verstaan onder een passende beleidsstructuur, een passende interne controle, een passende onafhankelijke interneauditfunctie, **[**een passende risicobeheerfunctie en, op advies van de FSMA, een passende onafhankelijke compliancefunctie**]**.*

§ 5. Onverminderd de bevoegdheden van het wettelijk bestuursorgaan inzake vaststelling van het algemeen beleid als bepaald bij het Wetboek van Vennootschappen, nemen de personen belast met de effectieve leiding van de verzekeringsonderneming, in voorkomend geval het directiecomité, onder toezicht van het wettelijk bestuursorgaan de nodige maatregelen voor de naleving van het bepaalde bij §§ 1, 2 en 3.
Het wettelijk bestuursorgaan van de verzekeringsonderneming controleert minstens eenmaal per jaar, in voorkomend geval via het auditcomité, of de onderneming beantwoordt aan het bepaalde bij §§ 1, 2 en 3 en het eerste lid van deze paragraaf, en neemt kennis van de genomen passende maatregelen.
*De personen belast met de effectieve leiding, in voorkomend geval het directiecomité, lichten minstens eenmaal per jaar het wettelijk bestuursorgaan, de **[**Bank**]** en de erkende revisor in.*

In de Wet Financieel Toezicht werd het artikel 87bis ingevoegd. Met betrekking tot het bevoegdheidsdomein van de FSMA verduidelijkt dit de opdracht, aanstelling en erkenning van Complianceofficers:

Art. 87bis

§ 1. De (…) verzekeringsondernemingen (…) stellen voor het naleven van artikel 45 §1 bedoelde regels (hierna) één of meerdere complianceofficers aan die de vereiste professionele betrouwbaarheid en passende kennis en ervaring bezitten.
Deze personen voeren de volgende opdrachten uit onder de verantwoordelijkheid van de effectieve leiding:
a) de controle op en de evaluatie van de aangepastheid en de efficiëntie van het beleid, de procedures en de maatregelen die de naleving beogen van de in art 45 bedoelde regels
b) het adviseren en het bijstaan van de relevante personen opdat deze hun bovenvermelde verplichtingen zouden nakomen.
De betrokken ondernemingen brengen de FSMA onverwijld op de hoogte van de aanstelling alsook van de wijzigingen in de functie van een complianceofficer.

§ 2. De Complianceofficers (…) dienen door de FSMA te worden erkend. De betrokken ondernemingen dienen daartoe een aanvraag tot erkenning in bij de FSMA.
Bij reglement bepaalt de FSMA:
- de vereisten inzake kennis, ervaring, vorming en professionele eerbaarheid;
- de modaliteiten van de erkenningsprocedure.
De FSMA publiceert op haar website een lijst met de complianceofficers die door haar erkend zijn bij de betrokken ondernemingen.

§ 3. In geval een complianceofficer niet langer beantwoordt aan de erkenningsvoorwaarden kan de FSMA overgaan tot herroepen van de erkenning op grond van een gemotiveerde beslissing en na de betrokkene te hebben gehoord. De FSMA kan beslissen deze herroeping publiek te maken door publicatie op haar website.

De uitwerking van artikel 14bis in Circulaires komt erop neer dat de stap van een bij KB bevestigd Reglement wordt overgeslagen, hoewel dit vanuit juridisch oogpunt het uniform vastleggen van definities en hun rechtskracht had kunnen verstevigen. De lezing van de vele circulaires inzake governance en controle wordt hierdoor niet vergemakkelijkt.

De Circulaire D255 werd impliciet aangevuld of herzien door volgende circulaires:

- De Circulaire PPB-2006-1-CPA inzake de **gezonde beheerspraktijken bij uitbesteding door verzekeringsondernemingen** (Circulaire uitbesteding).
  Deze omzendbrief legt taken op aan de Compliancefunctie op het vlak van de beslissing tot uitbesteding (Principe 3), de clausule over integriteitstoezicht en gedragsregels in de schriftelijke overeenkomst (Principe 5) en de controle door Interne Audit en Compliance (Principe 8).
- De Circulaire CPA-2008-13A inzake **Risicobeheer van de verzekeringsondernemingen**.
  Hierin worden risicomodellen en het beheer ervan behandeld. Kennis hiervan door de Compliance Officers en geregeld overleg hierover met de Risk Officers, is belangrijk gezien de vraag naar een *risk based approach.*

- De Circulaire PPB-2006-8-CPA inzake **Interne controle en interne audit**.
  Risicobeheersing, interne controlemaatregelen, en onpartijdigheid van de functie worden hierin al meer uitgewerkt, en dienden als voorbeeld voor de huidige teksten maar ook voor de inspecties van de Toezichthouders. Deze Circulaire zou in 2013 herzien worden.
- De Circulaire PPB-2007-6-CPB-CPA over de prudentiële verwachtingen van de CBFA inzake het **deugdelijk bestuur van financiële instellingen**.
  Beginsel V benoemt de onafhankelijke controlefuncties. Beginsel VIII formuleert de vereiste van een integriteitsbeleid. Punt F behandelt het deugdelijk bestuur in een groepscontext.
- De Circulaire PPB-2006-13-CPB-CPA over de **uitoefening van externe functies door de leiders van gereglementeerde ondernemingen**
  Deze omzendbrief beperkt de externe mandaten voor de effectieve leiding en de sleutelpersonen en onderwerpt het aanvaarden van dergelijke mandaten aan een bijzondere procedure binnen de onderneming, evenals aan een meldingsplicht aan de toezichthouder. Bij KB van 20 juni 2012 werd het Reglement van de NBB van 6 december 2011 gevalideerd. Dit vormt een nieuwe reglementaire basis voor deze circulaire.
- De Circulaire CBF2009-26 met beoordeling van het **interne controlesysteem** in een jaarlijks rapport.
- De Circulaire CBFA-2009-33 van 19 november 2009 over de **Actuariële functie.**
- De Circulaire CBFA-2009-34 van 26 november 2009 inzake **Behoorlijk beloningsbeleid.**
  Het beloningsbeleid met betrekking tot de effectieve leiding en de sleutelpersonen binnen een onderneming is ook op de compliancefunctie toepasselijk. De Compliance Officer wordt zowel bij de opstelling van dit beleid als bij de jaarlijkse toetsing ervan betrokken. Het beleid dient gericht te zijn op het voorkomen van belangenconflicten.
- De Circulaire CBFA-2011-09 en 2010-09 inzake de **Preventiewet Witwassen**.

De Compliance Officer en de effectieve leiding moeten daarenboven rekening houden met de wetteksten, reglementen en circulaires per werkdomein:

- De **Preventiewet witwassen** en haar reglementaire uitwerking vereist een "Verantwoordelijke Antiwitwassen" per onderneming en bepaalt zijn bevoegdheden, plichten en verantwoordelijkheid. De toezichthouders leggen deze functie bij de Compliancefunctie, met als gevolg dat deze regels omwille van hun karakter van openbare orde voorrang krijgen boven de hier besproken Circulaire Compliance.
- De **Privacywetgeving,** meer in het bijzonder het ontwerp van Europese verordening, vereist per onderneming ook een onafhankelijke "Privacy & data protection Officer". De toezichthouders leggen ook deze functie bij de Compliancefunctie, met als gevolg dat deze regels eveneens voorrang krijgen boven de hier besproken Circulaire Compliance.
- Naar aanleiding van de *Twin peaks*-hervorming van 2011 werd het art. 45 in de **Wet financieel toezicht** (2002) ingevoerd met hierin de catch-all-bepaling betreffende de bevoegdheid die aan de FSMA wordt toegekend. Deze zal de grondslag vormen voor nieuwe reglementen en wellicht ook voor taken, toegewezen aan de Compliancefunctie in de verzekeringssector.

4. Domeinen

4.1. Domeinen volgens de Circulaire

De aanhef van punt 1.2.1, blz 4, is duidelijk:

"het betreft ten minste de domeinen die hierna worden vermeld."

De opsomming die volgt, is dus niet limitatief. Ze kan aangevuld worden door de toezichthouders en door de effectieve leiding van de onderneming. De opgesomde domeinen dienen wel verplicht door de Compliancefunctie opgenomen te worden.

De Circulaire Compliance deelt de domeinen op per toezichthouder. Dit is nuttig voor het kennen van hun onderlinge bevoegdheidsverdeling (zie nummer 1.2.1.b, blz. 6 tot 8).

Schematisch overzicht

NBB	*FSMA*	*Andere regelgevingen en toezichtsorganen*	
		Regelgeving	*Toezicht*
Preventiewet Witwassen	*WFT art 45 §2-*	*W. Antidiscriminatie*	*Centrum Gelijke Kansen*
Bijzondere Mechanismen	*Bescherming verzekeringnemer, cliënteninformatie en publiciteit*	*W. Marktpraktijken en consumenten-bescherming*	*Economische inspectie*
Onverenigbaarheid mandaten, Fit&Proper	*W. Verzekeringsbemiddeling*	*W. Privacy*	*Privacycommissie*
Controlewet – art 14bis	*Controlewet – art 14bis*	*Codes Assuralia*	*Compliance Officer*
Deugdelijk bestuur	*W. Hypothecair krediet*	*Interne codes*	*Compliance Officer*
Uitbesteding	*W. Discriminatie – art.12*	*Financiële embargo's*	*CFI*
Behoorlijk beloningsbeleid	*Behoorlijk beloningsbeleid*	*Fatca, Bribery act*	*buitenlandse instellingen*

De in D.255 vermelde domeinen worden hernomen:

- Preventie witwassen;
- Preventie bijzondere mechanismen (fiscaal voorkomingsbeleid);
- Privacywetgeving;
- Antidiscriminatiewetgevingen;
- Consumentenbescherming en informatieverplichtingen, voorzien door de verzekeringswetgeving (incl. Wet aanvullende pensioenen) en de wet Hypothecaire krediet (onder meer publiciteitsregels).
  Deze wetgevingen bevatten zeer veel bepalingen van dwingend recht ter bescherming van de verzekeringsnemer of verzekerden;
- Verzekeringsbemiddelingswet.
  Punt 5.2 van de Circulaire D.255 inzake de controle op de tussenpersonen – andere dan gevolmachtigde agenten - werd geschrapt. Die opdracht noodzaakt o.i. een bijkomende wettelijke basis.

De nieuw toegevoegde domeinen zijn:

- Integriteitsaspecten behandeld in de Circulaires Deugdelijk bestuur, Uitbesteding, Behoorlijk beloningsbeleid en Externe mandaten: passende organisatie, geschiktheid bestuurders en leiders, naleving onverenigbaarheidsregels, belangenconflicten, behoorlijk beloningsbeleid, het hoofdstuk over het integriteitsbeleid in de Memo Governance. De ontwerp circulaire Fit & Proper voegt nieuwe taken toe;

- Reglementen op basis van art. 45 §§2 en 3 WFT tot bevordering van loyale, billijke en professionele behandeling van de belanghebbende partijen. ("Klant belang centraal"). Dit artikel stipuleert:

  § 2. Teneinde de loyale, billijke en professionele behandeling van de belanghebbende partijen te bevorderen kan de Koning, op advies van de FSMA en de Bank, voor de instellingen (inz. verzekeraars en verzekeringstussenpersonen), de regels bedoeld in § 1,eerste lid, 3°, uitbreiden met bepalingen die betrekking hebben op :

  - de informatieverplichtingen aan de belanghebbende partijen;
  - de contractuele verplichtingen en voorwaarden;
  - de verplichting de belangen van de cliënten optimaal te verzorgen (zorgplicht);
  - regelingen inzake de voordelen die verband houden met de verstrekte diensten;
  - het verstrekken van diensten via internet;
  - de publiciteitsregels;
  - de klachtenbehandeling;
  - transparantie over prijzen, vergoedingen en kosten;
  - toegankelijkheid van de verstrekte diensten.

  Hij kan inzonderheid verschillende regels bepalen naargelang het gaat om professionele of niet-professionele belanghebbende partijen of tussen sommige categorieën van professionele belanghebbende partijen onderling.

  § 3. Voor de toepassing van dit artikel worden met « belanghebbende partijen » bedoeld, de cliënten en potentiële cliënten van de betrokken ondernemingen, de verzekeringsnemers, de verzekerden en de begunstigden van de bij de verzekeringsondernemingen afgesloten verzekeringsovereenkomsten.

- Gedragscodes Assuralia: reclame bij individuele levensverzekeringen, schuldsaldoverzekering voor kandidaat-verzekerden met en verhoogd gezondheidsrisico, schadebeheer van ernstig gekwetsten, maatschappelijk verantwoorde tak 23-verzekeringen, de antiwitwascode.

- Wet van 6 april 2010 Marktpraktijken en consumentenbescherming (onder meer: reclame, deloyale praktijken, verkoop),

- De naleving van interne waarden en gedragscodes.

4.2. Andere domeinen toegewezen door de effectieve leiding

De effectieve leiding/het directiecomité kan domeinen toevoegen aan de Compliancefunctie, maar op basis van een risicoanalyse en in overleg met het Auditcomité.

De Circulaire Compliance vermeldt als voorbeelden de naleving van financiële embargo's en buitenlandse wetgeving zoals US FATCA en UK Bribery act. Het louter benoemen in deze Amerikaanse of Britse wetgevingen van de compliancefunctie volstaat op zichzelf niet om de daadwerkelijke verantwoordelijkheid automatisch bij de functie neer te leggen of alle uit te voeren verplichtingen aan de functie op te leggen. De kernelementen van deze wetgevingen vinden we overigens ook in het Belgisch recht bij de opdrachten van de compliancefunctie terug:

- het bestrijden van corruptie maakt een essentieel deel uit van het integriteitsbeleid (Circulaire Deugdelijk Bestuur, nr.60);

- het principe 'Ken-uw-klant', meer bepaald 'ken zijn economisch profiel', is een basisaspect van de identificatieverplichting in de Preventiewet.

De opsomming bij de bancaire instellingen is een andere bron van mogelijke domeinen, hetzij in de realiteit van vandaag, hetzij na eventuele toekomstige bijkomende reglementering door FSMA of wetgever. Daarbij komen volgende domeinen in het vizier:

- De MiFID gedragsregels.
  In de ontwerpdirectieve IMD II worden belangrijke stukken van deze regelgeving die de niet-professionele klant beschermen, toepasselijk gesteld op de verkoop van de levensverzekeringen.

- De regels inzake marktmisbruik.
  Daarbij denken wij zowel aan de regels inzake "insider trading" of "personal trading" in verzekeringsondernemingen die beursgenoteerd zijn of deel van een dergelijke groep uitmaken, als aan het beheer van de assets. Dit is a fortiori het geval indien de belanghebbenden in zgn. afgezonderde fondsen rechtstreeks of onrechtstreeks het assetbeheer bepalen.

- De opvolging van de klachtenbehandeling.
  Hier hebben we niet zozeer de behandeling zelf op het oog, maar wel het in kaart brengen van de tendensen bij de klachten, het behartigen van het klantenbelang, de naleving van de informatieplicht … Binnen de banksector dienen de MiFID-gerelateerde klachten door de compliancefunctie expliciet te worden gemonitored om te waarborgen dat bij het oplossen ervan voorrang wordt verleend aan de waarden (integriteit / klantbelang) boven de wettelijke normen.

In het kader van een efficiënte aansturing binnen de verzekeringsonderneming kunnen, ons inziens, de hierna volgende domeinen toegewezen worden aan de Compliancefunctie. Daarbij spelen overwegingen van uiteenlopende aard een rol, zoals de wenselijkheid om een domein in zijn integraliteit toe te kennen in plaats van over diverse functies te versnipperen, de toepasbaarheid van de discretie- en onafhankelijkheidsregels van de functie en/of de

optimalisering van de deskundigheid van de Compliance medewerkers. Telkens moet daarbij gewaakt worden over het eerbiedigen van de onafhankelijkheid en dient elk mogelijk belangenconflict vermeden te worden. Volgende domeinen komen in dit geval in beeld:

- de opvolging van de Controlewet;
- de opvolging van alle principes uit de Circulaires Deugdelijk bestuur en Uitbesteding;
- de toepassing van het Mededingingsrecht;
- het centraliseren en opvolgen van de Policies van de onderneming;
- het functioneren van de compliancefunctie als contactpunt voor derden (zoals fiscus, economische inspectie en gerechtelijke autoriteiten);
- het contactpunt voor de Klokkenluidersregeling, die ontegensprekelijk van elk degelijk integriteitsbeleid wezenlijk deel uitmaakt;
- het coördineren van fraudebestrijding, waarbij dit logisch voortvloeit uit de noodzaak en taak tot het bewaken van integriteit en reputatie; binnen een globaal integriteitskader bestrijden de inspectiediensten verzekeringsfraude in de eerste lijn; centraal dient men te waken over het vermijden en bestrijden van interne fraudes en fraudes door tussenpersonen;
- het volledige klachtenbeheer, al lijkt dit enkel mogelijk binnen kleinere verzekeringsinstellingen.

5. Definities en kernopdracht van de Compliancefunctie

5.1. Definities

In de Circulaire D.255 luidde de definitie nog als volgt:

> "*Compliance is een onafhankelijke functie binnen de organisatie, gericht op het onderzoek naar en het bevorderen van de naleving door de onderneming van de regels die verband houden met de integriteit van het verzekeringsberoep. (…)*"

Binnen deze omschrijving werden derhalve het begrip, de functie en de opdracht vermengd.

In de Circulaire Deugdelijk Bestuur leest men onder nr.60:

> "*Daarom is het belangrijk dat de leiding de strategische doelstellingen en de ondernemingswaarden van de financiële instelling vastlegt, alsook interne gedragscodes of formele voorschriften, die bepalen hoe de activiteiten worden gevoerd in integriteit (…) Voor de toepassing van deze waarden is het belangrijk dat de leiding zichzelf hoogstaande en strikte gedragsregels oplegt en het goede voorbeeld geeft ('tone at the top'). (…) De compliancefunctie vervult een belangrijke rol in de handhaving van het door de instelling vastgelegde beleid.*"

De nieuwe Circulaire Compliance geeft afzonderlijke definities. Voor een goed begrip worden de teksten hierna integraal geciteerd en de kernbegrippen in vetjes weergegeven. In het Compliance

Charter nemen we best de begrippen “Compliance”, “compliancefunctie” en “Compliancerisico” op, om dit aan alle stakeholders (medewerkers, tussenpersonen, klanten) te duiden.

5.1.1. *Het begrip “Compliance”.*

Tekst:

> *“Compliance is een onderdeel van de bedrijfscultuur van **elke instelling** dat de nadruk legt op eerlijkheid en integriteit, het naleven van **hoge ethische normen** bij het zakendoen en het naleven van zowel de **geest als de letter van de toepasselijke regelgeving.** Zowel de instelling als haar medewerkers dienen zich **integer te gedragen, dit is eerlijk, betrouwbaar en geloofwaardig. Cliënten** dienen steeds op een **loyale, billijke en professionele wijze te worden behandeld.**”*

De nieuwe circulaire stelt een hogere toetsingsnorm in, die ons inzien best in de Circulaire Deugdelijk bestuur opgenomen worden en bij uitbreiding zelfs in het wetgevend kader. De jurist zoekt tevergeefs naar wettelijke omschrijvingen van een aantal vage begrippen of blanco normen, zoals: “hoge ethische normen”, “geest van de wet”, “loyaal”, “billijk”.

Elke Compliance Officer krijgt geregeld te horen dat “men niet katholieker moet zijn dan de paus”. We kunnen nu naar de Circulaire Compliance verwijzen als bon mot. Overigens valt op dat bij het testen van integriteitsdilemma’s het overgrote deel van de medewerkers op eenzelfde wijze blijkt te reageren en zich daarbij op gemeenschappelijke basiswaarden en het gezond verstand baseert.

Een pragmatische aanpak om in het creëren van deze cultuur vooruitgang te boeken, kan bestaan uit volgende stappen:

- vooreerst de letter van de regelgeving duiden;
- vervolgens binnen dit kader de probleemloze, “veilige” zone aangeven en hetgeen buiten het kader valt als “zwarte” of “rode” zone aanstippen;
- hetgeen binnen het kader valt, maar buiten de veilige zone, als “grijze” of “oranje” zones duiden en hierop de genoemde begrippen hanteren om aldus een praktisch toepasselijk en voorspelbaar beleid te realiseren.

De integriteitsnorm kan ook perfect op sectorniveau of via wetgeving als basisnorm vastgelegd worden. Compliance als bedrijfscultuur kan, noch mag concurrentieverstorend werken. Bij de omschrijving van het begrip “Compliancerisico” vermeldt de toezichthouder trouwens:

> “***Geloofwaardigheid is de basis om actief te kunnen en mogen zijn in de financiële sector.”***

5.1.2. *Het begrip "Effectieve compliance"*

Tekst:

> *"Effectieve compliance houdt in dat de **waarden** die de instelling nastreeft, **ingebed zijn** in de manier waarop deze zaken doet. Effectieve compliance betekent dus dat de instelling niet enkel haar eigen belang nastreeft, maar **rekening houdt met de noden en belangen van haar cliënten.** Dit houdt ook in dat de instelling en haar medewerkers een integere aanpak hanteren wanneer ze worden geconfronteerd met situaties die mogelijk strijdig zijn met de waarden die de instelling nastreeft. Zowel de instelling als haar medewerkers dienen bereid te zijn hun gedrag bij te sturen."*

Men kan in deze definitie drie opdrachten onderscheiden. Hoe kunnen we die aanpakken?

- <u>De waarden inbedden in de dagelijkse bedrijfsvoering.</u>

  Dit vereist duidelijke procedures en communicatie, het invoeren van een meldingsplicht voor de atypische situaties (de grijze zones) en het bepalen van een escalatieproces. Een onderzoek bij een Amerikaans bedrijf toonde aan dat van de 100 integriteitsincidenten, de medewerkers de helft niet durfden te melden, maar dat anderzijds van de incidenten die ze wel aan hun leiding hadden gemeld, ruim 60 % werd "geseponeerd". Conclusie: op 100 incidenten bleken slechts 20 ervan gekend en aangepakt. Meldingsplicht voor de leidinggevenden en verplichte aanpak van elk gemeld probleem levert snel een verhoogde aandacht op en vermindert de schrik om te melden. In de Belgische cultuur werkt het systeem van de Angelsaksische whistleblower niet, voornamelijk uit vrees voor verklikking.

- <u>Rekening houden met de noden en belangen van de cliënten</u>.

  Dit is de basisregel van MiFID en de basisregel voor elke verzekeringstussenpersoon. Via deze opdracht wordt deze regel evenwel (ook) bij de verzekeringsonderneming gelegd. De Wet Financieel Toezicht gaf deze opdracht aan de FSMA, maar tot vandaag zonder concrete regelgeving. Naar verluidt, werkt de FSMA er momenteel aan om deze algemene norm in de wet te laten invoegen. De gedragsnorm voor de verzekeraar heeft impact op productbeheer, schadebeheer, verkoop, klachtenbeheer, …

- <u>De integere aanpak bij waardenconflict en bijsturing van gedrag.</u>

  In het integriteitsbeleid of het compliance charter moeten we voor de uitzonderlijke situaties die hier bedoeld worden, expliciet een escalatieprocedure voorzien met behandeling op het hoogste niveau van de onderneming.

5.1.3. *Het begrip "Compliancerisico"*

Tekst:

> *"Het Compliancerisico is een risico dat een instelling en/of haar medewerker(s)* ***gerechtelijk, administratief of reglementair worden gesanctioneerd wegens het niet naleven van de wettelijke en reglementaire integriteits- en gedragsregels met een verlies van reputatie en mogelijke financiële schade tot gevolg.*** *Dit verlies van reputatie kan ook het gevolg zijn van het* ***niet naleven van het intern beleid*** *terzake en van de eigen waarden en gedragsregels met betrekking tot de integriteit van de activiteiten van de instelling. Een reputatieverlies leidt tot aantasting van de geloofwaardigheid van de instelling en haar medewerkers.*
> ***Geloofwaardigheid is de basis om actief te kunnen en mogen zijn in de financiële sector."***

De laatste zin overstijgt duidelijk het niveau van een definitie. Als norm hoort dit thuis in de Controlewet.

Het Compliancerisico behoort tot de niet-kwantitatieve risico's. Met bovenstaande definitie wordt het opstellen van indicatoren wel mogelijk. De meting van het Compliancerisico kunnen we zo baseren op de in de regelgeving voorziene sanctionering, de impact op reputatie en/of de financiële impact.

Het komt enigszins vreemd over dat in de verdere tekst geregeld de meervoudsvorm (Compliancerisico's) wordt gebruikt.

5.1.4. *De Compliancefunctie*

Tekst:

> *"De Compliancefunctie is een onafhankelijke functie binnen de financiële instelling, gericht op de naleving van de regels die verband houden met:*
>
> *- de integriteit van de activiteiten van de instelling en*
> *- de beheersing van het Compliancerisico van de instelling."*

"De Compliancefunctie is een tweedelijnsfunctie" (zie Circulaire Compliance, nr. 3.2 en 3.3.4 – principe 7), gericht op de kwalitatieve doelstelling. De andere tweedelijnsfunctie, het Risicobeheer, is voornamelijk gericht op het risicomanagement vanuit de kwantitatieve doelstelling tot het aanhouden van voldoende kapitaal in de onderneming.

Door het begrip "Compliance" van de functie af te splitsen, wordt de situatie van de Compliancefunctie als *second line of defence* veel duidelijker.

In Circulaire D.255 werd de oprichting van een compliancecel die minstens coördinerend en sturend optreedt, als een gezonde praktijk aanbevolen. In het ontwerp van juli 2012 werden nog decentrale concepten beschreven. Deze bepalingen werden uiteindelijk geschrapt.

Om tot een compliancefunctie in maturiteit te komen, moet deze gepercipieerd worden als partner voor de business en niet uitsluitend als controle of 'gendarme' (IFE, 6.12.2012, Table ronde des Compliance Officers). De hierna omschreven opdrachten moeten in samenwerking met de business tot stand gebracht worden. De compliancecultuur dient aan de top en door het management volledig gedragen te worden. De adviesopdracht is hierbij cruciaal, maar ook het communiceren van de resultaten.

5.2. De opdrachten van de compliancefunctie (principe 1)

In Circulaire D.255 was de opdracht omschreven in Principe 7. Het naar voor halen van dit principe kan geïnterpreteerd worden als het benadrukken van de positionering van de Compliancefunctie.

> " ***Principe 1 –*** *De compliancefunctie staat in voor de identificatie en beoordeling van het compliancerisico. Zij zorgt voor het toezicht op, het testen van, het opstellen van aanbevelingen en het rapporteren over het compliancerisico in hoofde van de instelling.*
>
> *Voorts verleent de compliancefunctie advies en neemt zij deel aan de opstelling van richtlijnen omtrent de naleving van de regelgeving. Zij staat de effectieve leiding bij in de organisatie van de opleiding van de medewerkers inzake compliance en zij zorgt, in samenspraak met de operationele diensten, voor de sensibilisatie van de medewerkers inzake het compliancerisico. Zij fungeert als contactpunt voor de medewerkers.*
>
> *De compliancefunctie maakt minstens jaarlijks een actieplan op."*

De beschrijving van de opdracht is een toepassing van de COSO-methodiek:

- identificatie en beoordeling van het Compliancerisico (risk assessment);
- advies betreffende het beleid en het nemen van beheersmaatregelen;
- monitoring;
- opleiding en sensibilisering;
- een risk-based actieplan, met inbegrip van te verwachten ontwikkelingen (wet, systemen, markt).

5.2.1. *Risico-analyse*

De opdracht luidt:

- proactief compliancerisico's identificeren, documenteren en beoordelen;
- beoordelen van procedures, uitvoeren van controles en voorstellen van wijzigingen;
- het compliancerisico meten en maatregelen tot vermindering ervan voorstellen.

Begrippen

Voor een jurist staan in dit Principe een aantal **ongekende begrippen** bijeen vermeld**, zoals 'risk' en 'risk based approach'**, die mogelijks tegenstrijdig zijn of lijken met de basisopdracht die bestaat in het *"toezien op het naleven van alle wettelijke bepalingen"*. In de Circulaire D.255 werd het identificeren en analyseren van **de risico's** in de toelichting van principe 2 (uitwerken van integriteitsbeleid) vermeld, maar niet verder uitgewerkt – zodat we daar geen houvast vinden.

Elke wet moet correct ingevoerd worden. Daarbinnen is geen ruimte voor risicoaanvaarding. De onderneming kan echter wel, in functie van de risicobeoordeling en de risicoaanvaarding door de instelling, prioriteiten stellen op het gebied van invoeren van controles, geven van opleiding, uitbouwen en uitvoeren van monitoring en review van procedures.

Voor Interne Auditors en Risk Officers klinken deze begrippen wel bekend in de oren, maar het specifieke van het Compliancerisico is een moeilijkheid.We doelen hierbij meer bepaald op de werking van de compliancedomeinen doorheen tal van activiteiten en processen, de dimensie die hieraan gegeven wordt – met name hét ticket voor het uitoefenen van het bedrijf - en de moeilijke kwantificering ervan. Complementariteit van de functies Compliance, Risk en Interne Audit is een pluspunt. Overleg om samen tot een gezamenlijke taal, methodologie en risk-matrix te komen is essentieel.

Prioriteitstelling via technieken voor risicoanalyse:

Een eerste methode voor top-down assessment is via toepassing van de maturiteitsscores van de SOx-programma's:

score	invulling
1	oplossing/kennis ad hoc
2	kennis bij 1 of 2 personen & herhaalbaar
3	procedure uitgeschreven & ruim toepasbaar
4	vorming voor betrokkenen / controles geïnstalleerd / activiteit geïmplementeerd
5	Monitoring / review van procedures en processen

Deze maturiteitsscore komt telkens aan de orde bij nieuwe regelgeving (bv. Preventiewet en reglement 2010 betreffende witwassen), bij het herwerken van een verzekeringsproduct of bij het opstarten van een nieuwe activiteit. Pas vanaf niveau 3 komen we in de *Second line of defence*-benadering. In de voorgaande fases overheerst het adviseren.

In een uitgebreider assessment gebruikt men de risk-matrix, derhalve de methodiek en taal van de Risk Officer:

- De horizontale as van de matrix geeft de waarschijnlijkheid aan hetzij per tijdsperiode, hetzij binnen een combinatie van verscheidene parameters.

- De verticale as meet de impact door aan de financiële parameters een aantal niet-financiële parameters met betrekking tot het compliancerisico, toe te voegen: wetgevingsimpact, reputatie, klantenimpact. De subjectiviteit van deze parameters wordt geobjectiveerd, hetzij door definities te hanteren, hetzij door ze, waar mogelijk, te onderbouwen met concrete cijfergegevens (het aantal terecht bevonden klachten, het aantal geweigerde voorstellen in de antiwitwasprocedures, het aantal integriteitsissues, …).

- In de matrix worden de zones met respectievelijk laag, beperkt, matig, groot of zeer groot risico bepaald. De domeinen in de meest risicovolle zones bepalen dan de prioriteit van aanpak.

Voorbeelden van impact op het niveau van de niet-financiële parameters (naar believen te verfijnen):

	Laag	Beperkt	Matig	Groot	Zeer groot
Wetgeving	- overtreding interne procedure - geen straf-sanctie	- eenmalige melding aan toezichthouder - burgerlijk geding - lage geldboete	- onderzoek of herstelmaatregel door toezicht-houder of economische inspectie - strafonderzoek - matige kans op bestraffing	- formele sanctie-procedure door toezichthouder en/of onderzoek door mede-dingingsraad, - strafproces - zware geldboete	- gevangenisstraf - liquidatiestraf - omzetboete - schorsing of verlies licentie
Reputatie	- geen publiciteit - schade op korte termijn - klacht 1 klant	- beperkte media-aandacht - beperkt aantal klachten - schade op korte termijn - klacht door makelaar	- lokale media-aandacht - substantiële schade op medium termijn - aantal klachten van klanten of makelaars overstijgt welbepaald aantal	- lokale media-aandacht - substantiële schade op lange termijn - impact op aandelenkoers	- blijvende nationale media-aandacht - impact op aandelenkoers
Klanten	- minimale impact en beperkte schaal qua segment	- middelmatige impact en beperkte schaal qua segment	- middelmatige impact en middelmatige schaal qua segment	- gevoelige impact t.a.v. groot aantal klanten of volledig distributiekanaal	- gevoelige impact t.a.v. alle klanten of verscheidene distributie-kanalen

<u>Analyse van de compliance domeinen:</u>
Dit assessment moet uitgaan van een gemotiveerde analyse, enerzijds, van de wetgeving betreffende de compliance domeinen (soms 'cartografie' genoemd – zeer belangrijk hierbij is het onderzoek van het risico op en de omvang van een mogelijke sanctionering) en, anderzijds, van de reële activiteiten van het bedrijf.

Enkele voorbeelden:

- een verzekeraar “niet-leven” hoeft de Preventiewet niet te analyseren, heeft meer gevoelige gegevens te beheren onder de Privacywet en ondervindt minder impact op het vlak van leeftijdsdiscriminatie;
- de informatieplichten verschillen per verzekeringsproduct en/of per marktsegment (particulier versus professioneel).

Een moeilijkheid bij het opstellen van de analyse is te bepalen hoever men in detail dient te gaan. Moet elk wetsartikel worden besproken of mag men thema’s groeperen? Nemen wij als voorbeeld de Privacywet 1992, vertaalt deze vraag zich als volgt: bespreking van elk artikel of behandeling per thema zoals daar zijn IT security, direct marketing, medische gegevens en gerechtelijke gegevens. Elk van deze thema’s vormt immers een geheel van risico’s.

Een andere moeilijkheid is de keuze van aanpak: top-down of omgekeerd? Om snel tot maturiteitsniveau 3 te komen is de aanpak top-down te verkiezen. Om daarna niveaus 4 en 5 te bereiken, is een algemeen engagement binnen het bedrijf vereist met een approach down-top (uitzonderingen, vragen, voorstellen tot verdere verfijning, enz., komende vanuit de basis).

Nemen wij volgend geval als voorbeeld. In 2008 ging Lehman Brothers failliet en verscheidene Belgische verzekeraars hadden in hun portefeuille producten met fondsen of garantie van deze instelling. Los van het debat over de eventuele aansprakelijkheid van de instelling, kon men het risico als volgt schatten:

- qua wetgeving: matig (onderzoek economische inspectie, strafonderzoek)
- qua reputatie: zeer groot (verscheidene jaren nationale media-aandacht)
- qua klanten: matig tot groot (i.f.v. de omvang van de effectieve portefeuille).

Gemiddeld over de drie analyses betekende dit dus een groot risico (beperkte omvang portefeuille) of zelfs de zwaarste score ‘zeer groot’ (belangrijke portefeuille). Meestal neemt men de zwaarste score bij één parameter. Resultaat: rapportering aan het directie- en auditcomité was onvermijdelijk en actie door alle *lines of defence* bleek noodzakelijk.

In de Gedragscode Witwassen vinden we een ander voorbeeld van sectorbrede risicoinschatting van levensverzekeringsproducten in de opdeling van verzekeringsproducten naargelang zij een laag, matig of gevoelig witwasrisico lopen.

5.2.2. *Advisering en procedurenota’s*

De opdracht luidt om met het oog op het beheersen van het compliancerisico, binnen de opdracht van de compliancefunctie (Circulaire Compliance, nr.3.2.2):

- te adviseren over alle huidige en komende wetgeving;
- deel te nemen aan het uitwerken en bijwerken van het integriteitsbeleid via het uitwerken en bijsturen van procedures;
- maatregelen te nemen; (zie voor voorbeelden, hierna onder nr.5.2.4)
- deel te nemen aan de beraadslaging over nieuwe producten, diensten of markten;

- deel te nemen aan beraadslagingen over wijzigingen in de bedrijfsorganisatie.

We lezen hier een **doelgerichte bevoegdheid**.

De compliancefunctie stelt zich niet in de plaats van de effectieve leiding noch het operationele management, maar oefent deze opdracht in overleg met hen uit.

De adviesopdracht:

We herhalen dat het **principe 8** een bijzondere waarde aan het advies toekent. Volgens het principe "*comply or explain"* dient het besluit tot het niet opvolgen van een beslissing of aanbeveling toegelicht te worden en kan de compliancefunctie dit besluit in voorkomend geval via een escalatieprocedure bij een hoger hiërarchisch niveau in vraag stellen.

De adviesopdracht komt het meest frequent voor in de hierboven genoemde maturiteitsfases 1 tot 3 bij elke nieuwe regelgeving, voor elk nieuw activiteitendomein of product, …

Wat is een "adequate " procedure?

Om efficiënt te zijn:

- is zij gericht aan een duidelijk omschreven publiek;
- bevat zij duidelijke informatie;
- definieert zij klare verantwoordelijkheden in de *first line;*
- laat zij toe advies te verlenen en/of maatregelen te nemen in welbepaalde gevallen in de *second line;*
- bevat zij een escalatieprocedure bij meningsverschillen;
- vermijdt zij "shopping" tussen de diverse experten van de onderneming;
- legt zij daarenboven de rapportering vast.

Productontwikkeling en –review:

De toezichthouders benadrukken de tussenkomst van de compliancefunctie in een vroeg stadium van productontwikkeling of -wijzigingen (Presentatie van J. Swyngedouw en H.Lannoy, Forum Compliance, 14 juni 2012).

In 2011 verplichtte de Nederlandse toezichthouder alle verzekeraars om een review op te zetten van alle verzekeringsproducten met als doel "klantenbelang centraal". Hierbij was een zware opdracht voor de Compliance Officers weggelegd.

Tijdens het IFE-seminarie van 6.12.2012 formuleerden De Pover, De Meulenaere en Berden (Table ronde des Compliance Officers: débat avec l'assemblée) de rol van de compliancefunctie als *gate keeper* op het vlak van productontwikkeling met volgende opdrachten:

- controle op het bestaan van een ontwikkelingsprocedure;
- controle op het naleven ervan;
- risicoanalyse bij het opstarten van een ontwikkelingsproces;
- bewaken van het klantenbelang versus het bedrijfsbelang;
- controle op de documentatie en archivering.

Opvolgen van de wetgeving:

Opdat de compliancefunctie haar adviesopdracht binnen de compliancedomeinen naar behoren zou kunnen uitvoeren, benadrukt de Circulaire Compliance (nr. 3.2.6.) het belang van een degelijke *legal watch.* De verantwoordelijkheid met de toegewezen domeinen ligt bij de compliancefunctie , in samenwerking met de juridische functie.

5.2.3. *Opleiding, contactpunt en sensibilisering*

Het opstellen van procedurenota's volstaat niet. Opleidingssessies, gediversifieerd volgens doelgroep, vormen de logische volgende fase (nr.3.2.4). Ook deze opdracht dient in overleg met het operationele management ingevuld te worden.

Hoe *awareness* tot stand te brengen en op welke wijze die te meten, is een blijvende bezorgdheid van elke Compliance Officer. Het is daarbij een hele opgave om jaar na jaar voor elke doelgroep de juiste momenten te vinden om awareness te creëren en in stand te houden, gezien de vele opeenvolgende commerciële en administratieve piekperiodes.

Diverse belangrijke vragen stellen zich:

- Welke zijn de beste opleidingsvormen om een blijvend effect sorteren?
- Tegen welke kostprijs?
- Met welke frequentie?

Abstracte begrippen zoals 'integriteit', 'compliance', 'klantenbelang', enz. duiden zich niet zo gemakkelijk. Om de vorming hierover toegankelijker en doeltreffender te maken, verdient het aanbeveling:

- te werken rond concrete normen of gevallen;
- transparant te communiceren over incidenten en de aanpak ervan;
- reële voorbeelden te geven van giften en events;
- meldingsplicht in te voeren voor nevenfuncties, deelnames aan events, eindejaarsgiften, enz.

De antiwitwasreglementering legt zowel voor de interne medewerkers als voor het intermediair een bijzondere opleidingsplicht op. Algemene vorming hierover is al vrij standaard en ruim beschikbaar. Interne opleidingen dienen zich bijgevolg te richten op het eigen acceptatie- en waakzaamheidsbeleid. Geregelde coaching van de vaste contactpersonen in de *first line* is aangewezen om trends te duiden en praktische problemen aan te pakken. Tegelijkertijd maakt dit een vorm van monitoring van de procedures uit.

5.2.4. *Toezicht en testen (monitoring)*

De Circulaire Compliance geeft voor het eerst richtlijnen over de gewenste monitoring (nr.3.2.3).

"*De Compliancefunctie ziet er op toe dat de instelling de (…) integriteits- en gedragsregels naleeft.*"

Dit betreft een directe opdracht die onder de onafhankelijkheid van de functie hoort. De compliancefunctie beoordeelt de naleving van het beleid op integriteits- en reglementair vlak en de kwaliteit en efficiëntie van de controles. Waar nodig, stelt de compliancefunctie verbeteringen voor.

In eerste orde worden de **controleresultaten van de operationele diensten (*first line) gebruikt.*** In de hierboven genoemde procedures is het aangewezen de concrete controles op te sommen. In de SOx- en SolvencyII-programma's worden vele controles getest door personen die extern zijn aan de betrokken dienst.

De **Circulaire Interne controle** omschrijft in punt 1.2 algemene maatregelen van interne controle:

"*organisatiemaatregelen (zoals omschrijvingen van functies en verantwoordelijkheden, hiërarchische controle, functiescheiding), controlemaatregelen (zoals kruiselingse controles, dubbele handtekening, periodieke voorraadcontroles), boekhoudkundige maatregelen (zoals aansluiting van rekeningen, verantwoording van saldi, bijhouden van controleregisters) en maatregelen ter beveiliging van personen en activa.*"

In punt 1.3 komen dan specifieke maatregelen aan bod:

"*(…) niet of moeilijk meetbare risico's zoals het risico op vergissingen en fraude, het risico op juridisch onvolmaakte overeenkomsten en documenten en het reputatierisico. (…) Voor niet of moeilijk meetbare risico's neemt de onderneming de passende maatregelen zoals nauwkeurige analyse van de risico's en het opnemen van internationaal aanvaarde standaardbedingen in de overeenkomsten. (…) het is noodzakelijk dat de continuïteit en de betrouwbaarheid van de elektronische informatiesystemen verzekerd zijn.*"

De **Circulaire Uitbesteding** bepaalt in verscheidene principes toezichtmaatregelen om de continuïteit te verzekeren (principe 4), de verbintenissen scherp te stellen (principe 5), een aangepaste beveiliging te bekomen (principe 6), de interne audit en compliance toegang te geven (principe 7) en het revisoraal en prudentieel toezicht mogelijk te maken (principe 8). Belangrijke outsourcingscontracten vallen dus binnen de scope van de monitoring door de toezichtsorganen in tweede, derde en volgende lijn.

Aanvullend worden in de **Circulaire Compliance** technieken geadviseerd die tot het traditionele gamma van de auditberoepen behoren:

"- *het nemen en beoordelen van steekproeven van de uitgevoerde verrichtingen;*
- *het bijhouden en opvolgen van risico-indicatoren zoals aantal klachten en inbreuken;*
- *de observatie van de uitvoering van verrichtingen met en voor rekening van cliënten; (*nvdr: MiFID-regels)
- *het voeren van gesprekken met medewerkers; en*
- *het opvolgen van exceptieverslagen."* (nvdr: wordt hier bedoeld: analyse van incidenten)

Om de monitoring efficiënt te laten verlopen, verdient het zeker aanbeveling dat de andere controlefuncties hun rapporten (interne audit), testresultaten (risk) of analyses (actuariële functie) aan de compliancefunctie bezorgen.

5.2.5. *Actieplan*

Aanbeveling

De aanbeveling over het actieplan (nr.3.2.5) is tekstueel overgenomen van de **Circulaire Interne controle en Interne Audit.**

Tegelijk alle compliance domeinen tot maturiteitsniveau 5 brengen, jaarlijks alle nieuwe regelgeving verwerken (jaarlijks gemiddeld vijf belangrijke aanpassingen op belangrijke delen van de verzekeringsportefeuille of op de organisatie) en eventuele disfuncties rechtzetten, is voor elke instelling een onmogelijke opdracht. Om die reden steunt het plan op de risicoanalyse die we hoger probeerden op te maken.

De vraag naar een realistisch actieplan is zowel terecht als overbodig. Immers, door het opstellen van een risk-based prioriteitenlijstje worden onverwachte opdrachten meteen gewogen en in het plan ingevoegd.

De toezichthouders kunnen ook meewerken aan het terugdringen van "onverwachte opdrachten" door voor nieuwe regelgeving (haalbare) timings mee te geven en door hun eigen jaarlijkse themagebonden inspecties tijdig aan te kondigen. In het licht van openbaarheid van bestuur lijkt dit een gewenste evolutie, waarbij toezichthouders van andere landen zoals het UK en Nederland tot voorbeeld kunnen strekken.

Middelen

Tekst:

> *"Het actieplan omvat een staat van de **vereiste menselijke en materiële middelen**. Bij de menselijke middelen wordt niet enkel aandacht besteed aan het aantal personen maar ook aan de **vereiste bekwaamheid** om de geplande activiteiten te kunnen uitvoeren."*
>
> "*Het actieplan wordt (…) goedgekeurd door de effectieve leiding.* ***Deze goedkeuring houdt in dat zij de vereiste middelen ter beschikking stelt van de compliancefunctie."***

Het actieplan wordt bevestigd door het Auditcomité. Het ESMA-report stipuleert in nr. 47 dat:

- het budget consistent moet zijn met het compliancerisico dat de onderneming loopt;
- de Compliance Officer betrokken moet worden;
- elke beslissing over een significante budgetvermindering schriftelijk gedocumenteerd en gemotiveerd moet worden.

Een *risk-based* actieplan kan nooit de volledige scope van de complianceopdracht omvatten. Deze regel van de toezichthouder kwalificeert de opdracht van de compliancefunctie tot een

inspanningsverbintenis. De verplichting in hoofde van de effectieve leiding tot goedkeuring van het jaarplan en de beschikbare middelen heeft eveneens tot gevolg dat een probleem van non-compliance in een bepaald domein niet aan de compliancefunctie aangerekend kan worden, maar tot de verantwoordelijkheid van de effectieve leiding, c.q. de rechtspersoon, behoort.

6. Governance van de compliancefunctie

6.1. Verantwoordelijkheid van de raad van bestuur

6.1.1. *Principe 2 – de raad van bestuur is bevoegd voor het integriteitsbeleid.*

Tekst:

> "***Principe 2 -*** *De* (volledige) *raad van bestuur neemt het initiatief voor het bevorderen van het integer doen van zaken door de instelling. De raad van bestuur ziet er op toe dat de instelling beschikt over een passend integriteitsbeleid en ondernemingswaarden".*

Dit principe stemt overeen met Beginsel VII uit de **Circulaire Deugdelijk bestuur.** Het beveelt de regel *tone at the top* aan. Weliswaar is er een verschil leesbaar tussen de omschrijving " hoogstaande en strikte gedragsregels" in de **Circulaire Deugdelijk bestuur** en de omschrijving "hoge ethische normen, en naleven van zowel de geest als de letter van de regelgeving" in de definitie van Circulaire Compliance.

Het document met beschrijving van het integriteitsbeleid maakt deel uit van de **Memo Governance** (punt 7 van het model – Circulaire Deugdelijk bestuur) en bevat minstens volgende onderdelen:

- de strategische doelstellingen en ondernemingswaarden;
- de (opsomming van) interne codes, reglementen en voorkomingsbeleid met betrekking tot corruptie, geschenken en events, oneigenlijke zelfverrijking, onethisch of illegaal gedrag;
- een beleid rond belangenconflicten: analyse van mogelijke conflictgebieden, vastlegging van organisatorische en administratieve maatregelen, middelen om conflicten te beheren;
- een klokkenluiderregeling om klachten (in)direct bij een onafhankelijke functie of het auditcomité te rapporteren en te laten onderzoeken met bescherming van de bona fide klokkenluider en in overeenstemming met de adviezen van de Privacycommissie;
- de behandeling van cliëntenklachten.

Nieuwe aanbevelingen in de Circulaire Compliance:

- Voortaan moet ook de methodologie voor het opsporen en beheren van het Compliancerisico in het integriteitsbeleid toegevoegd worden.
- Jaarlijks dient de raad van bestuur het integriteitsbeleid te toetsen aan de activiteiten van de instelling. Dit dient inhoudelijk uitvoerig genotuleerd te worden. De notulen gelden voor de toezichthouder namelijk als bewijs van de toetsing.
- Gedragscodes dienen uitgewerkt te worden voor de medewerkers of voor bepaalde betrokken groepen van medewerkers. Deze aanbeveling is zinvol want, terwijl het beleid jaarlijks op ondernemingsniveau geëvalueerd en eventueel bijgestuurd wordt, dienen gedragscodes daarentegen een langere levensduur te hebben. Immers, elke gedragscode of procedurenota die verplichtingen voor een bediende inhoudt - en dus arbeidsrechtelijk sanctioneerbaar is -, moet volgens de Taalwetgeving minstens in het Frans en Nederlands

geschreven worden. Bovendien dient zij via het sociaal overleg binnen de onderneming op de gepaste wijze in de arbeidsrechtelijke verhoudingen geïntegreerd te worden. De Compliance Officer overlegt hierover dus best met de HR-directeur om per gedragscode enkel de bepalingen die vanuit sociaalrechtelijk oogpunt strikt noodzakelijk zijn, op te nemen.

6.1.2. *Principe 3 – het Auditcomité ziet toe op het permanent bestaan van een passende onafhankelijke compliancefunctie.*

Tekst:

> "***Principe 3*** *- De raad van bestuur ziet er op toe dat de effectieve leiding de nodige maatregelen neemt opdat de instelling blijvend beschikt over een passende onafhankelijke compliancefunctie om de naleving door de instelling, haar bestuurders, effectieve leiding, werknemers en gevolmachtigden te verzekeren van de rechtsregels in verband met de integriteit van het bedrijf.*
>
> *De raad van bestuur beoordeelt minstens jaarlijks of het Compliancerisico afdoende wordt herkend en beheerst*."

Het Auditcomité is het aangewezen comité binnen de raad van bestuur om deze toezichtfunctie op zich te nemen. De taak van het comité bestaat erin zich uitvoerig over de risico's te laten informeren. De omstandigheid dat het met niet-uitvoerende en onafhankelijke bestuurders wordt samengesteld, garandeert zijn objectiviteit. De andere interne onafhankelijke en externe controlefuncties rapporteren ook aan dit comité.

Het Auditcomité neemt kennis van en bevestigt:

- het Compliance Charter;
- het jaarlijks actieplan;
- de periodieke rapportering met overzicht van de belangrijkste vaststellingen en aanbevelingen;
- de belangrijke wijzigingen in het wettelijke kader met impact op het integriteitsbeleid en/of de organisatie van de compliancefunctie.

Opnieuw benadrukt de Circulaire Compliance een uitgebreide notulering van de ontvangen informatie, de beraadslaging en de besluiten omtrent de uit te voeren maatregelen.

De Belgische Code Deugdelijk bestuur spoort daarenboven de leden van het Auditcomité aan om zelf actief informatie in te winnen. Na de leden van het Directiecomité zijn de onafhankelijke controlefuncties daartoe de eerstaangewezen medewerkers van het bedrijf.

6.2. Verantwoordelijkheid van de effectieve leiding (principes 4 – 6)

De effectieve leiding/het directiecomité is zowel voor de eerstelijnscontroles als voor de beheersing van het Compliancerisico verantwoordelijk. De principes 4 tot 6 geven de details weer:

> *"**Principe 4 – De effectieve leiding is verantwoordelijk** voor de beheersing van het Compliancerisico. Hiertoe formuleert zij een integriteitsbeleid dat geregeld wordt geactualiseerd. Zij zorgt ervoor dat alle leden van de instelling er kennis van krijgen en het naleven.*
>
> ***Principe 5** – **De effectieve leiding dient de nodige maatregelen te nemen** opdat de instelling blijvend kan beschikken over een passende onafhankelijke compliancefunctie om de naleving door de instelling, haar bestuurders, effectieve leiding, werknemers en gevolmachtigden te verzekeren van de rechtsregels in verband met de integriteit van het bedrijf.*
> *Minstens jaarlijks brengt de effectieve leiding verslag uit bij de raad van bestuur.*
>
> ***Principe 6** – De **Compliancefunctie rapporteert** volgens een aangepaste frequentie en minstens jaarlijks **aan de effectieve leiding en informeert de raad van bestuur**"* (in casu het auditcomité).

<u>Aansprakelijkheid</u>

Principe 4 levert een gedeeltelijk antwoord op de aansprakelijkheidsvraag met betrekking tot de compliancefunctie (verantwoordelijkheid berust bij de effectieve leiding) en dient samen met principe 9 gelezen te worden (blijvende en permanente medewerker en dus verbonden door een arbeidsovereenkomst). De bezorgdheid die door het Forum Compliance werd geuit, is hiermee niet helemaal afgedekt. De Circulaire is voor de rechters geen "hard law". De interpretatie van de toezichthouder is voor hen niet bindend, zeker niet in strafrechtelijke procedures. We stellen dan ook vast dat de aansprakelijkheid van de Compliance Officer zowel binnen de onderneming als daarbuiten toeneemt en kunnen niet naast de vervolging (en soms veroordeling) kijken die een aantal collega's in binnen- en buitenland naar aanleiding van vaak sterk gemediatiseerde gerechtelijke procedures hebben opgelopen.

<u>Praktische aanbevelingen</u>

Om deze principes in de **praktijk** te laten werken formuleert de Circulaire nog **bijkomende aanbevelingen**:

- complianceverantwoordelijkheden binnen de organisatie aflijnen;
- de compliancefunctie tijdig over nieuwe ontwikkelingen, projecten en producten informeren;
- de compliancefunctie toegang geven tot dagorde, nota's en notulen van het directiecomité;
- de compliancefunctie structureel doen rapporteren over belangrijke problemen, tekortkomingen en/of inbreuken en ernstige incidenten met een overzicht van de belangrijke aanbevelingen en de opvolgingsstatus door de *first line;*
  hiermee vult de Circulaire Compliance verder in welke rapportering over Compliance in het ICS-rapport opgenomen moet worden;

- bij ernstige tekortkomingen van het integriteitsbeleid en bij het niet (tijdig) naleven van aanbevelingen van de compliancefunctie over corrigerende maatregelen beslissen;

- het interne controlesysteem in het jaarlijks rapport bespreken (**Circulaire ICS** van CBFA-2009-26);

- de compliancefunctie minstens jaarlijks in het directiecomité uitnodigen;

- de compliancefunctie onder de rechtstreekse hiërarchie van een lid van de effectieve leiding plaatsen. Uit diverse Circulaires blijkt dat het aanduiden van de compliancefunctie als functie op niveau N-1 een expliciet doel van de toezichthouders is.

Onverenigbaarheden

De Circulaire Compliance bepaalt voor het eerst de onverenigbaarheden in hoofde van de leidinggevende binnen de compliancefunctie:

- Elk mogelijk belangenconflict tussen de bevoegdheid over compliance en eventuele andere bevoegdheden dient vermeden te worden. Dit sluit meteen uit dat de leden van het directiecomité met bevoegdheden over commerciële en operationele afdelingen tevens de compliancefunctie zouden aansturen.

- Indien de compliancefunctie en de risicobeheerfunctie (beiden onafhankelijke controlefuncties) onder hetzelfde directielid vallen, dient betrokkene erover te waken ***"dat aan beide functies een gelijkwaardige aandacht wordt besteed".*** Deze bepaling zet beide functies op eenzelfde niveau en trekt consequent de tweedelijnsfunctie door. Het debat over de ondergeschiktheid van het Compliancerisico aan het Operationeel Risico – met weerspiegeling hiervan in de organisatie – werd aldus (minstens tijdelijk) door de Belgische toezichthouders beslecht.

- De compliancefunctie en de interne auditfunctie kunnen niet meer aan hetzelfde directielid rapporteren (tenzij bij kleine instellingen). De **Circulaire Interne Audit** bepaalt dat de interne auditfunctie aan de Voorzitter van het Directiecomité rapporteert. Een mogelijke ontwikkeling is dat de interne auditfunctie in de toekomst rechtstreeks aan de Voorzitter van het Auditcomité zal rapporteren, omdat zowel het Auditcomité als de interne auditfunctie tot de *third line of defence* behoren.

6.3. Relatie met transversale controlefuncties (principe 7)

Tekst:

> "***Principe 7 –*** *De Compliancefunctie maakt deel uit van een coherent geheel van transversale controlefuncties waartussen coördinatie noodzakelijk is."*

In dit principe werken de toezichthouders de concepten met betrekking tot *three lines of defence* en de onafhankelijke controlefuncties uit, die de Controlewet in het artikel 14bis bepaalde.

De eerste verdedigingslijn tegen alle risico's waaraan de instelling blootgesteld wordt, berust bij de verantwoordelijken van de operationele diensten. Dit dient ruim geïnterpreteerd te worden en omvat bijgevolg hieronder zowel commerciële, financiële, operationele als ondersteunende functies. Zij zijn verantwoordelijk voor alle interne controlemaatregelen. De Circulaire Compliance herhaalt bij wijze van good practice om alle procedures en controles te documenteren (maturiteitsniveau 3). Hierdoor kunnen vorming en monitoring makkelijker verlopen en wordt continuïteit gewaarborgd.

De tweede verdedigingslijn in een verzekeringsonderneming wordt gevormd door de compliancefunctie, de risicobeheersfunctie en de actuariële functie. De risicobeheersfunctie is belast met het risicobeheersysteem (zie **Circulaire Risicobeheer)**, met uitzondering van het compliancerisico. De actuariële functie (zie **Circulaire Actuariële functie)** heeft als opdracht bij elk nieuw product of tarief een oordeel te geven over de verwachte rentabiliteit en jaarlijks haar advies te geven over de rentabiliteit van de producten, technische voorzieningen, herverzekering en winstdeling. In haar adviezen beoordeelt de actuariële functie ook de naleving van wetgeving en is het dus zinvol deze adviezen met de compliancefunctie te delen.

De interne auditfunctie beoordeelt vanuit de derde lijn de aangepastheid van zowel de interne controlemaatregelen als de werking van de tweedelijnsfuncties. Periodiek voert De Interne Audit op het geheel van procedures controles volgens internationale normen uit. Zijn rapporten worden steeds aan het Auditcomité bezorgd.

De Circulaire Compliance vraagt de werkzaamheden (jaarplannen en opdrachten ad hoc) van de controlefuncties in tweede en derde lijn op elkaar af te stemmen, en te zorgen voor een passende uitwisseling van relevante informatie in direct contact.

De vraag wie het initiatief tot coördinatie neemt en hoe die eruit moet zien, wordt opengelaten. Elke onderneming en elke functie kan dus eigen initiatieven nemen. De effectieve leiding en het Auditcomité dienen hierbij hun rol te spelen.

Het Forum Compliance vroeg ook de relatie tussen de Compliancefunctie en de juridische functie te duiden. De toezichthouder is hierop zeer beperkt ingegaan. De situatie op het terrein is heel erg verschillend tussen banken en verzekeraars en tussen de kleine, middelgrote en grote instellingen. Bij kleinere instellingen worden beide functies nog vaak door één persoon of dienst uitgeoefend. De juridische functie wordt in de grotere instellingen belast met de opvolging en interpretatie van de wetgeving, de bewaking van het juridische risico en het corporate legal advies (IFE, 6.12.2012, Table ronde des Compliance Officers). Het ESMA- Final Report geeft in nrs. 64 tot 66 duidelijker guidelines voor de investeringsondernemingen. Het stipuleert dat de beide functies in kleine ondernemingen

kunnen samenblijven mits invoeren van een sterk uitgewerkte, rigide belangenconflictregeling en rapportering hierover aan de toezichthouder. Zodra de compliancefunctie evenwel meer dan 1 voltijdse job uitmaakt, moet die volgens het rapport een aparte organisatie krijgen.

Onverenigbaarheid van tweedelijns- en derdelijnsfuncties:

Het principe 7 stelt tevens duidelijk dat het uitvoeren van complianceopdrachten voor de medewerkers van Risicobeheer en Interne audit als **onverenigbaarheid** wordt beschouwd. Voor de juridische functie wordt dit niet zo expliciet gesteld, maar wordt onverenigbaarheid sterk aanbevolen. De **Circulaire Actuariële functie** bepaalt op haar beurt een onverenigbaarheid met de compliancefunctie.

6.4. Onafhankelijkheid van de compliancefunctie (principe 8)

Tekst:

> ***"Principe 8 –*** *De compliancefunctie dient onafhankelijk te zijn van de operationele activiteiten van de instelling."*

De bespreking van de onafhankelijkheid van de functie maakt het onderwerp van een afzonderlijke bijdrage uit. Niettemin, teneinde hier toch een volledig beeld te schetsen van alle nieuwigheden in de circulaire voor wat Governance betreft, worden hier enkele kernpunten aangestipt:

- het doelgerichte initiatiefrecht van de compliancefunctie, in alle omstandigheden;
- de kracht van de adviezen : *comply or explain*;
- de waarborg van vrije expressie van vaststellingen en beoordelingen;
- de mogelijkheid om op eigen initiatief rechtstreeks contact te nemen met de Voorzitter van de Raad van bestuur, en/of van het Auditcomité, de erkende commissaris en de toezichthouders.

Elk van deze punten noodzaakt een grondige analyse van de casus, het nauwkeurig formuleren van elk advies en het zorgvuldig beoordelen van de toegevoegde waarde van de contactname.

7. Organisatie van de compliancefunctie (principes 9 – 11)

Tekst:

> "***Principe 9 –*** *Elke instelling draagt er zorg voor dat de compliancefunctie passend en op permanente wijze wordt georganiseerd.*
>
> ***Principe 10 –*** *De compliancefunctie dient te kunnen beschikken over de nodige middelen, zowel menselijke als materiële, voor de uitoefening van haar opdrachten.*

Principe 11 – *Elke instelling zorgt er voor dat het hoofd en de medewerkers van de compliancefunctie hun opdrachten integer en discreet uitvoeren."*

In uitvoering van de Europese richtlijnen en van artikel 14bis van de Controlewet laten de toezichthouders er geen enkele twijfel over bestaan: de compliancefunctie moet een continue en permanente functie binnen de onderneming zijn.

Er is slechts 1 hoofd van de compliancefunctie per entiteit, die vanwege de FSMA de erkenning als **Compliance Officer** moet hebben verworven en een beoordeling *"fit en proper"* van de NBB moet krijgen. De medewerkers van de compliancefunctie moeten door een arbeidsovereenkomst met de instelling verbonden zijn.

Waar er sprake is van een continue functie, betekent dit dat er altijd een ervaren medewerker beschikbaar moet zijn. Dit vereist dus dat er operationeel gezorgd wordt voor een back-up of dat de compliancecel uit minstens 2 personen bestaat. Het betekent eveneens dat de eventuele andere taken die aan deze personen toegewezen worden, ondergeschikt moeten blijven aan de uitoefening van de compliancefunctie, die als hoofdtaak geldt. Andere taken blijven dus mogelijk, maar de instelling moet stevige "C*hinese walls"* creëren om belangenconflicten te vermijden. We verwijzen ook naar de hoger vermelde onverenigbaarheden met de andere onafhankelijke controlefuncties (zie principe 7).

De toezichthouders opteren er in deze Circulaire voor om het hoofd van de compliancecel (bij FSMA is dit dus de erkende Compliance Officer) in het organogram op het niveau N-1 te situeren (ook genoemd: directiekader, managementniveau, …). In de wetgeving en tal van circulaires is er sprake van een "sleutelpersoon". In D255 was het principieel nog mogelijk dat een lid van de effectieve leiding van de onderneming als Compliance Officer werd aangesteld. Deze selecteerde dan binnen zijn departement de betrokken medewerkers aan wie hij of zij een "compliancerol" toebedeelde. Behalve bij kleine instellingen vervalt deze mogelijkheid. Het hoge niveau van de compliancefunctie binnen de organisatie is tevens noodzakelijk om voldoende gezag, onafhankelijkheid, awareness en contacten op managersniveau mogelijk of makkelijker te maken.

De bestaffing van de Compliance cel bestaat, ons inziens, best uit personen met uiteenlopende diploma's (niet alleen juristen) en met voldoende ervaring binnen de sector., én maturiteit. Voor hen moet voorzien worden in een permanente vorming, in de eerste plaats om de noodzakelijke hoge graad van deskundigheid in stand te houden, maar tevens om de vereiste erkenning bij de FSMA te bekomen en te behouden. Gelijkaardige vormingsvereisten werden gedefinieerd in de Circulaires van de andere onafhankelijke controlefuncties.

Het bepalen van de nodige materiële middelen (budget) om de functie naar behoren te kunnen uitoefenen, maakt deel uit van het jaaractieplan en bevordert de onafhankelijkheid van de functie.

De medewerkers van de compliance cel bewaken het integriteitsbeleid van de instelling. Hun integriteit moet derhalve aan de hoogste normen voldoen. De Circulaire Compliance beveelt uitdrukkelijk aan dit te checken bij aanwerving of aanstelling (bv. opvragen van diploma, controle op blanco strafregister) en een antecedentenonderzoek uit te voeren (bv. referenties, eerdere werkervaring, lidmaatschap van beroepsorganisaties, check van publicaties, check via sociale media).

In de ontwerpcirculaire van de NBB van 21.12.2012 inzake haar “fit & proper” beleid, worden nog meer criteria aangegeven.

Discretie en beroepsgeheim

Discretie is een basisvoorwaarde om de functie uit te voeren. De medewerkers zijn op de hoogte van de strategische bedrijfsprojecten, behandelen contacten met de toezichthouders, behandelen incidenten met mogelijke impact op reputatie en/of behandelen fraudecases waarbij personeel betrokken kan zijn. Dit vereist daarenboven een hoge graad van objectieve ingesteldheid, ook al blijft de medewerker verbonden met de instelling. Zijn objectief en onafhankelijk onderzoek of advies blijft hoe dan ook een beslissing van de onderneming, die via een gerechtelijke procedure aan een rechterlijke toetsing kan worden onderworpen.

Bij gebrek aan een wettelijke regeling valt deze discretieplicht niet onder het begrip "beroepsgeheim". De meeste Compliance Officers met een juridische vorming zijn of kunnen evenwel lid worden van het Instituut voor Bedrijfsjuristen en zijn in die erkenning wel onderworpen aan een beroepsgeheim. De taken van de compliancefunctie vallen onder de criteria van erkenning als bedrijfsjurist, met name ‘*hoofdzakelijk advies van juridische aard verlenen aan de hoogste organen van het bedrijf*’. Domeinen als privacy, mededinging, marktpraktijken, ethische codes en good governance zijn immers basisdomeinen voor bedrijfsjuristen

De wijze van organisatie staat niet langer vermeld in de Circulaire (centraal of decentraal, mengvormen, contactpunten …). De opdeling van de verantwoordelijkheden tussen de *first* en *second line of defence* laat een heldere benaming en structuur toe. De meeste instellingen hebben – in navolging van de eerder door de CBFA aanbevolen ‘best practices’ – reeds sinds enige tijd een intern netwerk van "*compliance correspondenten*" ingesteld. Deze contactpersonen binnen de *first line* behouden vandaag nog meer dan vroeger hun nut als aanspreekpunt voor collega's binnen het eigen departement en als contactpersoon van het departement met de centrale Compliancefunctie. De verdere uitbouw van een centrale cel blijkt evenwel noodzakelijk. De toezichthouder vraagt om in alle functiebeschrijvingen het beheer van het compliancerisico expliciet als taak op te nemen.

De compliancefunctie heeft toegang tot alle departementen en activiteiten..

8. Proportionaliteitsprincipes

8.1. De compliancefunctie in een groepscontext (principe 12)

Tekst:

> ***"Principe 12*** *- Het integriteitsbeleid en de compliancefunctie in een groep worden centraal aangestuurd door de moederinstelling. Deze dienen in overeenstemming te zijn met de plaatselijke wetten en reglementen.”*

Het integriteitsbeleid en globale richtlijnen worden centraal aangestuurd, maar aangepast aan lokale regelgeving. Dit basisprincipe komt tegemoet aan de oorspronkelijke doelstelling om als

(beursgenoteerde) financiële instelling een coherent imago op te bouwen en te behouden. Specifiek voor de controlefuncties verhoogt dergelijke aansturing de onafhankelijkheid.

De controlefuncties kunnen functioneel vanuit de groep aangestuurd worden, maar moeten daadwerkelijk op het niveau van elke dochteronderneming uitgebouwd worden, telkens met een verantwoordelijke die ook door de effectieve leiding van de dochteronderneming mee aangestuurd kan worden en waaraan die leiding opdrachten kan geven. De Circulaire tekent hiervoor een matrixstructuur uit (zie ook de **Circulaire Deugdelijk bestuur**, nrs 85 tot 94.). Per dochterentiteit moeten een (erkende) Compliance Officer en een antiwitwasverantwoordelijke aangesteld worden. En daarbij geldt:

> "*De compliancefunctie van de moederonderneming staat in voor de samenwerking, de coördinatie, het verlenen van steun en advies, en het stroomlijnen van de verschillende dochters."(Circulaire Compliance, blz.25)*

In een groepscontext komen nieuwe accenten aan de orde die de compliancefunctie onafhankelijk dient te monitoren, meer bepaald:

- het binnen de groep uitbesteden van operationele en/of ondersteunende diensten;
- belangenconflicten binnen de groep die voortvloeien uit groepsstrategieën;
- cumuls van functies bij één persoon die de governance doorkruisen.

8.2. Beroep op een deskundige (principe 13)

Tekst:

> "***Principe 13 -*** *De verantwoordelijkheid van de instelling om wetten en reglementen na te leven kan niet worden uitbesteed. Voor nauwkeurige gespecificeerde opdrachten inzake compliance kan in voorkomend geval tijdelijk een beroep gedaan worden op een deskundige."*

Het hoofd van de compliancefunctie kan voor een tijdelijke en nauwkeurig gespecificeerde opdracht op een deskundige een beroep doen. Dit principe sluit ook aan bij **principe 9.** Men denkt hierbij bv. aan de implementatie van MiFID of Fatca-rules. Het tijdelijke karakter van deze mogelijkheid wordt nogmaals benadrukt door de uitdrukkelijke vraag om tot assimilatie van knowhow binnen het vaste team te komen. Binnen een groepscontext ligt hier duidelijk een coördinatieopdracht voor de centrale functie, meer bepaald het detacheren van een specialist naar de dochter- of moederonderneming om een welbepaald domein in te richten.

De criteria voor een goede keuze zijn als *good practice* opgelijst. Onder punt 7 werden deze reeds als criteria voor de aanwerving van de medewerkers vermeld.

Ten aanzien van een dergelijke deskundige dient het belang van de onafhankelijkheid en het vermijden van belangenconflicten te worden onderstreept. In die zin is het onaanvaardbaar dat diezelfde deskundige kort voordien als 'jurist' of consultant een welbepaalde activiteit heeft ingericht, om deze daarna in de hoedanigheid van compliancefunctie te gaan monitoren. Eenzelfde

principe vinden we terug in de **Circulaire Interne Controle en Interne Audit**, en in de wettelijke criteria voor aanstelling van de onafhankelijke bestuurder.

8.3. Kleinere instellingen (principe 14)

Tekst:

> ***"Principe 14 –*** *In kleinere instellingen kan de compliancefunctie uitgeoefend worden door een lid van de effectieve leiding. In voorkomend geval kan beroep gedaan worden op een deskundige. De instelling informeert hieromtrent voorafgaandelijk de toezichthoudende overheden."*

Welke instellingen worden hier bedoeld? De Circulaire vermeldt geen enkele verduidelijking qua omvang of omzet. De instelling kiest zelf, maar moet voorafgaandelijk haar keuze bij de toezichthouders aanmelden en met hun eventuele opmerkingen rekening houden. We kunnen daarbij denken aan niche-verzekeraars, kleine dochterondernelmingen binnen een groep, bedrijven die om reden van erkenningsproblematiek afgesplitst werden (bv. het onder eenzelfde merknaam uitoefenen van de activiteiten Leven, Niet-leven, Arbeidsongevallen, …) of bedrijven in de fase van run-off. Voor de pensioenfondsen bepaalt de toepasselijke Circulaire dat de uitbesteding van de functie onder leiding van een directielid steeds mogelijk is.

Het lid van de effectieve leiding dient zelf aangemeld te worden als verantwoordelijke voor de compliancefunctie. Dit houdt meteen ook in dat hij de erkenning van de FSMA moet hebben verworven (met alle vereisten inzake ervaring, examen, diploma en permanente opleiding vandien).

Het risico op mogelijke belangenconflicten, zoals onder de vorige principes besproken, zal wellicht groter zijn. Dergelijke conflicten dienen bijgevolg zowel structureel als in de praktijk vermeden worden. Een combinatie met de risicobeheerfunctie wordt eventueel toegelaten.

De criteria voor het beroep op een deskundige zijn dezelfde als onder het vorige principe, maar bij kleinere instellingen kan het om een blijvende opdracht gaan die deeltijds wordt uitgeoefend. Bijgevolg dienen hierop de modaliteiten van de **Circulaire Uitbesteding** toegepast te worden. De deskundige kan ook intern binnen de groep gekozen worden. De mogelijkheid bestaat dus om op de erkende Compliance Officer of medewerker van een zusterbedrijf een beroep te doen.

9. Samenvatting

De Circulaire Compliancefunctie van NBB en FSMA van 4 december 2012 vervangt de vroegere Circulaire D.255. Ze werkt de compliancefunctie uit zoals opgenomen in het vernieuwde artikel 14bis van de Controlewet.

Naast de zichtbare verschillen (de Circulaire D.255 telde 10 bladzijden, de huidige daarentegen 24; de Circulaire D.255 stelde 10 principes voorop, de huidige voorziet er 14), werden diepgaande evoluties zwart op wit geformaliseerd die in andere wetten of Circulaires reeds gedeeltelijk aan bod gekomen waren.

De Compliancefunctie wordt meteen sterk geduid:

> "*De compliancefunctie is voor de financiële instellingen van fundamenteel belang voor de beheersing van hun integriteit en voor de bescherming van de financiële consument.*"

> "*De Compliancefunctie is belast met het toezicht op de naleving van de wettelijke en/of reglementaire integriteits- en gedragsregels, die van toepassing zijn op de instellingen;*"

Meteen wordt de functie als een sleutelfunctie voor het beheer van een verzekeringsonderneming naar voor geschoven, naast de (minimaal 2) leden van de effectieve leiding of het Directiecomité, de Interne Auditor, de riskfunctie en de actuariële functie. Beide toezichthouders uiten hun voorkeur voor het principe waarbij per onderneming één hoofd van de Compliancefunctie verplicht moet worden aangesteld, maar niet meer dan één.

Het aantal domeinen onder toezicht van de Compliancefunctie is sterk uitgebreid van de "prioritaire" vijf domeinen, naar "tenminste" vijftien. Alle wetten met bepalingen van dwingend recht die de consument beschermen, moeten opgevolgd worden. De effectieve leiding kan hieraan nog domeinen toevoegen. De evoluties rond IMD II en MiFID II zullen op hun beurt ongetwijfeld voor een verdere uitbreiding zorgen. De werkdomeinen worden opgedeeld volgens de financiële sectoren en volgens de bevoegdheden van de respectievelijke toezichthouders.

Schematisch overzicht

NBB	*FSMA*	*Andere regelgevingen en toezichtsorganen*	
		Regelgeving	*Toezicht*
Preventiewet Witwassen	*WFT art 45 §2-*	*W. Antidiscriminatie*	*Centrum Gelijke Kansen*
Bijzondere Mechanismen	*Bescherming verzekeringnemer, cliënteninformatie en publiciteit*	*W. Marktpraktijken en consumenten-bescherming*	*Economische inspectie*
Onverenigbaarheid mandaten, Fit&Proper	*W. Verzekeringsbemiddeling*	*W. Privacy*	*Privacycommissie*
Controlewet – art 14bis	*Controlewet – art 14bis*	*Codes Assuralia*	*Compliance Officer*
Deugdelijk bestuur	*W. Hypothecair krediet*	*Interne codes*	*Compliance Officer*
Uitbesteding	*W. Discriminatie –art 12*	*Financiële embargo's*	*CFI*
Behoorlijk beloningsbeleid	*Behoorlijk beloningsbeleid*	*Fatca, Bribery act*	*buitenlandse instellingen*

De nieuwe Circulaire Compliance geeft afzonderlijke definities voor de begrippen “Compliance”, “Effectieve Compliance”, “compliancerisico” en “compliancefunctie”. In het Compliance Charter nemen we best deze begrippen op om dit aan alle stakeholders (medewerkers, tussenpersonen, klanten) te duiden.

De toezichthouders hebben gekozen voor een duidelijke toepassing van het COSO-model met de *three lines of defence*. De opdracht wordt als eerste principe opgenomen:

- identificatie en beoordeling van het compliancerisico (risk assessment);
- advies betreffende het beleid en het nemen van beheersmaatregelen verlenen;
- monitoring;
- opleiding, sensibilisering;
- risk-based actieplan met inbegrip van te verwachten ontwikkelingen (wet, systemen, markt).

Het COSO-model komt verder terug in de positionering van de compliancefunctie als tweedelijnsfunctie, de nog duidelijkere afscheiding van de andere transversale (controle)functies en de versterking van de interne governance. De proportionaliteit wordt gedefinieerd in drie principes:

- de regels voor het werken binnen een groepsstructuur (principe 12);
- de modaliteiten betreffende de mogelijkheid om op een externe deskundige een beroep te doen (principe 13);
- de regeling voor kleinere instellingen (principe 14).

De adviezen van de compliancefunctie krijgen een bijzondere kracht door toepassing van het principe “comply or explain”. Ze zijn niet bindend, maar evenmin vrijblijvend. De effectieve leiding van de onderneming kan er dus enkel van afwijken mits duidelijke motivering. Daarenboven is de effectieve leiding verantwoordelijk.

De principes worden als norm gesteld en niet als aanbeveling. Ze worden veelal uitgebreid toegelicht met good practices. De rechtsgrond en –kracht van deze "soft law" is evenwel niet altijd duidelijk.

Het wordt een grote uitdaging voor de Compliance Officers om de gevraagde omvangrijke risicoanalyse met monitoringtechnieken te combineren en zo tot een beheersinstrument voor de leiding van de instelling te komen.

De evolutie in de periode 2005 – 2012 leidde tot een verhoogde aansprakelijkheid van de Compliancefunctie. Ter illustratie hiervan kan worden verwezen naar het spanningsveld met eerste lijn en management, de actieve monitoringrol, de aanzienlijke uitbreiding van domeinen, de gevallen van Compliance Officers die bij diverse gerechtelijke en gemediatiseerde procedures in binnen- en buitenland betrokken raakten.

Aldus ontstaat het gevoel dat deze evolutie ertoe leidt dat de Compliance Officer straks volgens de beste Britse traditie een *"public servant within a private company"* kan worden genoemd.