# 4 Compliance risicomanagement: een holistische benadering

*Robert van Altena*

## 1. Introductie

Compliance risicomanagement heeft tegenwoordig de volle aandacht van veel bestuurders en commissarissen. Voor financiële instellingen vloeit deze aandacht voort uit het streven naar herstel van vertrouwen en de bijbehorende nationale en internationale regels en codes met hun nadruk op risicomanagement. Risicomanagement dat zich richt op zowel continuïteit van de financiële instelling als op de zorgplicht jegens de klant. Voor veel bestuurders van corporates (non-financiële ondernemingen) staat compliance risicomanagement op de agenda vanwege ontwikkelingen in regelgeving, zoals de zeer onlangs van kracht geworden UK Bribery Act, of het geconfronteerd worden met impactvolle incidenten op gebied van compliance. Incidenten die zich met name lijken af te spelen in de sfeer van regels die door overheden worden gesteld ten aanzien van het exporteren en doorleveren van goederen (export controls), zaken doen in en met internationaal geboycotte landen en regels op gebied van corruptie en omkoping. De pijn voor organisaties ligt naast reputatieverlies daarbij met name in de zeer strenge sancties en boetes die staan op schending van deze regels. Op onderdelen is er zelfs pijn voor de individuele bestuurders in de vorm van persoonlijke aansprakelijk te worden gesteld.

In deze bijdrage aan het boek wordt compliance risicomanagement beschreven vanuit de optiek van de bestuurskamer, toegespitst op de rol van commissarissen en de hun omringde staffunctionarissen zoals de compliance officer. De rol van commissarissen wordt beschreven vanuit een two tier omgeving, maar is ceteris paribus ook van toepassing in een one tier omgeving bij de invulling van de rol van algemeen bestuurder (non-executive). Waar in de rest van de tekst wordt gesproken van bestuur wordt dan ook het dagelijkse uitvoerende bestuur bedoeld.

In dit hoofdstuk wordt allereerst ingegaan op compliance risicomanagement met een korte introductie van risicomanagement vanuit een breder perspectief. Dit geschiedt aan de hand van het COSO-ERM framework. In de tweede paragraaf wordt een holistische benadering van compliance risicomanagement beschreven in de vorm van een GRC-framework. In de derde paragraaf wordt vervolgens ingegaan op praktische deelaspecten van compliance risicomanagement.

## 2. Compliance risicomanagement

Om tot denken in termen van compliance risicomanagement te komen dient er een aantal denkstappen te worden gezet.

De eerste denkstap behelst de bereidheid om te kijken naar compliance in ruime zin. Compliance in ruime zin betekent voldoen aan zowel de voorschriften (*rules*) van de wet- en regelgeving als de geest (*principles*) met zicht op de achterliggende maatschappelijke open normen. Waarbij zowel huidige als toekomstige normen een rol spelen. Compliance in ruime zin behelst ook voldoen aan al hetgeen de organisatie met zijn stakeholders afspreekt, al of niet uit vrije wil. Denk hierbij aan gedragscodes en andere uitingen, bijvoorbeeld op het gebied van maatschappelijk verantwoord ondernemen.

De tweede denkstap behelst het denken aan compliance in termen van risico, waarbij het oogmerk is om de schaarse middelen van de organisatie zo optimaal mogelijk in te zetten.

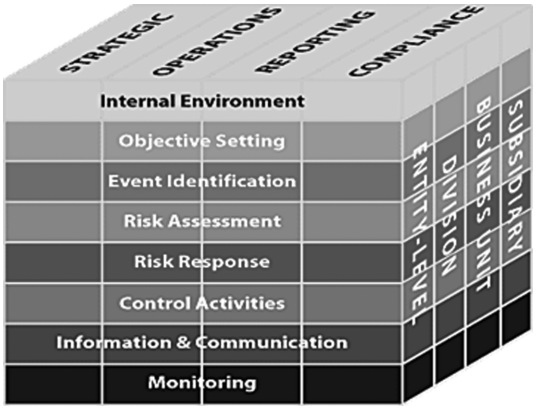
Beide denkstappen komen uitstekend tot uitdrukking in de definitie van compliance risico zoals die wordt gehanteerd door het Basel Committee on Banking Supervision:

> *"Compliance risk is defined as the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a financial institute may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct applicable to its activities."*

De voorafgaande definitie kan door commissarissen uitstekend praktisch worden gebruikt als kapstok voor de vragen die kunnen worden gesteld in het kader van het uitoefenen van toezicht op de manier waarop het bestuur invulling geeft aan compliance risicomanagement. Denk daarbij aan vragen zoals: Welke sancties zouden door overheid, (externe) toezichthouders of contractpartijen kunnen worden uitgevaardigd? Wat beschouwt het bestuur als een materieel verlies? Wellicht interessanter geformuleerd: Welke financiële verliezen uit hoofde van compliance overtredingen kan de onderneming dragen of acht het bestuur acceptabel? Hoe mitigeren we mogelijke reputatieschade? Hoe blijft het bestuur van de organisatie op de hoogte van alle relevante wetten, regels en vrijwillige standaarden? Met name die toekomstige regels met grote impact op strategie of onderdelen van het bedrijfsmodel. Hoe gaan we om met de eigen gedragscode? Zijn er bedrijfsactiviteiten die een verhoogd risico lopen?

Hoe kan het compliance risico door de onderneming worden gemanaged? Daarvoor kan een beroep worden gedaan op een risicomanagement framework, zoals het Enterprise Risk Management – Integrated Framework van de Committee of Sponsoring Organisations of the Threadway Commission (COSO). Dit framework wordt in toelichtingen bij codes als de Nederlandse Corporate Governance Code en wetten als de US Sarbanes-Oxley Act met name genoemd als zijnde een algemeen acceptabel te achten risicomanagement framework.

Het COSO ERM-Integrated Framework kent vier doelen en acht bouwstenen. De doelen en bouwstenen vormen samen met de dimensies voor de verschillende lagen van de organisatie (van de organisatie als geconsolideerd geheel tot een individuele groepsmaatschappij) een stelsel dat grafisch vaak als een kubus wordt weergegeven.




De vier doelen van risicomanagement zijn:

- Strategisch: behalen van ondernemingsdoelstellingen;
- Operationeel: effectiviteit en efficiency van bedrijfsprocessen;
- Verantwoorden: betrouwbaarheid van de externe en interne verantwoordingen; en
- Compliance: naleving van geldende wet- en regelgeving.

De acht bouwstenen van risicomanagement zijn:

- Interne omgeving: De interne omgeving betreft de cultuur van de organisatie en daarin komen aspecten als normen en waarden, omgangsvormen, groepsdynamiek (‘tone at the top’) en risicobereidheid tot uitdrukking.
- Formuleren van doelstellingen: Doelstellingen op gebied van strategie, effectiviteit en efficiency van de bedrijfsvoering (innovatief vermogen, klanttevredenheid, procesoptimalisering etc.), verantwoording (zowel financieel als non-financieel) en compliance. Doelstellingen gekoppeld aan relevante kwantificering: hoeveel rendement wordt verlangd en hoeveel (kapitaal)risico’s is de organisatie bereid te lopen?
- Identificeren van gebeurtenissen: Interne en externe gebeurtenissen die invloed hebben op het behalen van de doelstellingen van de ondernemingen worden geïdentificeerd, daarbij rekeninghoudend met kans en impact op geformuleerde doelstellingen. Hierbij staan in de praktische uitvoering aspecten centraal als: mogelijke

externe of interne bronnen, volledigheid daarvan, manier van identificeren (self assessment door medewerkers in groepssessies met behulp van stemkastjes etc.), analyse van historische data, beschouwen van interdependentie tussen gebeurtenissen en opstellen van mogelijke scenario's op basis van historische gegevens.
- Risicobeoordeling: Risico s worden geanalyseerd, rekening houdend met hun waarschijnlijkheid en impact ter bepaling van het inherente risico (bruto risico) en het restrisico (netto risico) na inachtneming van de getroffen beheersmaatregelen.
- Reactie op risico: De organisatie kan vier risicostrategieën invullen: risico's vermijden, accepteren, verminderen of delen met derden. De organisatie formuleert hiervoor bewust beleid. In de reactie wordt rekening gehouden met de tevoren vastgestelde risicotoleranties.
- Beheersingsactiviteiten: Risicomanagement komt tot uitdrukking in beheersmaatregelen, onder andere in de vorm van functiescheidingen, analyses door het management, richtlijnen en procedures en maatregelen in de informatie- en communicatiesystemen.
- Informatie en Communicatie: Relevante informatie over het risicomanagement van de organisatie wordt verzameld en gecommuniceerd op een manier die medewerkers in staat stelt hun verantwoordelijkheden in te vullen.
- Monitoren: Het systeem van risicomanagement wordt bewaakt door voortdurende managementactiviteiten (*ongoing monitoring*) en door afzonderlijke evaluaties (*fresh look*) door stafmedewerkers, zoals compliance officers en risicomanagers. Let wel: monitoren vindt plaats binnen het systeem; het toetsen en eventueel ter discussie stellen van de invulling van het gehele risicomanagement systeem, of onderdelen daarvan, vindt plaats door onafhankelijke spelers, zoals interne accountants. Auditen is derhalve geen bouwsteen van een risicomanagement framework zelf.

Vaak vormt de zogenaamde 'in-control verklaring' door de voor risicomanagement verantwoordelijke bestuurders een sluitstuk van het risicomanagement en een middel om stakeholders te informeren over de kwaliteit van het risicomanagement en een positieve bewering te doen over de opzet, bestaan en werking van het systeem van risicomanagement. Let wel: in control verklaringen worden niet gegeven door commissarissen, aangezien zij geen verantwoordelijkheid dragen voor de operationele invulling van het risicomanagement framework.

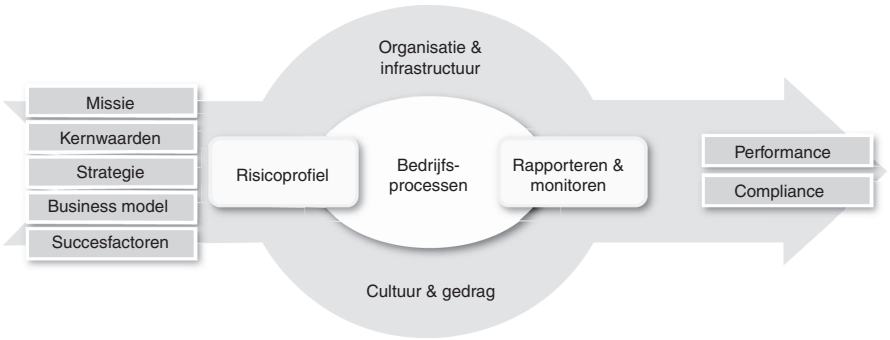
Kritiek van velen op een systeem van risicomanagement in de vorm van het COSO-ERM Integrated Framework is dat de bouwstenen en de invulling van de maatregelen en procedures binnen de bouwstenen erg technisch van karakter zijn en niet aansluiten bij het instrumentarium van ondernemers en business managers. Het begrijpen en beïnvloeden van de individuele bouwstenen en het risicomanagement als geheel lijkt dan met name voorbehouden aan spelers als risicomanagers en interne accountants. Voor bestuurders van ondernemingen en commissarissen vormt dit, nogal zwak uitgedrukt, een grote uitdaging. In de praktijk zien we dan ook dat bestuurders en commissarissen er bij gebaat zijn om risicomanagement te benaderen vanuit een meer op de bedrijfsvoering, managementcyclus en beleving van generalisten gerichte holistische benadering van risicomanagement. In de volgende paragraaf wordt een dergelijke benadering nader beschreven.

## 3. Holistische benadering van Governance, Risico en Compliance

Door velen wordt een risicomanagementsysteem ingericht op basis van de COSO-bouwstenen als te theoretisch en zeer bewerkelijk ervaren, zoals hiervoor al werd aangeven. In de praktijk kunnen we dan ook waarnemen dat risicomanagement op een meer holistische wijze wordt benaderd en dat daarbij veelal gebruik wordt gemaakt van de totaalaanduiding Governance, Risico en Compliance (GRC). Het bijkomende voordeel van deze benadering is dat er meer nadrukkelijke aandacht is voor compliance in wisselwerking met ondernemingsbreed risicomanagement. Voor commissarissen en bestuurders is een bijkomend voordeel van GRC dat Governance ook uitgebreid aan de orde komt in termen die bestuurders en commissarissen vertrouwd is en aansluit bij het gedachtegoed van corporate governance codes.

Holisme betekent volgens het woordenboek Van Dale: de opvatting dat er een samenhang bestaat in de werkelijkheid die enkel uit een beschouwing in het geheel blijkt en niet terug te vinden is in de onderdelen. Het beschouwen van de organisatie vanuit samenhang en als geheel sluit goed aan bij de toezichthoudende rol van commissarissen.

In de onderstaande wordt in één beeld een schets getoond van een mogelijke invulling van een holistische benadering van risicomanagement op basis van GRC.




Bron: GRC-Framework KPMG (interpretatie van auteur)

Een holistische benadering sluit aan op de manier waarop vanuit de bestuurskamer wordt gekeken naar de organisatie en de manier waarop de organisatie haar (compliance)risico's beheerst. Een manier van benaderen die zeer geschikt is voor interne toezichthouders, zoals commissarissen, die zich op zekere afstand bevinden van de dagelijkse bedrijfsvoering en wel de rol hebben om toe te zien of de belangen van de organisatie worden gediend door het handelen van de bestuurders. Op een manier die recht doet aan de strategische en operationele managementcyclus van de organisatie.

Een holistische benadering, zoals tot uitdrukking gebracht in voorafgaande afbeelding, maakt ook duidelijk dat het heel belangrijk is om de besturing in te richten door te starten bij de missie en van daaruit de verschillende stappen te doorlopen en niet te zwichten voor de verleiding om te starten aan de 'achterkant' en dan gefragmenteerd terug te grijpen op onderdelen van de cyclus. Dit kan vaak worden waargenomen bij organisaties die onder toezicht zijn gesteld van externe toezichthouders (bijvoorbeeld DNB en AFM voor wat betreft financiële instellingen). Dit uit zich dan in het accent leggen op het reageren op nieuwe compliance leidraden, controleprotocollen, individuele aanwijzingen en onderzoeksbevindingen van de externe toezichthouder. Hierdoor lopen de bestuurders het risico om daarin geheel mee te gaan en zelf ook met name het accent te gaan leggen op rapporteren en monitoren: en zo wellicht nooit tot de werkelijk verklarende organisatorische elementen door te dringen.

In de volgende alinea's worden enkele elementen van een GRC-Framework nader toegelicht. Waarbij we ons richten op een benadering die de verbinding tussen GRC en compliance risicomanagent door commissarissen duidelijk maakt.

### *3.1 Kernwaarden*

De kernwaarden vormen letterlijk en figuurlijk de kern voor het handelen van de bestuurders en medewerkers van de organisatie. De organisatie betrekt haar kernwaarden op de hele keten van haar bedrijfsvoering, dus ook op leveranciers en andere business partners. De kernwaarden worden met name expliciet uitgedrukt door middel van de gedragsode van de organisatie. Van de organisatie mag verwacht worden dat zij zal trachten daadwerkelijk compliant te zijn met haar eigen kernwaarden en een vorm van handhaving in te richten. De kernwaarden zullen in de pas lopen met maatschappelijk acceptabel geachte waarden, zoals die ook in wetten, regels en codes verankerd zijn. Commissarissen dienen zich met het proces van totstandkomen en bewaken van kernwaarden heel nadrukkelijk bezig te houden, vanwege het grote belang daarvan voor het functioneren van de organisatie. En dit ook extern te uiten, bijvoorbeeld door de gedragscode ook expliciet te bekrachtigen, bijvoorbeeld door ondertekening, en uit te dragen.

### *3.2 Strategie*

Bij het bepalen en het formuleren van een strategie maakt de organisatie keuzen over haar toekomst. In de theorie worden, onder andere door Keuning en Eppink, drie strategische hoofdvragen onderscheiden: Hoe positioneren wij ons in de markt en hoe onderscheiden wij ons ten opzichte van de andere partijen in de markt? (positioneringsstrategie), In welke mate zal de organisatie zich differentiëren of juist specialiseren? (differentiatiestrategie), en Hoe gaan wij de strategie in de praktijk brengen? (uitvoeringsstrategie). Compliance speelt in de beantwoording van al de drie strategievragen een grote rol. Voor positioneringkeuzen is compliance van groot

belang. De organisatie moet in staat kunnen zijn te voldoen aan de eisen die worden gesteld aan markttoegang (denk bijvoorbeeld aan een grote corporate die de treasury functie verzelfstandigt en bancaire activiteiten ontplooit en daarvoor een vergunning dient te verkrijgen) en marktcontinuïteit (denk hiervoor bijvoorbeeld aan de gloeilampenfabriek die te maken krijgt met een overheid die de productie van gloeilampen verbiedt). De organisatie moet tevens in continuïteit kunnen voldoen aan de eisen die worden gesteld aan het gedrag van de organisatie en haar medewerkers in de markt (bijvoorbeeld in het voorkomen van verstrengeling van de belangen van de organisatie en haar individuele medewerkers met de belangen van klanten).

Voor wat betreft differentiatiekeuzen zal de vraag opkomen of een organisatie door compliant te zijn met haar eigen kernwaarden en externe regels zich positief kan onderscheiden van de concurrentie. Een voorbeeld hiervan is momenteel zichtbaar in het gedrag van Nederlandse verzekeraars na het collectieve echec in verband met de in het verleden verkochte beleggingsverzekeringen, die inmiddels door het leven gaan als woekerpolissen. De individuele verzekeraars proberen zich positief te onderscheiden door expliciet compliant te zijn met de eigen kernwaarden en dat streven en de kernwaarden zelf nadrukkelijk te communiceren met de klanten.

In de uitvoeringskeuzen van de strategie speelt compliance ook een grote rol. Bijvoorbeeld door het beantwoorden van de vraag: Welke eisen stellen wij aan onze business partners? Dit geldt van verzekeraars in de relatie met tussenpersonen tot een multinational in relatie tot zijn lokale agent in het Midden-Oosten. Strategiebepaling is uiteraard een belangrijk toezichtdomein voor commissarissen en dit geldt ook de compliance elementen daarvan.

### *3.3 Succesfactoren*

De term succesfactoren in de zin van kritische succesfactoren (KSF) is met name bekend geworden door de theorieën ontwikkeld in de jaren zeventig door denkers als Rockart, Kaplan en Norton. Kritische succesfactoren betreffen dan de factoren die doorslaggevend zijn voor het succes of falen van een organisatie. Deze factoren vormen de belangrijkste onderdelen voor het management informatiesysteem en komen mede tot uitdrukking in instrumenten zoals de Balanced Scorecard. De vier domeinen van de Balanced Scorecard (klantperspectief, innovatieperspectief, financieel perspectief en de bedrijfsprocessen) kennen een zeer grote wisselwerking met compliance. Compliance in de vorm van voldoen aan de kernwaarden (gedragscode) van de organisatie en voldoen aan geldende wetten en regels, inclusief zelfregulering, is een belangrijke ingangsvariabele voor de vier domeinen. Andersom zal de manier waarop de Balanced Scorecard wordt ingevuld, bepalen hoe de organisatie wordt blootgesteld aan de kansen en beperkingen die compliance met zich brengt. Sommige theoretici stellen overigens dat een organisatie over het algemeen maximaal acht echt cruciale succesfactoren zal hebben. Het is zaak voor de commissarissen om voor deze acht cruciale succesfactoren te onderkennen wat de wisselwerking is met compliance.

### *3.4 Risicoprofiel*

Het vaststellen van het risicoprofiel geschiedt ex ante en wordt gedaan door de bestuurders met input en toetsing door commissarissen. In sommige gevallen zullen de commissarissen ook formeel het mandaat hebben om het risicoprofiel ex ante vast te stellen. In het vaststellen staan eigenlijk vier vragen centraal:

– Welke risico's zijn wij bereid te lopen?
– Hoeveel rendement verlangen wij?
– Welke (gekwantificeerde) risicotoleranties zijn wij bereid te hanteren?
– Hoe alloceren wij de risico's (en benodigde kapitalen) naar de activiteiten en bedrijfsonderdelen?

Om deze vragen te kunnen beantwoorden zullen bestuurders en commissarissen gezamenlijk zicht dienen te krijgen op de kansen en gevolgen die onzekere gebeurtenissen zullen kunnen hebben op de risico's die de organisatie loopt. Tevens zal daarbij worden nagedacht over de risicostrategieën die de organisatie wenst in te zetten. Ruwweg bestaan er, zoals hierboven al aangestipt, vier risicostrategieën: accepteren (financiële buffers creëren om de pijn te kunnen dragen), reduceren (versterken van de organisatie en beheersingsmaatregelen), overdragen (verzekeren, allianties aangaan met andere marktpartijen) of beëindigen (terugtrekken van de markt, desinvesteren). Het onderkennen van de gebeurtenissen uit hoofde van veranderingen in compliance, zoals op komst zijnde wetswijzigingen en een veranderend beroep van het maatschappelijk verkeer op de kernwaarden van de organisatie, zijn over het algemeen erg impactvol en vormen derhalve een belangrijke bron voor risico's. Kenmerk van deze wijzigingen van compliance is wel dat de kans over het algemeen goed lijkt in te schatten, zolang de organisatie maar op de hoogte is van de actuele ontwikkelingen in wet- en regelgeving en een goede antenne heeft voor maatschappelijke ontwikkelingen. Heel anders is dat voor incidenten op gebied van compliance. Compliance incidenten kunnen impactvol zijn en hebben een slechtere kansvoorspelbaarheid. Verderop in dit hoofdstuk komen we nog terug op de praktische invulling die hieraan kan worden gegeven, zowel voor wat betreft het handelen van bestuurders en commissarissen als de rol van de stafmedewerker betrokken bij compliance (compliance officer).

### *3.5 Organisatie en infrastructuur*

De taken, bevoegdheden en verantwoordelijkheden van commissarissen met betrekking tot compliance en risicomanagement zijn, naast statutaire bepalingen, formeel vastgelegd in wetten, regels en codes. Daarnaast is het van grote waarde om enkele good-practices te beschouwen.

### *3.5.1 Formele eisen aan commissarissen*

Toegespitst op de Nederlandse situatie is het zinvol om de Nederlandse Corporate Governance Code (de Code) en de Bankencode aan de orde te stellen. Bedenk dat de Nederlandse Corporate Governance Code uitsluitend van toepassing is op beursgenoteerde ondernemingen (en voor wat betreft de bepalingen aangaande de auditcommissie indirect via de wet ook op zogenaamde niet-beursgenoteerde Organisaties van Openbaar Belang (OOB's), zoals banken en verzekeraars) en dat de Bankencode uitsluitend van toepassing is op banken. Desondanks is kennisnemen hiervan voor elke commissaris verstandig.

De Nederlandse Corporate Governance Code kent twee bepalingen waarin compliance risicomanagement met name aan de orde komt. Ten eerste bepaalt de Code dat de raad van commissarissen in ieder geval eenmaal per jaar de strategie en de voornaamste risico's verbonden aan de onderneming, de uitkomsten van de beoordeling door het bestuur van de opzet en werking van de interne risicobeheersings- en controlesystemen, alsmede eventuele significante wijzigingen hierin, bespreekt. Van het houden van de besprekingen wordt melding gemaakt in het verslag van de raad van commissarissen. Ten tweede bepaalt de Code dat de auditcommissie zich in ieder geval richt op het toezicht op het bestuur ten aanzien van de werking van de interne risicobeheersings- en controle-systemen, waaronder het toezicht op de naleving van de relevante wet- en regelgeving en het toezicht op de werking van gedragscodes.

De Bankencode kent drie domeinen die in het kader van compliance risicomanagement van belang zijn: het centraal stellen van de klant, de moreel-ethische verklaring en de rol van commissarissen met betrekking tot het algehele risicobeleid van de bank . Overigens is het ook heel interessant dat de code een bepaling over educatie kent die nadrukkelijk stelt dat op gebied van compliance educatie voorgeschreven is aangaande zorgplicht jegens de klant en integriteit.

De code stelt dat het centraal stellen van de klant een noodzakelijke voorwaarde is voor de continuïteit van de bank en dat de raad van bestuur er voor zorgt dat de bank haar klanten te allen tijde zorgvuldig behandelt. De raad van bestuur dient er zorg voor te dragen dat de zorgplicht jegens de klant wordt verankerd in de cultuur van de bank.

De code stelt dat leden van de raad van bestuur hun functie uitoefenen op een zorgvuldige, deskundige en integere manier met inachtneming van de van toepassing zijnde wet- en regelgeving, codes en reglementen. Ieder lid van de raad van bestuur tekent een moreel-ethische verklaring, waarvoor de code een model-verklaring bevat. Dit model kan iedere bank naar eigen inzicht aanvullen. De raad van bestuur draagt er zorg voor dat de bedoelde verklaring wordt vertaald in principes die gelden als leidraad voor het handelen van alle medewerkers van de bank.

De code stelt dat bestuurders verantwoordelijk zijn voor het vaststellen, uitvoeren, monitoren en waar nodig bijstellen van het algehele risicobeleid van de bank. De risicobereidheid wordt op voorstel van de raad van bestuur tenminste jaarlijks ter goedkeuring aan de raad van commissarissen voorgelegd. Tussentijdse materiële wijzigingen van de risicobereidheid worden eveneens ter goedkeuring aan de raad van commissarissen voorgelegd. De raad van commissarissen houdt toezicht op het door de raad van bestuur gevoerde risicobeleid. Daartoe bespreekt de raad van commissarissen het risicoprofiel van de bank en beoordeelt hij op strategisch niveau of kapitaalallocatie en liquiditeitsbeslag in algemene zin in overeenstemming zijn met de goedgekeurde risicobereidheid. Bij de uitoefening van deze toezichtrol wordt de raad van commissarissen geadviseerd door de risicocommissie die hiertoe uit de raad van commissarissen is gevormd. De raad van commissarissen beoordeelt periodiek op strategisch niveau of de bedrijfsactiviteiten in algemene zin passen binnen de risicobereidheid van de bank. De voor deze beoordeling relevante informatie wordt op zodanige wijze door de raad van bestuur aan de raad van commissarissen verstrekt dat deze laatste in staat is zich daar een gedegen oordeel over te vormen.

De code stelt dat iedere bank een Product Goedkeuringsproces heeft. De raad van bestuur draagt zorg voor de inrichting van het Product Goedkeuringsproces en is verantwoordelijk voor het adequaat functioneren daarvan. Producten die het Product Goedkeuringsproces binnen de bank doorlopen worden niet op de markt gebracht of gedistribueerd zonder een zorgvuldige afweging van de risico's door de risicomanagementfunctie binnen de bank en zorgvuldige toetsing van andere relevante aspecten, waaronder de zorgplicht jegens de klant. De interne auditfunctie controleert op basis van een jaarlijkse risico-analyse of opzet, bestaan en werking van het proces effectief zijn en informeert de raad van bestuur en de desbetreffende (risico)commissie van de raad van commissarissen omtrent de uitkomsten hiervan.

Tussen de interne auditfunctie, de externe accountant en de risico- of auditcommissie van de raad van commissarissen vindt periodiek informatie-uitwisseling plaats. In het kader van deze informatie uitwisseling is ook de risicoanalyse en het auditplan van de interne auditfunctie en van de externe accountant onderwerp van overleg.

### *3.5.2 Board effectiveness*

Board effectiveness ten aanzien van risk en compliance is een onderdeel van een GRC-framework en krijgt tegenwoordig zelfs nadrukkelijk de aandacht van externe toezichthouders en wordt daarmee ook als compliance aspect gepositioneerd. De Board is effectief als zij belangen van de organisatie en stakeholders adequaat dient op basis van een evenwichtig en consistent besluitvormingsproces , zowel voor de korte als de lange termijn

Effectiviteit wordt bepaald door organisatorische elementen, zoals structuur (taken, bevoegdheden), competentie (deskundigheid, vaardigheid, attitude en

onafhankelijkheid) en risk management (risk en control frameworks, wisselwerking met lijnonfhankelijke functionarissen', externe accountant)

Effectiviteit wordt tevens, en niet in het minst, bepaald door de groepsdynamiek binnen en tussen de Raad van Bestuur en Raad van Commissarissen en het handelen van de individuele leden daarbinnen. De interactie met stakeholders is hierbij ook van belang; 'van interactie met aandeelhouders of bestuursleden van de coöperatieve vereniging tot interactie met de externe toezichthouders'.

De effectiviteit wordt gediend door periodiek board evaluaties. Naast interne zelf-evaluatie, zal evaluatie op basis van een 'fresh look met vreemde ogen' door een externe autoriteit zoals DNB een krachtig instrument kunnen zijn.

Waaraan voldoet een goede evaluatie van Board effectiveness?

- De gehanteerde criteria en evaluatie methodiek worden gedragen door de betrokken bestuurders en commissarissen en doen recht aan de natuurlijke interactie tussen bestuurders en commissarissen;
- De evaluatie is geloofwaardig voor de stakeholders van de organisatie, zowel in wezen als schijn;
- De criteria zijn gebaseerd op algemeen geaccepteerde relevante good (c.q. best) practices, zoals die blijken uit codes; en
- De bevindingen uit de evaluatie kennen een deugdelijke grondslag en zijn aantoonbaar en reproduceerbaar.

### *3.5.3 Vastleggen taken en verantwoordelijkheden*

Verderop in deze bijdrage wordt nader ingegaan op de praktische invulling van de taken van commissarissen en de bijbehorende competenties. Verantwoordelijkheden worden met bepaald door algemeen ondernemingsrecht, statuten, governance codes en specifieke regels, meestal branchegericht. Een binnen een GRC-framwork en daarmee in de praktijk vaak gehanteerd instrument is de zogenaamde RACI-methode. De RACI methode maakt per categorie van bedrijfsbeslissingen (eventueel verbijzonderd naar individuele bedrijfsprocessen) duidelijk wie *Responsible*, *Accountable*, *Consulted* en *Informed* wordt. Waarbij conventies worden gehanteerd zoals bijvoorbeeld ten aanzien van Responsible dat er slechts één functionaris echt Responsible is. De nadruk ligt daarbij dan op de verantwoordelijkheid om beslissingen te initiëren en in te brengen in een bestuur dat in collectiviteit *Accountable* is.

### *3.5.4. Infrastructuur*

De infrastructuur voor compliance risicomanagement gaat het met name over instrumenten op het terrein van informatie, communicatie en technologie die de gehele GRC-cyclus kunnen ondersteunen of delen ervan. In praktijk komen we op dit terrein zowel systemen tegen met een integraal karakter, zogenaamde Enterprise Resource

Planning systemen, als systemen die meer gericht zijn op procesbeschrijvingen en/ of vastleggen van waarnemingen en incidenten. Laatstgenoemde systemen hebben veelal een workflow management karakter. Belangrijk is dat commissarissen zich realiseren op welke onderdelen van de GRC-cyclus de systemen ondersteuning bieden en misschien belangrijker op welke onderdelen niet. De ervaring leert dat de meer strategische aspecten van (compliance) risicomanagement zich nauwelijks laten vangen door geautomatiseerde systemen.

### *3.6 Cultuur en gedrag*

Cultuur en gedrag vormen de basis voor risicomanagement. In de gestileerde weergave van een GRC-framework worden cultuur en gedrag ook vaak letterlijk als basis opgenomen. In cultuur en gedrag komen de kernwaarden van de organisatie tot uitdrukking, zoals die veelal expliciet zijn gevat in de gedragsode van de organisatie. Van bestuurders en commissarissen mag verwacht worden dat zij zich zeer bewust zijn van het belang van cultuur en gedrag voor het risicomanagement en de beheersing van de organisatie. In de praktijk zijn er diverse manieren om cultuur en gedrag bewust mee te nemen in het managen van de risico's, variërend van doorlopen van cultuurprogramma's tot het inrichten en toetsen van zogenaamde soft controls, beheersingsinstrumenten die gebruiken maken van het gedrag van mensen.

### *3.7 Bedrijfsprocessen inrichten aan de van compliancethema's*

De kern van compliance risicomanagement betreft de vertaling ervan naar de daadwerkelijke bedrijfsprocessen op zo'n manier dat de spelers op de werkvloer in staat zijn compliance als onderdeel te zien van hun dagelijkse werkzaamheden en in staat worden gesteld instrumenten te gebruiken die deze risico's ondervangen.

In de praktijk komen we een paar aspecten tegen die vermeldenswaard zijn:

- Inrichting van compliance in de bedrijfsprocessen aan de hand van compliancethema's, zoals bijvoorbeeld consumentenbescherming, privacy, veiligheid. De compliancethema's bevatten per thema een set van normen die zijn afgeleid uit de relevante regels. Voordeel van deze werkwijze is dat de spelers op de werkvloer zelf niet geconfronteerd worden met gedetailleerde wetsbepalingen en regels, maar er (veelal op stafmatig centraal niveau) binnen de organisatie al een vertaalslag heeft plaatsgevonden.
- De compliancethema's worden vertaald naar controlehandelingen, die onderdeel worden van de gehele set van controlehandelingen die op de werkvloer plaatsvinden. Zo worden controlehandelingen met betrekking tot compliance gecombineerd met die voor financiële verslaggeving (boekhouden) en operationele beheersing (klantacceptatie etc.). In de theorie van accountants valt vaak de term 'key controls' waarmee wordt bedoeld een set van controlehandelingen die doorslaggevend zijn voor het geheel van beheersing en veelal een gecombineerd karakter hebben.

### *3.8 Rapporteren en monitoren*

Een slotstuk van een GRC-cyclus wordt gevormd door rapporteren en monitoren. Voor rapportering is het van groot belang dat alle stappen van GRC worden afgedekt; van vertaling van strategie naar risicoprofiel tot werking van de controlehandelingen op basis van compliancethema's in de bedrijfsprocessen. In de praktijk komen we hier zogenaamde non-financial risk en/of compliance dashboards tegen. De rapportering is verbonden met monitoringswerkzaamheden. In heel praktisch Nederlands betreft monitoren het vinger aan de pols houden van de werking van risicomanagement en GRC als geheel. We komen twee vormen van monitoren tegen. Het doorlopend monitoren dat in de bedrijfsprocessen zelf geschiedt door de medewerkers van de organisatie en de business managers ('ongoing monitoring') en het monitoren door stafmedewerkers zoals compliance officers en risicomanagers ('fresh look monitoring') op basis van deelwaarneming gericht op signaleren van probleemgebieden, geven van feed back en advies aan de medewerkers van de organisatie die als 'eigenaren' van de bedrijfsprocessen worden beschouwd. Een commissaris zal in het kader van zijn toezicht op GRC en risicomanagement kennisnemen van de rapportages en de uitkomsten van 'fresh look monitoring' . Het kennisnemen van de bevindingen van de 'fresh look monitoring' kan onder andere door de daarvoor verantwoordelijke staffunctionaris, zoals een compliance officer, te bevragen.

## 4. Waarnemingen vanuit de praktijk

In het voorafgaande is compliance risicomanagement beschreven aan de hand van de onderdelen van een GRC-framework. In dit onderdeel wordt nader ingegaan op de dagelijkse praktijk teneinde de GRC-benadering geur en kleur te geven. Daarvoor worden twee zaken belicht: enkele compliance good-practices en nadere beschouwing van de mogelijke rol van de compliance officer.

### *4.1 Compliance good-practices voor commissarissen*

"De commissarissen dienen een gepast inzicht te hebben in de typen compliancerisico waaraan de organisatie blootstaat. De commissarissen dienen een redelijke mate van due diligence uit te oefenen zodat de effectiviteit van het complianceprogramma wordt gewaarborgd, door minstens een keer per jaar een rapport te evalueren over de effectiviteit van dit programma. Het niveau van de technische kennis die commissarissen dienen te bezitten om deze verantwoordelijkheden uit te kunnen oefenen kan uiteenlopen, afhankelijk van de specifieke omstandigheden binnen de organisatie." Voorafgaande is een vrije interpretatie van een deel van een toespraak van een vertegenwoordiger van een Amerikaanse toezichthouder.

Om de redelijke mate van due diligence ten aanzien van compliance collectief goed in te vullen, is het belangrijk dat binnen de Raad van Commissarissen de volgende

vaardigheden aanwezig zijn zodat compliance zowel proactief als in het geval van incidenten goed kan worden neergezet:

- Begrijpen wat de potentiële impact van regelgeving is op het bedrijfsmodel en de strategische doelen van de onderneming (zoals eerder in deze bijdrage beschreven aan de hand van de onderdelen van een GRC-cyclus);
- Goed kunnen onderhandelen met en reageren op toezichthoudende autoriteiten, met name in het geval van incidenten;
- Beschikken over communicatievaardigheden zodat men in staat is voldoende informatie te bieden over het complianceniveau van de onderneming en de perceptie hierover te beïnvloeden, zowel wat betreft externe stakeholders zoals investeerders en klanten als interne stakeholders zoals werknemers en gebonden agenten;
- Toegang hebben tot aan compliance gerelateerde technische kennis, zowel intern (bij de functionarissen voor compliance, juridische zaken en risicobeheer en binnen hun organisatie- en gegevensstructuren) als extern (inzicht hebben in de impact van regelgeving op de markten en jurisdicties waar de onderneming actief is), en bekend zijn met 'state-of-the-art' ontwikkelingen omtrent compliancemanagement binnen de peergroup van de onderneming; en
- Zich bewust zijn van de kwaliteit van de organisatie en het risicomanagement van compliance binnen de onderneming.

### *4.2 Rol van de compliance officer*

In het algemeen is de rol van de compliance officer binnen corporate governance niet specifiek beschreven. Sommigen codes stellen dat het gewenst is een dergelijke onafhankelijke functionaris te hebben die de risico's van overtreding van regelgeving stelselmatig monitort. In de praktijk zien we aan aantal best practices met betrekking tot de rol en werkzaamheden van de compliance officer op het vlak van het ondersteunen van de rol van bestuurders en commissarissen.

- Ondersteuning bieden aan bestuurders en commissarissen zodat deze begrijpen wat de potentiële impact van regelgeving is op het bedrijfsmodel en de strategische doelen van de onderneming;
- Goede relaties onderhouden met sleutelspelers binnen toezichthoudende autoriteiten teneinde de directie te kunnen informeren over de 'ongeschreven regels en gevoeligheden' in de omgang met deze autoriteiten, bijvoorbeeld in het geval van incidenten;
- Rapporteren aan de bestuurders en commissarissen teneinde deze in staat te stellen met de interne en externe stakeholders te communiceren over de compliancestatus; zowel doorlopende rapportage gericht op de organisatie als ad-hoc rapportage van potentiële en daadwerkelijke incidenten;
- Toegang bieden tot aan compliance gerelateerde technische kennis inzake de impact van regelgeving op de markten en jurisdicties waar de onderneming actief is, en inzicht bieden in 'state-of-the-art' ontwikkelingen omtrent compliancemanagement binnen de peergroup van de onderneming; en

- Zorgen dat de bestuurders en commissarissen zich bewust worden en blijven van de kwaliteit van het compliancemanagement binnen de onderneming en van hun specifieke rol gezien de impact van de 'toon aan de top'.

We zien steeds vaker dat audit- en/of risico en compliancecommissies van de raad van commissarissen afzonderlijke besloten sessies houden met de compliance officer, hoewel dit nog niet een algemeen aanvaarde praktijk is. Deze sessies vinden plaats na afloop van de periodieke vergaderingen van de betreffende commissie. De bestuurders worden gevraagd de zaal te verlaten en vervolgens verzoeken de leden van de commissie de compliance officer om commentaar te geven op issues en vragen te beantwoorden. Deze werkwijze is al vele jaren heel gangbaar voor wat betreft de relatie met externe en interne auditors.

**Tot slot**

Compliance risicomanagement benaderen als onderdeel van de strategische en operationele managementcyclus van de organisatie helpt bestuurders en commissarissen. Voor de praktische invulling kan daarbij gebruik gemaakt worden van een holistische benadering zoals die in deze bijdrage is uitgewerkt aan de hand van een Governance, Risico en Compliance framework. Een GRC-framework sluit in de regel uitstekend aan op de manier waarop bestuurders en commissarissen kijken naar de organisatie en de manier waarop de organisatie haar (compliance)risico's beheerst. Compliance risicomanagement heeft de bestuurskamer bereikt en de Engelsen zouden daaraan toevoegen 'and is there to stay'.