# 8 Compliance en integriteit kloppen aan de hoogste deur van de governancestructuur

*Sylvie Bleker-van Eyk*

## 8.1. Inleiding

Compliance en integriteit zijn als onderwerpen niet meer weg te denken op bestuurlijk niveau. Zowel bestuurders als commissarissen raken langzaam gewend aan deze nieuwe pionnen op het schaakbord, maar het spelen hiermee is nog wat onwennig. Zo moet de compliance officer kunnen escaleren wanneer de organisatie door – meestal non-financiële – risico's bedreigd wordt. Dit kan door het bestuur als bedreigend worden ervaren. Compliance en integriteit kloppen aan de hoogste deur van de governance-structuur. Dient compliance ieder kwartaal plaats te laten nemen aan de vergadering van de Raad van Bestuur (RvB) en zelfs de Raad van Commissarissen (RvC)? Moet de compliance officer beschikken over een directe lijn naar de Audit Committee?

Zowel bestuurders als commissarissen kunnen rechtstreeks worden aangesproken op non-compliant gedrag binnen de organisatie. Zo troffen de bestuursvoorzitter en enkele voormalige commissarissen van de Woningcorporatie een schikking met Vestia van € 4,8 miljoen, in ruil voor het intrekken van een rechtszaak door Vestia.[1] Het Openbaar Ministerie (OM) ziet de voorzitter van de RvC als de persoon die uiteindelijk de macht heeft in te grijpen indien de organisatie strafbare fouten begaat. Het OM verwacht in dergelijke situaties een rigide ingreep door de RvB en – indien de RvB in gebreke blijft – de RvC. Zo niet dan acht het OM ook de RvC (met de voorzitter als eerstaangesprokene) verantwoordelijk voor het in stand houden van strafbare praktijken.

De rol van bestuurders en commissarissen doorgaat ingrijpende veranderingen. Naar aanleiding van een lange reeks compliance- en integriteitgerelateerde incidenten in verschillende sectoren worden er steeds vaker eisen gesteld aan de deskundigheid en integriteit van de bestuurders en commissarissen. Dit geschied door de toezichthouder of de branchevereniging. In het herzieningsvoorstel voor de Corporate Governance Code komt het onderwerp van specifieke deskundigheid eveneens naar voren in principe 2.1.4.[2] De commissaris wordt verwacht deskundig

1 www.nrc.nl/nieuws/2016/01/06/vestia-treft-schikkingen-met-oud-bestuurder-staal-en-oud-commissarissen.

2 "Elke commissaris en elke bestuurder beschikt over de specifieke deskundigheid die noodzakelijk is voor de vervulling van zijn taak. Elke commissaris dient geschikt te zijn om de hoofdlijnen van het totale beleid te beoordelen. Minimaal één commissaris beschikt over specifieke deskundigheid op het gebied van technologische innovatie en nieuwe business modellen." De Nederlandse Corporate Governance Code, Voorstel voor herziening, Een uitnodiging voor commentaar, www.commissiecorporategovernance.nl/download/?id=2786, p. 28.

en integer te zijn. Deskundigheid kan worden getoetst en daarin kunnen de commissarissen worden bijgespijkerd. Integriteit daarentegen zit in de mens zelf. De kennis van de normen kan worden getraind; zo ook de gewenste handelswijze, maar de daad bij het woord voegen blijft een kwestie van het persoonlijk handelen 'in het moment'.

In dit hoofdstuk wordt antwoord gegeven op de vraag hoe belangrijk compliance is in de bestuurskamer en hoe bestuurders en commissarissen met compliance dienen om te gaan. Hiervoor zal eerst worden omschreven wat onder compliance wordt verstaan. Vervolgens wordt beschreven wat de positie is van compliance binnen de organisatie en hoe deze dient te worden vertaald in de governancestructuur om uiteindelijk een vorm van handleiding te bieden voor bestuurders en commissarissen voor een optimale werkrelatie met de compliance officer.

## 8.2. Wat wordt verstaan onder compliance en integriteit?

In de nieuwe Corporate Governance Code wordt geen definitie gegeven omtrent hetgeen onder compliance wordt verstaan.[3] Wel blijkt dat de beheersing van compliancerisico's een vaste plaats heeft verworven. In principe 1.2.3 wordt vastgesteld:

*"Het bestuur monitort de werking van de interne risicobeheersings- en controlesystemen en voert ten minste jaarlijks een systematische controle uit op de effectiviteit van de opzet en de werking van de systemen. Deze monitoring ziet op alle materiële controlemaatregelen, waaronder de financiële, operationele en compliance (curs. ed.) aspecten, en houdt rekening met geconstateerde zwaktes en geleerde lessen, signalen van klokkenluiders en bevindingen van de interne audit functie en de externe accountant. Waar nodig worden verbeteringen in interne risicobeheersings- en controlesystemen doorgevoerd."*

In principe 1.4.1 staat vermeld dat het bestuur in het bestuursverslag verantwoording aflegt over:

*"i. de uitvoering van het risico assessment en beschrijft de voornaamste risico's waarvoor de vennootschap zich geplaatst ziet en de risk appetite van de vennootschap. Hierbij kan gedacht worden aan strategische, operationele, financiële, compliance en niet-financiële risico's."*

Ten slotte, in principe 1.2.3. staat dat het bestuur ten minste jaarlijks een systematische controle uitvoert op de effectiviteit van de opzet en de werking van de interne risicobeheersings- en controlesystemen. Deze monitoring ziet op alle materiële controlemaatregelen, waaronder de financiële, operationele en compli-

3 De Nederlandse Corporate Governance Code, Voorstel voor herziening, Een uitnodiging voor commentaar, www.commissiecorporategovernance.nl/download/?id=2786, p. 12 en 16.

ance-aspecten. Hier staat compliance blijkbaar weer wat steviger in de schoenen; het hoort erbij, terwijl het in 1.4.1.i meer als een optie wordt neergezet.

Helaas geeft het voorstel tot de herziening van de Corporate Governance Code geen duidelijkheid omtrent hetgeen onder compliance moet worden verstaan. De vaste plaats van compliance binnen de governance van een organisatie verdient een duidelijkere verankering binnen de Corporate Governance Code. Immers compliance betreft de wijze waarop binnen de grenzen van de wet en de intern en extern gemaakte afspraken de kerndoelstellingen van de organisatie behaald dienen te worden. Een voorbeeld kan hier verhelderend werken. Uit wet- en regelgeving vloeien verplichtingen voort die bij het risico van niet-naleving een directe relatie kunnen hebben met de 'license to operate' van de organisatie. Neem bijvoorbeeld de financiële instellingen. Zij dienen compliant te zijn met een ingewikkeld net van wet- en regelgeving, anders lopen ze het gevaar hun vergunning te verliezen. Zij moeten zich ook aan de Arbowet 1998 houden, maar de naleving hiervan zal bij human resources worden belegd en niet bij compliance. Echter, bij een advieskantoor op het gebied van Arbowetgeving, zal de naleving van de Arbowet 1998 een cruciaal onderdeel zijn en bij compliance kunnen worden ondergebracht. Immers, de geloofwaardigheid van het kantoor en daarmee de 'license to operate' is in gevaar indien het zelf de Arbowetgeving aan haar laars lapt. Complianceri-sico's zijn risico's die de spreekwoordelijke 'stekker' uit de onderneming kunnen halen, of in ieder geval kunnen leiden tot grote materiële en ook reputatieschade.

In deze bijdrage zal de volgende definitie van compliance worden gehanteerd:[4]

"*Het in de meest algemene zin bevorderen en handhaven van de (Europese/inter) nationale wet- en regelgeving en van de interne normen en procedures van de organisatie, te bescherming van de integriteit van de organisatie, alsmede de integriteit van haar bestuurders en medewerkers met als doel (compliance) risico's te beheersen en de daaruit voortvloeiende schade te voorkomen."*

Deze definitie is in één woord samen te vatten: compliance is *gedrag.* Het is de opdracht om binnen de lijntjes te kleuren. De zwarte lijn rondom de kleurplaat is samengesteld uit wet- en regelgeving. Deze mag niet overschreden worden. De interne processen en procedures inclusief de interne gedragsnormen vormen het kleurenpalet waardoor iedere organisatie haar eigen kleurplaat vormt. Het is dan ook niet verstandig om interne gedragsnormen via 'copy paste' van het internet te halen, want kern van de organisatie wordt gevormd door bij haar passend gedrag en dat kan niet gekopieerd worden: het is immers de eigen identiteit.

Uit bovenstaande definitie blijkt dat integriteit onlosmakelijk verbonden is aan compliance. Immers ook het niet naleven van intern geldende normen en richtlijnen

4 Prof. Dr. S.C. Bleker-van Eyk, Van Holbewoner tot Marsverkenner, inaugurale reden, VU, 23 juni 2015, p. 2.

kunnen risico's met zich meebrengen en zelfs in het ergste geval de 'license to operate' in gevaar brengen.

Wie in de voorgestelde herziening van de Corporate Governance Code zoekt naar verwijzingen omtrent de integriteit van de organisatie, haar bestuurders en medewerkers komt niet verder dan de verwijzingen rond de integriteit van de financiële verslaglegging en het 'In control statement'.[5] Wederom ontbreekt de beschrijving van een belangrijk onderdeel: 'integriteit'! Het is duidelijk een zeer beperkte visie op integriteit en richt zich vooral op de correcte weergave van de financiële verslaglegging. Imtech Duitsland vormt een uitstekend voorbeeld van de risico's van de beperkte zienswijze. Imtech Duitsland liet steeds mooie resultaten zien. Jarenlang werd niet getwijfeld aan de integriteit van de verslaglegging, totdat bleek dat het in de basis bijna volledig ontbrak aan interne risicobeheerssystemen. Er was niet eens een internal audit of controlfunctie. Liquiditeit werd geschapen door bijvoorbeeld een voorschot verkregen dankzij omkoping.[6]

Integriteit is niet een term die zich eenvoudig laat vatten in een paar kernelementen. Integriteit lijkt wel het hete kooltje dat heen en weer wordt gegooid. Wie wil zijn handen branden aan iets wat ongrijpbaar lijkt, maar dat wel ernstige verwondingen kan aanbrengen. Opvallend is dat het begrip *integriteit* doorgaans gekoppeld wordt aan de *persoonlijke* integriteit. Aan de hand van verschillende termen zoals 'onkreukbaar', 'eerlijk', 'oprecht', 'onomkoopbaar' of 'betrouwbaar' wordt getracht de kenmerken aan te geven waar een 'integer' persoon over dient te beschikken. Het gaat om personen en daarom vinden we het moeilijk om die rechtstreeks op hun karaktereigenschappen aan te spreken. Integriteit heeft alles te maken met 'handelen in het moment'. Het zijn de omstandigheden van het moment die soms tot grote onverwachte handelingen kunnen leiden. Zo kan een 'grijs muisje' onder extreme omstandigheden zich ontpoppen tot een ware held. Echter, het komt ook voor dat mensen waarvan eenieder denkt dat zij voldoen aan alle bovenstaande kernmerken van integriteit genadeloos door de mand vallen. De vraag die dan gesteld moet worden is: was het een wolf in schaapskleren of was het onder die omstandigheden begrijpelijk dat de persoon handelde in strijd met alles waar hij of zij voor staat? Een mooi voorbeeld was een bestuurslid van een grote financiële instelling die bij de douane in een Afrikaans land gevraagd werd naar zijn vaccinatieboekje. Zijn paspoort had hij wel bij zich, maar niet zijn vaccinatieboekje. Hij werd voor het dilemma gesteld: betalen of geïnjecteerd worden met een vieze naald die de ambtenaar tevoorschijn haalde. Hier is de keuze eenvoudig. Niemand zal zijn integriteit in twijfel trekken, ook al heeft hij een ambtenaar omgekocht. Maar wat nu in het geval dat een RvC al gedurende lange tijd alle zeilen bij moet zetten om een bedrijf in zwaar weer te herfinancieren. Wekelijkse vergaderingen die tot in de nacht duren. Dan verschijnt er plots een brief bij de voorzitter van de RvC van de compliance officer waarin een probleem rondom

5 De Nederlandse Corporate Governance Code, Voorstel voor herziening, Een uitnodiging voor commentaar, www.commissiecorporategovernance.nl/download/?id=2786, p. 16.
6 http://nos.nl/artikel/2021546-imtech-mogelijk-weer-betrokken-bij-schandaal.html.

de integriteit van de CFO aan bod komt. Het doorspelen van de brief aan de overige commissarissen kan grote gevolgen hebben voor het gehele bedrijf. Wat te doen? Dit is een groot dilemma waar zeer verschillend op gereageerd kan worden. Ook zijn er verschillende gradaties mogelijk in de te volgen acties. Persoonlijke integriteit is een gloeiend kooltje; je weet pas wat je doet als je in die omstandigheden wordt geplaatst. Het is verstandig om bestuurders en commissarissen op gezette tijden een dilemmatraining te geven. Geen gratuite dilemma's, maar zaken die op het scherpst van de snede moeten worden beslist. Wellicht is simulatietraining hier een goede optie.

Compliance- en integriteitsmanagement richt zich op het gedrag van mensen in een organisatorisch verband, dat wordt begrensd door extern en intern gemaakte afspraken; de *organisatorische* integriteit. Hier ligt de nadruk op de interne normen die met elkaar zijn afgesproken en waar allen die deelnemen aan de organisatie zich aan dienen te houden. De normen gelden binnen de organisatie en afwijkend gedrag wordt doorgaans niet aanvaard en kan zelfs reden zijn om een arbeidscontract te beëindigen. De normen tekenen het wezen van de organisatie en organisatorische integriteit speelt zich af binnen de kaders van de gestelde normen. Zo kan vanuit het perspectief van organisatorische integriteit de Maffia gezien worden als een uiterst integere organisatie. Op de overtreding van een van de kernwaarden van de organisatie – de omertà – staat een duidelijke straf. Gelukkig wordt er bij organisatorische integriteit uitgegaan van organisaties die hun activiteiten niet uitoefenen buiten de kaders van de nationale strafwetgeving.

Doorgaans komen we bij de zoektocht naar de integriteit van een organisatie terecht bij de algemene normen zoals neergelegd in de gedragscode en die grotendeels overeenkomen met de gedragsnormen die gelden binnen het land – of liever gezegd continent – waar de moedermaatschappij is opgericht. De kunst is dan ook om bij multinationale ondernemingen die juiste toon te vinden die culturen met elkaar verbindt in plaats van scheidt. Een prachtig voorbeeld in deze is de Nederlandse norm die eind jaren zestig van de vorige eeuw gold binnen een in Nederland gebaseerde multinationale onderneming omtrent gezondheidszorg. In Nederland werd de gezondheidszorg voor medewerkers en hun gezin vanuit de onderneming gratis verzorgd. Een jonge manager kreeg zijn eerste directeurschap in Afrika. Hij moest een fabriek neerzetten. Er waren destijds nogal wat problemen in verschillende Afrikaanse landen en de moedermaatschappij had ook al enige problemen ondervonden. Een manager vroeg directeur hoe er ter plaatse met de gezondheidzorg moest worden omgegaan? De directeur beantwoordde de vraag eenvoudig door te zeggen dat hij dezelfde norm wilde hanteren als in Nederland: gratis gezondheidzorg voor alle medewerkers en hun gezin. De manager legde uit dat in dit Afrikaanse land het 'gezin' in feite het gehele dorp behelst. De jonge directeur begreep het probleem niet en paste de Nederlandse regel ruimhartig toe. Achteraf bleek het een van de fabrieken te zijn waar weinig problemen waren door de sociale rust die er heerste. Een toevalstreffer? Nee, een vertaling van een nationale norm naar een universeel erkend beginsel van gelijkheid. Twee schijnbaar tegenstrijdige

uitgangspunten bleken één gelijkluidende kern te hebben: gezondheidzorg binnen de sociale omgeving van de medewerker biedt rust en bevordert de capaciteit van de medewerker. De definitie van de 'sociale omgeving' is cultureel bepaald.

Veel vaker zien we de krampachtige vertaling van 'Westerse' normen naar andere culturen toe. Bepaalde waarden zijn nu eenmaal niet overal gelijk en kunnen stuiten op weerstand. Bijvoorbeeld de gelijkheid van de vrouw en het recht van de vrouw om buitenshuis te werken. De Verenigde Naties en de Internationale Arbeidsorganisatie maken zich hier hard voor. Veranderingen vinden vaak plaats via de weg van de geleidelijkheid en educatie. Er is geen gulden regel die aangeeft wat wel en wat niet kan. Het is en blijft mensenwerk, waarbij diplomatie, tact en wederzijds respect de boventoon dienen te voeren.

Ten slotte, er bestaat ook nog de integriteit van het systeem, zoals bijvoorbeeld het financiële systeem. Bij systeemintegriteit spelen naast het gedrag nog andere systeemtechnische factoren mee. Bij deze vorm van integriteit zal in deze bijdrage verder niet worden stilgestaan.

## 8.3. De compliancefunctie

### *8.3.1 De plaats van compliance binnen de organisatie*

Financiële instellingen zijn vanaf het eind van de jaren negentig van de vorige eeuw langzaamaan vertrouwd geraakt met compliance. Na de schandalen van begin van deze eeuw en de daaropvolgende economische en financiële crisis, is het belang van compliance voor financiële instellingen niet meer weg te denken.

Langzaam wordt de term 'compliance' ook bekend bij andere sectoren. Het is niet ongebruikelijk dat alvorens na te denken over de mogelijke inrichting van compliance in een niet-financiële organisatie, eerst een blik geworpen wordt hoe de financiële instellingen het hebben aangepakt: 'beter goed gestolen dan slecht bedacht'. Helaas gaat deze gedachte niet op. Ten eerste, het betreft een zwaar gereguleerde markt met specifieke nationale, internationale en buitenlandse wetgeving en toezichthouders. Daarnaast blijkt dat compliance bij financiële instellingen ontstaan is als reactie op steeds verdergaande regulering en niet is ontstaan op basis van een weloverwogen strategische ingreep in de structuur. Een kritische blik verdient aanbeveling bij het opzetten van een compliancestructuur. Ter illustratie een praktijkvoorbeeld van enige jaren geleden, waarin een bestuurder in overleg met een – toen nog in de kinderschoenen staande – toezichthouder besloot dat de niet-financiële onderneming een compliancefunctie moest opzetten. Gezamenlijk hadden zij een financiële instelling om hulp gevraagd en gingen aan de slag met een compliance die bij een bank paste maar niet bij deze organisatie.

Bij de definitie van compliance werd hierboven gesteld dat het dient ter verwezenlijking van de kerndoelstellingen. De compliance moet 'passen' bij de soort van bedrijvigheid en dient aan te haken bij de vereisten die de toepasselijke toezichthouders stellen bij de verwezenlijking van die doelstellingen. De mate waarin de markt gereguleerd is, zal een belangrijke stempel drukken op de aard en de omvang van de te realiseren compliancefunctie.

Compliance past uitstekend in de gedachte van de 'five lines of defense'. Intern zijn er drie defensielinies te onderscheiden: de business, de adviserende en ondersteunende onderdelen en als derde de intern controlerende onderdelen. De vierde defensielinie wordt gevormd door de externe accountant. Ten slotte, de toezichthouder vormt de vijfde defensielinie. Compliance heeft een adviserende rol en past derhalve in de tweede linie. Een belangrijke les die we uit de afgelopen economische en financiële crisis kunnen trekken is dat compliance steeds vaker de bal toegespeeld krijgt vanuit de business waar het de besluitvorming rond omstreden zaken betreft, terwijl compliance adviseert en niet direct bij het spel betrokken is. Hetzelfde overkomt internal audit, die in het spel de rol van grensrechter speelt. In de financiële instellingen werden te moeilijke vraagstukken steeds vaker teruggelegd bij compliance (en zelfs bij internal audit) met de vraag: "mag dit of mag dit niet". Het betrof allerlei onderwerpen zoals transacties en klantacceptatie. Hier gaat iets fout! Immers, de business zelf dient de besluiten te nemen en niet de verantwoordelijkheid voor de te nemen besluiten elders te beleggen. De business besluit of een transactie is toegestaan, of een klant wel of niet wordt geaccepteerd. Compliance heeft tot taak de kaders waarbinnen het spel wordt gespeeld, te stellen en te adviseren over nieuwe wet- en regelgeving, interne gedragsnormen et cetera. Het is begrijpelijk maar ongewenst dat de business zich tot compliance wendt. Vandaar dat tegenwoordig bij financiële instellingen ook medewerkers met compliancekennis in de eerste lijn worden geplaatst.

Deze gang van zaken lijkt wellicht omslachtig en wekt de indruk dat compliance het gloeiende kooltje niet durft pas te pakken, maar er is een goede reden voor deze gang van zaken.

In de business worden de besluiten genomen. Compliance adviseert de business en daarmee ook de RvB als ultieme verantwoordelijke in de business, omtrent de kaders waarbinnen gewerkt dient te worden. Het management dient ervoor te zorgen dat de medewerkers op de hoogte zijn en blijven van de kaders waarbinnen ze hun werk moeten vervullen. Compliance onderzoekt welke verplichtingen de wet- en regelgeving stellen. Compliance adviseert omtrent de wet- en regelgeving en verzorgt de training van het personeel in de business. Op zich geen eenvoudige klus! Er zijn veel wetten en regels en vele toezichthouders. De regels zijn lang niet altijd op elkaar afgestemd en soms worden er zelfs ronduit tegenstrijdige eisen gesteld. Wat in het ene land mag, kan elders strikt verboden zijn. De wereld is niet zwart-wit, maar kent vele grijsschakeringen. De business – de RvB – besluit uiteindelijk welke risk appetite de organisatie heeft: zeilt het aan de wind of juist

zeer behoudend. Die keuze ligt niet bij compliance! Toch heeft compliance hier een rol te spelen, zeker waar de onderneming surft op de golf tussen het toelaatbare en het ontoelaatbare, te weten: de rol van compliance als counterveiling power.

### *8.3.2 Compliance als counterveiling power*

De afgelopen tijd heeft De Nederlandsche Bank (DNB) steeds meer aandacht getoond voor hetgeen zich afspeelt in de bestuurskamer. Een belangrijk onderwerp voor DNB is het organiseren van 'tegenspraak' binnen een organisatie. In 2013 stelt DNB dat zij het opvallend vindt "dat slechts enkele organisaties bewuste maatregelen hebben genomen om tegenspraak in de top van de organisatie structureel te organiseren".[7] De meest belangrijke taak van de compliance officer is die van counterveiling power ten opzichte van de business. Compliance dient haar geluid tot in de bestuurskamer te kunnen laten horen. Zelfs gedurende de Audit Committee-vergaderingen van de RvC. Immers het is de taak van compliance om als bemiddellaar en evenwichtshersteller te fungeren tussen de belangen van de onderneming en de belangen van de samenleving die verwoord zijn in de wet- en regelgeving en de interne integriteitsnormen. Zelfs de interne integriteitsnormen moeten volgens DNB bezien worden in het licht van maatschappelijk aanvaardbare normen. In haar reactie op de zogenoemde Panama Papers stelt DNB dat het niet meer voldoende is dat een organisatie zich houdt aan de wet en de eigen interne integriteitsnormen. Volgens DNB moet het gedrag van de organisatie ook overeenkomen met de geldende maatschappelijke normen.[8] Hier zien we opnieuw de belangrijke link tussen compliance en integriteit, waarbij DNB een brede uitleg geeft aan geldende integriteitnormen door te stellen dat wettelijk toegestaan kan worden 'overruled' door 'maatschappelijk betamelijk gedrag', waarbij gekeken wordt naar wat de maatschappelijk aanvaarde norm is 'in het moment'.

Het onderwerp van 'counterveiling power' is gelanceerd door de econoom Galbraith. Hij stelde dat "private economic power is held in check by the countervailing power of those who are subject to it".[9] Galbraith verwijst hier naar de krachtenvelden binnen de markteconomie waarbij hij stelt dat de economische macht die in de handen van een relatief klein aantal bedrijven ligt zorgt voor sterkere aanbieders, maar uiteindelijk ook leidt tot sterkere afnemers. Volgens Galbraith "the existence of (…) power creates an incentive to the organization of another position of power that neutralizes it".[10] De mogelijkheden voor externe 'tegenspraak' wordt voor organisaties steeds groter door de moderne ontwikkelingen zoals social media. Het is echter van belang om ook interne 'tegenspraak' te institutionaliseren. Dat wil zeggen dat binnen de organisatie de mogelijkheid gegenereerd moet worden waar andere geluiden kunnen doordringen tot de RvB

7 DNB, Leading by example,Gedrag in de Bestuurskamer: cultuur, 9 maart 2013, p. 7.
8 www.dnb.nl/nieuws/nieuwsoverzicht-en-archief/persberichten-2016/dnb341434.jsp, 19 mei 2016.
9 J. K. Galbraith, American Capitalism: chapter IX: The Concept of Countervailing Power, Houghton Mifflin, Boston, 1952, p. 118.
10 Galbraith 1952, p. 119.

en de RvC, opdat zij een zo goed mogelijk afgewogen beslissing nemen. In feite dient de discussie rond de twee zijden van iedere medaille geïnstitutionaliseerd te worden.

De vraag is echter waar de counterveiling power dient te liggen; bij de Ondernemingsraad? Echter, de Ondernemingsraad heeft een beperkt takenpakket voor ingrijpende zaken die de onderneming wezenlijk treffen (advies) of zaken die de medewerkers rechtstreeks treffen (instemming).[11] Daarbij treedt de Ondernemingsraad op in het belang van de medewerkers en niet zozeer in het algemeen belang. Gezocht wordt naar de 'Japie Krekel' van de onderneming die met kennis van de kaders het debat aangaat over de invulling van de kaders en duidelijk de rode kaart trekt zodra de kaders worden overschreden of het in strijd is met hetgeen maatschappelijk betamelijk is. Alhoewel de laatste waarschuwing niet per se hoeft te leiden tot het stopzetten van een activiteit. Dat is afhankelijk van de door de RvB vastgestelde risk appetite.

Wil de compliance officer zijn rol als counterveiling power daadwerkelijk kunnen uitoefenen, moet er naast het periodiek overleg met de RvB en de RvC ook een directe lijn zijn tussen de compliance officer en de voorzitter van de RvC of de Audit Committee. Immers, het is van belang dat als de compliance officer een acuut probleem onderkent voor de organisatie en de RvB de ernst van het risico naar de mening van de compliance officer onjuist inschat, dat hij zich rechtstreeks kan wenden tot de RvC. Het spreekt voor zich dat het een uitzonderlijk geval zal betreffen. Zo ook het geval dat de compliance officer ziet dat (leden van) de RvB zich willens en wetens bezighouden met ongeoorloofde praktijken. In dat geval moet hij direct toegang hebben tot de RvC en als hij daar nul op het rekest krijgt, zal hij zich moeten wenden tot de toezichthouder.

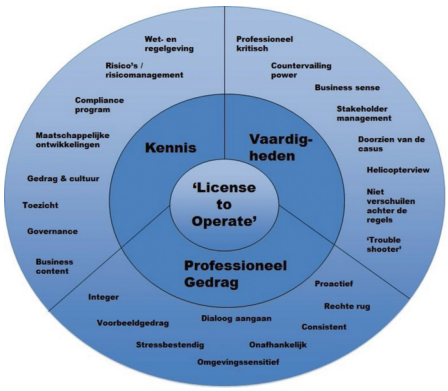
De compliance officer dient dus naast de behoeder van de risico's voor het overtreden van wet- en regelgeving, tevens het ethisch geweten van de organisatie te zijn. Immers, de compliance officer is de behoeder van de interne normen en regels waaronder de gedragsnormen.

Hieronder zal nader worden ingegaan op de structuur van de compliancefunctie. Echter, wil de compliance officer ook het geweten van de organisatie zijn, dan moeten er strenge eisen worden gesteld aan de deskundigheid en de integriteit van de compliance officer, alsmede de meer persoonlijke kenmerken zoals: vastberadenheid, rechte rug, onkreukbaarheid, argumentatiekunde et cetera. Opvallend is dat voor bestuurders en commissarissen steeds vaker strenge vereisten worden gesteld aan hun deskundigheid en integriteit, maar dat men soortgelijke vereisten niet vindt bij compliance officers. Organisaties stellen nu zelf vereisten zoals een DSI-registratie, een Verklaring omtrent Gedrag (in zoverre deze VoG inhoudelijk zoden aan de dijk zet voor de functie van een morele dijkbewaarder) en minimale

11 Wet op de Ondernemingsraden: artikel 25 WOR (adviesrecht) en artikel 27 WOR (instemmingsrecht).

opleidingsvereisten. Echter, aan degene die het tegengeluid moet laten horen en zijn of haar rug recht moet houden tegenover zijn of haar meerdere (de bestuurder), worden minder vereisten gesteld. Wellicht de moeite waard om hier meer inzicht te verschaffen in de eigenschappen en vaardigheden die van een compliance officer mogen worden verwacht. Zoals bij alles in het leven moeten ook bij de compliance officer de verschillende eigenschappen in balans zijn. Immers, een notoire dwarsdenker of een jaknikker zullen een goede en effectieve dialoog in de weg staan. In figuur 1 zijn de vereisten onderverdeeld in vaardigheden, eigenschappen en professioneel gedrag.[12]

***Figuur 1*: Vereisten aan de compliance officer: vaardigheden, eigenschappen en professioneel gedrag**




### *8.3.3 Compliancestructuur*

In deze bijdrage zal verder niet worden stilgestaan bij de opzet van compliance binnen de grote financiële instellingen, maar zal met name gekeken worden naar niet-financiële grote en middelgrote organisaties, waarbij de omvang van de functie afhankelijk is van marktomstandigheden.

Ook buiten de financiële sector zien we bij de grotere (multi)nationale ondernemingen het onderwerp van compliance steeds meer naar voren komen. Dit kan allerlei redenen hebben. Bijvoorbeeld omdat de markt sterk gereguleerd is. Denk hier aan de telecombedrijven of de energiesector. In feite kent iedere sector wel min of meer een vorm van regulering, al is het maar vanuit de Autoriteit Consument en Markt (ACM), waarbinnen onder andere gekeken wordt naar eerlijke concurrentie. Nederland kent honderden toezichthouders. Waarvan slechts de grote bekendheid genieten. Vele kleinere toezichthouders zijn actief in een specifieke niche.

12 Postdoctorale Opleiding Compliance & Integriteit Management, openingscollege 2015, VU, p. 17.

De structuur van de compliance dient te worden vastgesteld in een zogenoemd 'Compliance Charter'. Dit document dient als een soort van 'grondwet' voor compliance en moet idealiter de volgende onderwerpen beschrijven:

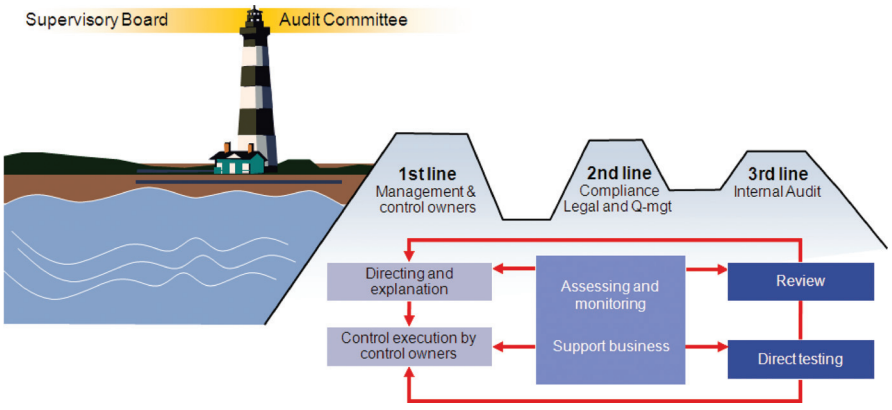
1. De visie van de organisatie over compliance en de doelstelling die de organisatie met compliance wenst te bereiken. Dit doel zal gekoppeld moeten zijn aan de realisatie van de kerndoelstellingen van de organisatie.
2. Het toepassingsgebied van compliance. Welke wet- en regelgeving valt onder de noemer van compliance, inclusief de interne gedragsregels?
3. De opzet van de compliancefunctie. De structuur hangt af van verschillende omstandigheden zoals bijvoorbeeld de mate waarin de markt gereguleerd is of de omvang van de organisatie. Zo kan een moedermaatschappij besluiten dat iedere dochteronderneming een eigen compliance officer of zelfs compliance-afdeling heeft. In een markt die niet sterk gereguleerd is, kan het zijn dat iedere dochteronderneming een parttime compliance officer heeft. De crux is de structuur zo op te zetten dat compliance op de juiste wijze binnen de onderneming is belegd en dat de taken die compliance dient te vervullen ook daadwerkelijk vervuld kunnen worden. Compliance is maatwerk.
4. Het beleggen van de verantwoordelijkheid voor compliance alsmede het afleggen van verantwoording over compliance dient strak te worden vastgelegd. De verantwoordelijkheid dient allereerst in de eerste defensielinie te worden belegd en de eindverantwoordelijkheid ligt bij de RvB. De RvC houdt uiteindelijk toezicht. Voor wat betreft verantwoording van de compliancefunctie hangt het ervan af hoe uitgebreid de structuur is binnen de eerste linie. Indien dochtermaatschappijen een eigen compliancestructuur hebben, zal de lokale compliance officer (of een medewerker bij wie ook compliancetaken zijn neergelegd) verantwoording afleggen aan de manager in de eerste linie. Immers, de business is verantwoordelijk voor compliance. Daarnaast zal de compliance officer in de eerste linie ook een functionele rapportagelijn hebben naar het hoofd van compliance van het moederbedrijf.
5. Interne training is van groot belang voor het blijvend bewustzijn van de organisatie voor compliancerisico's en dient daarom ook apart in het Charter benadrukt te worden. Het opstellen, verzorgen en onderhouden van compliancegerelateerde trainingen behoort tot een van de hoofdtaken van compliance.
6. De opzet en werking van een Compliance Comité. Compliance kan niet goed functioneren indien het niet de juiste contacten onderhoudt met de overige onderdelen van de organisatie. Zo dient compliance in het kader van het auditen en monitoren van de naleving van het compliancebeleid samen te werken met internal audit of internal control. Bij compliance-overtredingen zullen de afdelingen juridische zaken en human resources een rol spelen. Ook interne communicatie is van belang voor het communiceren van het compliancebeleid en de interne trainingen. Van groot belang is ook de IT-afdeling, gezien het feit dat veel zaken op gebied van compliance door IT kunnen worden ondersteund. Dit komt ook de efficiëntie ten goede. Het verdient dan ook aanbeveling om een Compliance Comité op te richten waarin al deze functies vertegenwoordigd

zijn en dat periodiek samenkomt voor onderlinge afstemming en het kort houden van de onderlinge lijnen.
7. Ten slotte dient het Compliance Charter duidelijk de taken en bevoegdheden weer te geven. Hierbij dient onderscheid gemaakt te worden tussen de taken en bevoegdheden van de Compliance officer en die van de overige medewerkers met compliancegerelateerde taken (bijvoorbeeld de lokale compliance officers).

In de praktijk is het niet altijd even eenvoudig om een uitgebreid compliancenetwerk op te stellen. Creativiteit biedt daar oplossingen. Bijvoorbeeld: een grote bouwonderneming bestaat uit vele verschillende juridische entiteiten. De projecten worden uitgevoerd met andere grote aannemers en de projecten vormen een eigen juridische entiteit. Een mogelijke oplossing kan zijn om vanuit de moedermaatschappij een *Compliance Shared Service Center* (CSSC) op te richten onder leiding van de compliance officer. De moedermaatschappij zal doorgaans opgesplitst zijn in clusters met ieder hun eigen specialiteit (infrastructuur, bouw et cetera). Onder de clusters kunnen vele verschillende juridische entiteiten worden geplaatst. De clusters krijgen een compliance officer die de verantwoordelijkheid voor de uitvoering van de compliance taken krijgen binnen hun cluster. Echter, het beleid wordt vastgesteld bij de moedermaatschappij en de vele taken worden vervuld door het CSSC ter ondersteuning van de lokale compliance officers of personen met compliancegerelateerde taken. Denk hier bijvoorbeeld aan het monitoren van de compliance door middel van specifieke tools zoals op het gebied van belangenverstrengeling, geschenken, klokkenluiders en sponsoring. Onderzoeken naar overtredingen worden uitgevoerd door het CSSC waarin ook medewerkers van juridische zaken, internal audit, human resources, communicatie meewerken.

Figuur 2 illustreert de rol van compliance en de relatie met de eerste en de tweede linie voor wat betreft de 'dijkbewaking' van de organisatie.

***Figuur 2*: Rol compliance en de relatie eerste en tweede linie**



### *8.3.4 Risk based compliance*

Compliance dient een jaarprogramma op te stellen, waarin de prioriteiten voor het komende jaar alsmede het budget worden vastgesteld. Compliance kan niet alles oppakken. De praktijk leert dat het een steeds veranderende wirwar is aan wet- en regelgeving en eisen van toezichthouders. Compliance dient dus op basis van prioritering te worden aangepakt. De prioritering is rechtstreeks gekoppeld aan de risk appetite van de organisatie. De RvB stelt periodiek de risk appetite van de organisatie vast, in goed overleg met de RvC. Hierbij zal ook aandacht geschonken moeten worden aan de compliancerisico's en in hoeverre deze coûte-que-coûte moeten worden afgedekt. In de praktijk zien we vaak dat zodra een organisatie in het vizier komt van de autoriteiten door vervolging in Nederland – of nog erger – of in het buitenland (de Verenigde Staten van Amerika) de risk appetite omslaat naar risico-aversie die zich op bepaalde gebieden uit in een nultolerantiebeleid met betrekking tot specifieke compliancerisico's.

Het is onverstandig om bij de periodieke – ten minste jaarlijkse – risicoanalyse van de organisatie alle compliancerisico's op één grote hoop te gooien. Dit is echter wel wat in de praktijk vaak gebeurt. Tijdens de sessie met de RvB wordt vaak *het* compliancerisico gewogen. In feite bestaan er vele compliancerisico's en is het van belang om deze risico's van te voren binnen de organisatie in kaart te brengen en vervolgens voor te leggen aan de RvB zodat deze de risico's – na analyse van kans en impact – kunnen prioriteren. De onderbouwing van de belangrijke compliance-risico's dienen ook besproken te worden met de RvC die immers de ultieme interne toezichthouder is. De RvC moet zich realiseren dat ze ook aandacht moet besteden aan compliance en de interne mitigatie van compliancerisico's.

## 8.4. De ISO 19600 Compliance Richtlijn[13]

Een organisatie tracht handen en voeten te geven aan compliance. Als de compliancestructuur dan eenmaal staat, is ook de vraag hoe het staat met de compliance van de organisaties waarmee zij zaken doet. Immers, een compliance-probleem houdt niet op te bestaan zodra het probleem is doorverkocht aan een ander. Het complianceprobleem van de andere onderneming besmet de eigen organisatie door het verkoop- of inkoopkanaal. Zijn er mogelijkheden om inzicht te krijgen van de staat van compliance van de organisaties binnen de supply chain?

De eerste oplossing voor dit probleem is het houden van compliance audits bij de toeleveranciers van de organisaties. Dit is een omslachtige en kostbare manier en wordt – risk based – toegepast door grote organisaties. Het betreft vaak specifieke risico's zoals het gebruik van slavenarbeid of kinderarbeid door de toeleveranciers en weer door diens leveranciers. Naast het belang dat organisaties hechten aan de

13 De auteur is voorzitter van de Nederlandse NEN Commissie inzake de ISO 19600 Compliance Richtlijn.

naleving van mensenrechten, speelt ook de reputatieschade een belangrijke rol bij de opzet van dergelijke audits.

We zien dat er steeds meer certificerende organisaties zijn die dit werk uit handen nemen en waar de organisatie zich bij kan aansluiten. Dit kan voor eenieder binnen de supply chain gunstig zijn. Naast certificering speelt ook internationale standaardisatie en normalisatie een belangrijke rol bij de inschatting van de mogelijke compliancerisico's binnen de supply chain. Alom bekend is de ISO (International Standardization Organization) norm 9001 inzake kwaliteitsmanagement of ISO 14001 milieumanagementsysteem waaraan certificering gekoppeld is, zodat de organisatie weet aan welke vereisten de interne systemen van de toeleverancier voldoen.

In 2012 heeft de Australische Normalisatiecommissie een voorstel gemaakt voor een internationale standaardnorm op het gebied van compliance. Volgens een vast patroon zijn er vervolgens nationale normalisatiecommissies aangehaakt om te komen tot een internationale norm. Zo ook de NEN (Nederlandse Norm). De NEN-commissie inzake ISO 19600 heeft zich hard gemaakt om ISO 19600 niet tot vaststaande 'norm' te verheffen met daarbij behorende certificering. Dit zou immers een ongelijk speelveld zijn voor organisaties. De compliancestructuur kan niet in de vorm van 'one size fits all' worden aanvaard. Compliance is maatwerk en moet passen binnen de organisatie, anders schiet het zijn doel voorbij. Tevens zou het betekenen dat MKB-bedrijven niet door de certificering heen zouden kunnen komen, omdat het optuigen van een grote kerstboom niet past binnen het MKB. Het verzet van Nederland heeft ertoe geleid dat in plaats van een norm een richtlijn tot stand is gekomen, waaraan organisaties houvast kunnen ontlenen voor het opzetten van hun compliance. Het doel van ISO 19600 is compliance een onderdeel te maken van de dagelijkse bedrijfsvoering.

Teleurstellend is dat de ISO 19600 Richtlijn niet dieper ingaat op de integriteit van de organisatie. De richtlijn is uitgebreid op het gedeelte van de leidersrol en daarmee de 'tone at the top', maar aan het minimum stelsel voor gedragsnormen wordt verder weinig aandacht besteed. Helemaal gelukkig is de Nederlandse vertegenwoordiging dus niet. Compliance richt zich op het naleven van wet- en regelgeving alsmede *interne normen.* Naleven vereist een bepaald *gedrag.* Ondanks verwoede pogingen van de Nederlandse delegatie is er toch te weinig aandacht in de richtlijn voor integriteit en cultuur. Compliance is slechts mogelijk als er een juiste culturele voedingsbodem is die past bij de organisatie en compliance verder tot bloeien brengt.

## 8.5. Conclusie

De afgelopen jaren is het duidelijk geworden dat er duidelijk verandering komt in de rol van de commissarissen voor wat betreft het toezicht op compliance en

integriteit binnen de organisatie. Dat de leden van de RvB direct verantwoordelijk zijn voor hun eigen gedrag is een feit, maar steeds vaker worden zij als eindverantwoordelijken aansprakelijk gesteld voor ernstige compliance- en integriteitsincidenten binnen de organisatie.

Het is zaak dat de RvB en de RvC zich steeds meer bewust worden van het belang van compliance en integriteitsmanagement binnen hun organisatie. De daaraan gekoppelde risico's zijn van dien aard dat ze van directe invloed zijn op de 'license to operate'.

Willen de RvB en de RvC zicht hebben op de compliance- en integriteitsrisico's, dan zullen ze compliance en integriteit een duidelijke positie moeten geven binnen de organisatie. Let wel! Compliance is maatwerk. Met copy paste komt de organisatie bedrogen uit, want dan is het een dode letter én dat is op zichzelf reeds weer een risico erbij. Vervolgens zullen ze regelmatig met compliance om de tafel moeten zitten om de discussie aan te gaan en bijtijds risico's te kunnen bijsturen. Ook moet de deur van de RvB en de RvC openstaan voor de compliance officer. Daarbij moet dan wel aangetekend worden dat er verhoogde vereisten gesteld worden aan de deskundigheid en integriteit van de compliance officer, omdat hij of zij invloed uitoefent op het hoogste governanceniveau. Kortom: nog volop werk in uitvoering!