

Interview: Angelique Keijsers

Leer medewerkers zelf de spiegel oppakken

Compliancethema

Nieuwe governanceregels voor banken en beleggingsondernemingen



GOVERNANCE

Colofon

De Compliance Officer is het vakblad voor compliance officers en andere betrokkenen bij het compliance-proces. De doelgroep bestaat uit compliance officers, bestuurders, toezichthouders, secretarissen van de vennootschap en bedrijfsjuristen die betrokken zijn bij het uitvoeren van compliance-taken.

Redactie:

Sharon Karsten (bureauredactie) en Cora Wielenga (eindredactie)
Tel 088 99 88 100 E-mail:
redactie@complianceofficer.nl

Aan deze editie werken

verder mee: Paolo Bouman, Albert de Jong, Joost Montens, Sharda Poelloe, Björn Schuitemaker, Constant van Tuyl van Serooskerken, Hanne Wanders, Cora Wielenga

Fotografie: Wilco van Dijen

Vormgeving: Tangram Studio

Druk: Platform P, Rotterdam

Uitgever: Nederlands Compliance Instituut, Postbus 5111, Capelle aan den IJssel

Advertenties: Diane Bakker

Tel 088 99 88 100 E-mail:
bakker@compliance-instituut.nl

Nieuwsfeiten, ingezonden artikelen en personeelsmutaties kunt u per e-mail doorgeven aan redactie@complianceofficer.nl.

Het abonnement is gratis voor de doelgroep. Abonnees buiten de doelgroep: € 50 (bij 4 edities).

Oplage 3.400 exemplaren
ISSN 1878-7991

www.complianceofficer.nl



Inhoud

- 3** Van de redactie
- 4** Interview Angelique Keijzers
- 8** **Compliancethema**
Nieuwe governance-regels voor banken en beleggingsondernemingen
- 15** **Compliancecolumn**
Governance or gaffernance
- 16** **Compliancepraktijk**
Ontslag en tuchtrecht banken?
- 20** **Speakers' Corner**
Waar is het touwtje in de compliance toolkit?
- 24** **Compliance-onderzoek**
Onderzoeksresultaten over de inrichting van de compliancefunctie bij Nederlandse financiële ondernemingen
- 28** **Compliancethema**
Het risicoconcept; een inhoudsloze mantra of een pseudoniem voor (meer) onzekerheid?
- 34** **Compliance-agenda**

Vanzelfsprekend



In deze editie van de Compliance Officer staan we stil bij het thema Governance. Dit thema is inmiddels zo vanzelfsprekend voor compliance officers om als onderdeel van hun werk te zien, dat het haast niet meer voor te stellen is dat dit een paar jaar geleden nog niet het geval was. Ik ben zelf in 2004 gestart met het compliancevak. In december 2003 was net de eerste versie van de Nederlandse Corporate Governance Code vastgesteld door de commissie Tabaksblat. Met de komst van die eerste Nederlandse governancecode werd governance een thema voor beursgenoteerde ondernemingen. Het stond daarmee nog niet standaard op de agenda van financiële ondernemingen zonder beursnotering. In de afgelopen jaren is dat veranderd. Ongetwijfeld heeft de crisis daaraan bijgedragen. Verschillende brancheorganisaties kwamen met governancecodes. De Code Pensioenfondsen, de DUFAS Principes van Fondsbestuur, de Code Banken en de Code Verzekeraars kwamen voorbij. Inmiddels zijn veel regels en principes uit deze zelfreguleringen overgenomen in wetgeving. Ook in de ogen van de financieel toezichthouders nam het belang van dit thema toe. Waar het bij toezichthouders eerst nog niet op de agenda stond, zijn er nu expertisecentra ingericht die zich specialiseren in governance en aanverwante thema's. Kortom, het thema governance is nu niet meer weg te denken uit het werkveld van het financieel toezicht en daarmee het werkveld van de compliance officers. In hoeverre helpt een goede governance financiële organisaties eigenlijk? Biedt een goede governance een garantie op geen of weinig misstanden? Was het maar zo eenvoudig. Ik sluit me voor wat betreft governance aan bij de uitspraak die de commissie Halsema heeft gedaan in het rapport 'Een lastig gesprek': *“Een goede structuur en goede regels kunnen slecht gedrag niet voorkomen, maar*

goed gedrag kan wel redding brengen bij een slechte structuur en slechte regels.” We moeten ons dus niet blindstaren op de structuur en regels. Het gedrag wint het van de structuur en regels. Gelukkig wordt gedrag en organisatiecultuur steeds vaker als onderdeel van de governance gezien. Wat mij betreft een verstandig inzicht. Zowel in de laatste versie van de Nederlandse Corporate Governance Code als in de conceptrichtlijnen van de EBA over interne governance wordt expliciet aandacht geschonken aan het belang van organisatiecultuur. Zo wordt op grond van de Nederlandse governancecode van bestuurders en commissarissen verlangd dat zij een cultuur creëren die het gewenste gedrag en integer handelen binnen de onderneming stimuleert. In de EBA-governancerichtlijnen is opgenomen dat het bestuur verantwoordelijk is voor een organisatiecultuur en voor organisatiewaarden die ervoor zorgen dat verantwoordelijk en ethisch gedrag mogelijk is. En daarnaast wordt er gesproken over het instellen van een 'Commissie ethiek, gedrag en compliance' in de raad van commissarissen. Ook in Engelse en Amerikaanse documentatie wordt steeds explicieter stilgestaan bij het belang van organisatiecultuur als onderdeel van de governance. Zo blijkt uit het onderzoeksrapport over Wells Fargo dat de oorzaken van de misstanden niet alleen in de structuur, maar evenzeer in de cultuur worden gevonden.

In mijn werk merk ik dat veel bestuurders, commissarissen en compliance officers het thema 'gedrag en cultuur' nog niet echt oppakken. Het belang ervan wordt onderkend, maar 'ermee aan de slag gaan' is voor veel mensen nog best lastig. Ik zie dat als koudwatervrees. Het is een onderwerp waar je het bijna niet mee oneens kunt zijn. En tegelijkertijd is het enorm spannend om bewust met organisatiecultuur, organisatiewaarden en gedrag aan de slag te gaan. Ik hoop dat we met het thema 'gedrag en cultuur' dezelfde weg bewandelen zoals we dat met governance hebben gedaan. Over een paar jaar zou het dan voor iedereen heel vanzelfsprekend moeten zijn om 'gedrag en cultuur' te integreren in zijn werk. Dan is het actief werken met de organisatiecultuur, het werken met organisatiewaarden en het observeren en interpreteren van gedrag gewoon onderdeel van het standaardpakket aan werkzaamheden van bestuurders, commissarissen en compliance officers.

Cora Wielenga

A close-up portrait of a woman with long, wavy brown hair, smiling warmly. She is wearing a dark blazer over a white top and a delicate necklace with a circular pendant. The background is softly blurred, showing vertical lines of light and shadow.

Angelique Keijsers:

**'Leer medewerkers
zelf de spiegel
oppakken'**

Ook al was ze partner bij EY, toen Rabobank belde, hoefde ze niet lang na te denken. Want werken aan compliance binnen een uitdagend bedrijf, en zelf 'met de voeten in de modder staan', dat is wat *Angelique Keijsers* toch het liefste doet. Per 1 november 2016 trad ze in dienst als chief compliance officer van Rabobank. Na een lange werkdag neemt ze nog uitvoerig de tijd om met Paolo Bouman te praten over wat haar bezighoudt in haar nieuwe functie.

Niet veel mensen zullen een partnership bij een van de 'big four' opgeven voor een volgende stap.

Waarom deed jij dat wel? "Dat heeft met mijn achtergrond te maken. Ik was registeraccount bij PWC en maakte in 2000 de overstap naar ABN AMRO waar ik acht jaar werkzaam was binnen audit en compliance. Dat heb ik altijd heel erg leuk gevonden. Er speelden spannende issues en ik gedij goed onder de druk die daarbij komt kijken. Iets waar mijn analytisch vermogen als voormalig registeraccountant zeer behulpzaam bij was. Toen ik werd gebeld door EY of ik aan hun klanten compliance services zou willen aanbieden, voelde ik een aarzeling. Ik hou er nu eenmaal van om zelf problemen op te lossen. Maar bij ABN AMRO werd een veranderingsproces ingezet toen Fortis, RBS en Santander binnenkwamen en het idee om een eigen afdeling te hebben, en daarmee andere bedrijven te gaan helpen, was heel verleidelijk. Ik vertrok naar EY en had daar acht waanzinnig mooie jaren. Ik deed de meest extreem boeiende onderzoeken, in alle soorten en maten. Van een penningmeester die met de pot geld was vertrokken, tot diepgravende fraudeonderzoeken die de landelijke dagbladen haalden. Daarnaast leverde ik een belangrijke bijdrage aan het opzetten van compliance-beleid bij banken, waaronder Rabobank, maar ook bij niet-financiële instellingen. Toch zag ik me dit – werken vanaf de zijlijn – niet tot mijn pensioen doen. En Rabobank stond op mijn korte lijstje van mogelijke bedrijven waar ik nog wel eens aan de slag zou willen."

En toen belde Rabobank. "Ja, toeval bestaat niet. De timing was perfect, want de reorganisatie bij Rabobank biedt mij ook nog de kans om mede vorm te geven aan de nieuwe organisatie. Ik hoefde niet lang na te denken. Uiteindelijk vind ik met mijn voeten in de modder staan toch het leukst. Niet alleen de vinger op de zere plek leggen, maar ook zelf zorgen dat een organisatie sterker wordt. Ik heb het als consultant wel meegemaakt dat ik

vooral voor window dressing werd binnengehaald, dat in het management nauwelijks commitment bestond voor verbetering van de integriteit. Ik herkende dit soms al na vijf minuten. Dan gaf ik zelf aan dat ik me afvroeg of deze investering in tijd en geld wel de moeite waard was. Daar kon men raar van opkijken. Zo'n uitspraak verwacht je niet van een consultant. Bij Rabobank behoort integriteit tot de kernwaarden en krijg ik alle mogelijkheden daar aan bij te dragen."

Over de reorganisatie. Is Rabobank nog steeds een coöperatie nu alle lokale banken zijn gefuseerd tot één bank?

"Jazeker, want de coöperatieve rechtsvorm is niet veranderd. Sinds 1 januari 2016 is Rabobank één coöperatie van honderddrie lokale banken, met één bankvergunning en één bankbalans. Voorheen waren de leden lid van een lokale bank, nu zijn ze lid van die ene coöperatieve bank. In deze nieuwe structuur is de ledeninvloed versterkt. Elke lokale Rabobank levert namelijk via de voorzitter van de eigen, lokale raad van commissarissen een rechtstreekse vertegenwoordiging namens de leden in het hoogste orgaan van de coöperatie, de Algemene Ledenraad. Deze raad stelt de jaarrekening vast, keurt de jaarlijkse begroting op hoofdlijnen goed, benoemt de leden van de raad van commissarissen en verleent de opdracht aan de externe accountant. Ook heeft de Algemene Ledenraad goedkeuringsrechten voor voorgenomen beslissingen door de raad van bestuur, zoals bij grote overnames of samenwerkingsverbanden. Voor mijn vak speelt, dat het in de oude structuur lastiger was om te kunnen blijven voldoen aan de eisen die voortkomen uit het Europese banktoezicht."

Wat zijn jouw plannen en doelen bij Rabobank?

"Ik wil dat we bij compliance veel meer 'forward looking' worden. We zijn nog reactief en zouden veel meer moeten vooruitlopen op wet- en regelgeving. Door dat te

doen, kunnen we de business beter ondersteunen en kan de business zijn klanten beter bedienen. Want uiteindelijk draait het om tevreden klanten. Een tweede aandachtspunt komt voort uit de centralisatie van compliance. We zullen een nóg consistenter beleid en werkproces moeten doorvoeren in al onze activiteiten in binnen- en buitenland. Het derde punt is het scherper afbakenen van onze three lines of defense. De eerste lijn is de business zelf: medewerkers moeten helder hebben wat onze processen en richtlijnen zijn. De tweede lijn is risk en compliance. Wij zijn de experts in wet- regelgeving en moeten zorgen dat die regels en onze eigen ambities goed zijn vertaald in interne processen en beleid. Tot slot is er de derde lijn, audit, die onafhankelijk toetst of de eerste en tweede lijn in control zijn en de risico's goed afdekken. Ik vind dat de eerste lijn nog iets te snel naar de tweede lijn stapt. Dat heeft ook te maken met de cultuur binnen Rabobank die gericht is op samenwerken en het samen oplossen van problemen. Maar medewerkers moeten zelf verantwoordelijkheid nemen en kunnen nemen. Dat betekent dat wij ervoor moeten zorgen dat zij nog beter in staat zijn om zelf in te schatten of een klant, een product of de combinatie een hoog of laag risico draagt. Bij een hoog risico hoort een advies van de tweede lijn, dus in al die gevallen ben ik blij als ze bij ons aankloppen, zodat wij kunnen toetsen of hun zaak past bij de risk appetite van Rabobank."

Kun je schetsen hoe compliance is gestructureerd binnen Rabobank? "We hebben in totaal zeshonderd compliance officers wereldwijd: driehonderdvijftig in Nederland voor de lokale banken en de centrale functies, en tweehonderdvijftig in ons wereldwijde netwerk. Door de centralisatie van compliance is ook de organisatie ervan veranderd. Zo worden de lokale banken nu regionaal ondersteund door zogenaamde kring compliance officers; zij zijn sparring partner voor een aantal banken. Centrale functies vind je binnen de afdeling operations en expertise; daar monitoren ze transacties en reageren op fraude-, witwas- of sanctiesignalen. Ook is er een afdeling die forensisch onderzoek verricht naar niet-integer gedrag. We zijn nu bezig om die drie centrale afdelingen anders in te richten. Minder vanuit de organisatiestructuur en meer vanuit de kerntaken die van compliance worden verwacht. Dat gaan we doen met expertteams. Het eerste team doet assessments, en houdt zich bezig met risicoanalyses en het beleid dat daarbij hoort. Het tweede team bewaakt wereldwijd de kwaliteit door monitoring. Het derde team bestaat uit de adviseurs, de sparring partners voor de business. Het vierde team houdt zich bezig met klant-acceptatie, witwassen en sancties, onderwerpen die bij

Vraag je nooit af:
'Kan ik dit wel op
deze manier zeggen?'
Doe het gewoon,
want dáár ben je
voor gevraagd.

alle banken nog altijd hoog op de agenda staan. Tot slot hebben we nog de teams die de ondersteunende activiteiten, waaronder transactiemonitoring en bijzondere onderzoeken, voor de organisatie verrichten en uiteraard de strategische managementactiviteiten van de compliance-organisatie zelf. "

Wat betekent deze nieuwe structuur voor jullie compliance officers? "Het werk wordt veel leuker! Want je krijgt zo de kans om je nog meer te specialiseren in je talent en vakmanschap. Je hoeft niet meer alles te doen. Iemand die graag beleid schrijft, is een andere persoonlijkheid dan iemand die graag monitort of iemand die graag adviseert. Het betekent dat je kerntaak smaller wordt, maar tegelijk dat de scope van je werk verbreedt. Dus als het opstellen van beleid jouw expertise is, dan ga je dat niet alleen doen voor corruptie maar ook voor andere onderwerpen, en niet meer alleen voor Nederland maar ook internationaal. Je onderwerpen worden dus afwisselender en je komt veel meer in je eigen kracht te staan."

Een heel andere vraag. Wat vind je van de EBA guidelines on internal governance die in oktober vorig jaar zijn gepubliceerd? "Hoe duidelijker de rol van compliancefuncties wordt, des te beter en de nieuwe guidelines dragen daaraan bij. Ik geef toe dat het soms makkelijk is dat er regels zijn waarnaar je kunt verwijzen, ze geven je een soort rugdekking. Maar je hebt natuurlijk liever dat dit niet nodig is, dat er in je organisatie voldoende bewustzijn is over wat de maatschappij van haar verwacht. Ik vind ook niet dat je naar aanleiding van elk issue de regels weer verder moet aanscherpen. Met de bestaande regelgeving en de eigen afweging over welke risico's je wel en niet neemt, kunnen we al een prima way

of working neerzetten. Kijk goed naar het gedrag en de cultuur, zorg voor een goede analyse van de issues en kijk hoe je die in de toekomst voorkomt. Dat helpt meer dan het verder aanscherpen van de regelgeving."

Hoe is de onafhankelijkheid van jouw rol binnen Rabobank gewaarborgd? Ben je daar tevreden over?

"De onafhankelijkheid van de compliance officer begint bij de compliance officer zelf. Voel je dat je vrij bent om je rol in te vullen? In mijn rol hier voel ik dat zo. Dat heeft te maken met het feit dat ik direct rapporteer aan de CRO; met haar heb ik een goed en open contact. Daarnaast heb ik een open communicatielijnen naar de bestuursvoorzitter; periodiek, maar ook ad hoc als ik zaken wil adresseren. Verder spreek ik periodiek met alle bestuursleden, met de voorzitter van de raad van commissarissen en de voorzitters van de audit committee en risk committee. Zowel met bestuursleden als met commissarissen heb ik een-op-een gesprekken. Ik voel me daar echt heel comfortabel bij.

Ik weet uit mijn consultancytijd dat dit zeker niet vanzelfsprekend is. Mocht de raad van bestuur op enig moment niet blij zijn met mijn acteren, dan zullen zij dat met de raad van commissarissen moeten opnemen, want ook zij gaan over de aanname en ontslag van de chieft compliance officer. Dat vind ik belangrijke voorwaarden om mijn rol goed uit te kunnen voeren."

Je wilde weer zelf met je voeten in de modder staan. Lukt dat als chieft compliance officer?

"O ja hoor. Ik voer nog steeds fijne gesprekken waarbij ik integriteitsdilemma's opvoer. Bijvoorbeeld als sparring-partner van het bestuur. Ik vind het heerlijk om twee verschillende meningen naar elkaar toe te laten bewegen door het stellen van de juiste vragen. Net zoals ik graag gesprekken voer met de business en dan bijvoorbeeld de vraag stel: 'Als dit morgen op de voorpagina van de krant staat, wat vind je daar dan van?' Men zegt wel eens dat compliance officers de taak hebben om de organisatie een spiegel voor te houden, maar ik zeg liever dat het onze taak is alle medewerkers te leren zelf de spiegel op te pakken."

Heb je tips voor compliance officers? "Blijf dicht bij jezelf en besef wat je rol is in de organisatie. Je bent er om de business te helpen. Het kan eigenlijk niet dat jij een heel andere conclusie over een zaak trekt dan de business. Want jullie willen allebei hetzelfde: tevreden klanten. Dus ook als je voelt dat de business misschien denkt 'O jee, daar heb je ze weer': wees trots op je vak. Je vervult een belangrijke rol en beschikt over belangrijke kennis. De business heeft je nodig. Vraag je nooit af: 'Kan ik dit wel op deze manier zeggen?' Doe het gewoon, want dáár ben je voor gevraagd. Ik heb nooit een blad voor mijn mond genomen en ben daar heel blij mee."



Nieuwe governance-regels voor banken en beleggingsondernemingen

Hanne Wanders en Cora Wielenga¹

EBA heeft in 2016 een concept voor de nieuwe richtlijnen² voor interne governance bij banken en beleggingsondernemingen uitgebracht. Deze nieuwe richtlijnen zullen de huidige richtlijnen voor interne governance³ gaan vervangen. In deze bijdrage gaan we in op de inhoud van de nieuwe richtlijnen. We belichten een aantal wijzigingen die wat ons betreft het vermelden waard zijn en plaatsen kanttekeningen bij de nieuwe richtlijnen. We sluiten af met een advies aan de compliance officers van Nederlandse financiële ondernemingen.

Juridische grondslag

Op grond van artikel 74 van de CRD IV⁴ mag de EBA richtlijnen uitwerken op het gebied van governance. Deze richtlijnen zijn van toepassing op individuele instellingen of, wanneer er sprake is van een groep, op de hele groep (ook al is de CRD niet rechtstreeks van toepassing op dochterondernemingen).

Reikwijdte EBA-richtlijnen voor interne governance

De EBA-richtlijnen zijn van toepassing op banken en beleggingsondernemingen. Bank en beleggingsondernemingen doen er wat ons betreft verstandig aan om kennis te nemen van deze richtlijnen en op basis van deze richtlijnen te evalueren of er interne aanpassingen noodzakelijk zullen zijn. Hoewel deze regels op dit moment alleen van toepassing zijn op banken en beleggingsondernemingen, is het vaak zo dat dergelijke

regels op een later moment ook van toepassing worden op andere financiële ondernemingen.

Definitie van internal governance

Er bestaan veel definities van (interne) governance. In de EBA-richtlijnen wordt de volgende definitie meegegeven van internal governance:

"Internal governance omvat alle standaarden en principes die er zijn om het onderstaande te bepalen dan wel in te richten:

- *doelen, strategieën en risicomanagementsysteem van de organisatie;*
- *organisatie van de business;*
- *verantwoordelijkheden en bevoegdheden;*
- *rapportagelijnen en informatiestromen;*
- *raamwerk van interne controle;*
- *financiële en beloningsprocessen;*
- *ICT-systemen;*
- *uitbestedingen;*
- *business continuity management."*

In onze eigen woorden: alle systemen in de breedste zin van het woord, die je nodig hebt om een organisatie op een verantwoorde manier te kunnen voeren.

1 Dit artikel is gebaseerd op een artikel van beide auteurs dat op 10 januari 2017 is gepubliceerd op www.compliance-instituut.nl.

2 EBA, Consultation paper, Draft Guidelines on internal governance, 28 October 2016.

3 EBA, EBA Guidelines on Internal Governance (GL 44), 27 September 2011.

4 Richtlijn 2013/36/EU.

Wat valt er op in de nieuwe EBA-richtlijnen?

Veel verplichtingen uit de nieuwe richtlijnen zijn eerder al verwerkt in de Nederlandse regelgeving en zullen daardoor zeer waarschijnlijk geen effect hebben op de Nederlandse banken en beleggingsondernemingen. Een aantal verplichtingen vallen op, omdat ze tot nu toe nog niet geëxpliciteerd zijn in Nederlandse wetgeving of nog niet gangbaar zijn in het dagelijkse nationale dan wel Europese toezicht. We lichten een aantal wijzigingen toe.

Deze richtlijnen vormen een prima basis voor de evaluatie van de compliancefunctie

1. De raad van bestuur is verantwoordelijk voor de organisatiecultuur en waarden die ervoor zorgen dat verantwoordelijk en ethisch gedrag mogelijk is.⁵ Een gedragscode of een vergelijkbaar instrument maakt hier onderdeel van uit. Hoewel DNB en AFM al een aantal jaar toezicht houden op de organisatiecultuur van financiële ondernemingen, is het wat ons betreft nieuw dat op Europees niveau wordt gesproken over organisatiecultuur en waarden die gericht zijn op ethisch gedrag. In de richtlijnen van 2011 wordt organisatiecultuur alleen in verband gebracht met 'risk culture'. Daarnaast wordt in de richtlijnen uit 2011 ook gesproken over ethische standaarden; deze werden echter nog niet in verband gebracht met de impact die organisatiecultuur kan hebben op gedrag van mensen. Met de komst van het SSM hadden we voorzien dat het toezicht op gedrag en cultuur, uitgeoefend door DNB, aan belang zou inboeten, maar deze nieuwe richtlijnen wijzen erop dat Europa dat belang toch ook onderkent. We kunnen dat alleen maar toejuichen.
2. Significante instellingen mogen, naast de klassieke commissies in de raad van commissarissen, zoals de remuneratiecommissie en de risico- & auditcommissie, ook andere commissies benoemen, zoals bijvoorbeeld een commissie ethiek, gedrag en compliance. Er wordt benoemd dat niet-significante instellingen dit ook mogen doen.⁶ Omdat wordt aangegeven dat het mag, is hier geen sprake van een verplichting. Het is dus niet goed in te schatten of dit nu ook werkelijk verwacht wordt. Wij schatten zelf in dat van significante instellingen verwacht zal worden om deze gespecialiseerde commissies in te stellen en dat zij zich zullen moeten verantwoorden wanneer zij niet overgaan tot dergelijke commissies. Voor andere instellingen zal dit waarschijnlijk (vooralsnog) niet aan de orde zijn.
3. Er wordt meer nadruk gelegd op het beleid over interne governance.⁷ Daarbij wordt aangegeven dat compliance en de andere risico beheersende functies daarvoor input moeten leveren. En daarnaast moet compliance beoordelen in hoeverre de 'internal governance policy' in lijn is met interne regels en externe wet- en regelgeving. Dat is op zich logisch, maar was nog niet eerder geëxpliciteerd.
4. Er wordt meer nadruk gelegd op een beheerste en consistente risicocultuur.⁸ In deze versie van de richtlijnen wordt nader geduid wat onder een risicocultuur wordt verstaan. Hierbij wordt expliciet ingegaan op de waarden van de organisatie, het gedrag van het bestuur, bespreekbaarheid, tegenspraak en verantwoording afleggen. Het valt op dat er een aantal elementen uit het cultuurhuis van DNB⁹ expliciet genoemd worden in de regeling. De ECB onderkent blijkbaar het nut van het monitoren van gedragsbeïnvloedende factoren.
5. Er zijn meer regels opgenomen ten aanzien van de organisatiewaarden en de gedragscode.¹⁰ Er wordt daarbij expliciet gemaakt dat de ethische standaarden ook op uitbestedingspartijen van toepassing moeten zijn.

5 Artikel 19j.

6 Artikel 36.

7 Artikel 70 e.v.

8 Artikel 80 e.v.

9 DNB, De 7 Elementen van een Integere Cultuur. Beleidsvisie en aanpak gedrag en cultuur bij financiële ondernemingen 2010-2014, november 2009.

10 Artikel 85 e.v.

6. Voor het hoofd audit, hoofd risk en het hoofd compliance geldt dat zij een directe rapportagelijnen moeten hebben naar de raad van commissarissen.¹¹ Het is onze ervaring dat deze functionarissen doorgaans al een directe rapportagelijnen hebben naar de raad van commissarissen. Deze verplichting kan de functionarissen helpen die nog geen directe rapportagelijnen hebben. In de richtlijnen wordt overigens niet gesproken over een periodieke rapportagelijnen. Dat is wat ons betreft wel een voorwaarde, want als slechts een escalatielijnen wordt ingericht zonder reguliere rapportagelijnen, bestaat het risico dat de drempel om hier gebruik van te maken als te hoog wordt ervaren. We adviseren compliance officers om ieder kwartaal aan de raad van commissarissen te rapporteren en daarnaast onverwijld in het geval van incidenten. Overigens is in de nieuwe EBA-richtlijnen aangegeven dat de frequentie naar inzicht van de compliance officer ingesteld mag worden.
7. Op grond van de nieuwe richtlijnen mag het hoofd audit, hoofd risk en het hoofd compliance niet overgeplaatst of ontslagen worden zonder voorafgaande instemming van de raad van commissarissen. Bij significante instellingen moeten de nationale externe toezichthouders onverwijld geïnformeerd worden over een benoeming, overplaatsing dan wel vertrek van een hoofd audit, hoofd risk en het hoofd compliance.¹² In de oude richtlijnen was het alleen verplicht om de raad van commissarissen te informeren over de aanstelling dan wel overplaatsing dan wel ontslag van een chief risk officer. We juichen het toe dat de raad van commissarissen instemmingsrecht heeft bij het ontslag dan wel overplaatsing van het hoofd compliance. Het zou nog mooier zijn wanneer de raad van commissarissen eveneens instemmingsrecht krijgt bij de benoeming van het hoofd compliance. Bij een aantal financiële ondernemingen in Nederland is dat al het geval, maar gangbaar kunnen we het (nog) niet noemen.
8. De combinatie van tweedelijnsfuncties is geëxpliciteerd. Het is voor sommige organisaties toegestaan om de risico- en compliance-functie te combineren. Uitgangspunt is proportionaliteit. Voor meer complexe instellingen is dit niet langer toegestaan. De interne auditfunctie mag ongeacht de complexiteit van de organisaties nooit gecombineerd worden met een andere risico beheersende functie.¹³
9. Operationele taken van de compliance-, risico- en auditfunctie mogen uitbesteed worden. Ook hier is het uitgangspunt proportionaliteit.¹⁴
10. De verplichting tot het hebben van een PARP is in de nieuwe richtlijnen nu uitgebreid naar een verplichting tot het hebben van veranderprocedures wanneer er materiële wijzigingen zijn aan processen en systemen. De compliance- en risicofunctie moeten monitoren of wordt voldaan aan het PARP en de veranderprocedures.¹⁵

Regeling misstanden en klokkenluidersregeling

Naast bovengenoemde wijzigingen is in de nieuwe versie van de richtlijnen ook een verplichting ten aanzien van een onafhankelijk meldpunt toegevoegd. Banken en beleggingsondernemingen zijn op grond van de nieuwe EBA-richtlijnen verplicht om een onafhankelijk meldpunt in te richten waar medewerkers, buiten de standaard rapportagelijnen om, een vermoeden van een overtreding kunnen melden.

Organisaties in Nederland met meer dan vijftig medewerkers hebben overigens al sinds 1 juli 2016 een verplichting tot het inrichten van een klokkenluidersregeling. Door deze EBA-richtlijnen zullen banken en

beleggingsondernemingen met minder dan vijftig werknemers ook een klokkenluidersregeling moeten implementeren.

In de richtlijnen wordt vermeld dat de compliance officer, de auditafdeling of een specifiek aangewezen meldpunt uit de klokkenluidersregeling het onafhankelijke meldpunt kan zijn. Wat ons betreft is het niet wenselijk om de compliance officer als meldpunt uit de klokkenluidersregeling te laten optreden. De gedachte hierachter is gelegen in het feit dat de compliance officer vaak een verplichting heeft om incidenten te melden aan een externe toezichthouder op grond van een regeling incidenten. Deze verplichte meldplicht staat op gespannen voet met de geheimhouding die een meldpunt op grond van de klokkenluidersregeling zou moeten waarborgen. Wanneer de compliance officer als meldpunt van de klokkenluidersregeling wordt benaderd kan er een spagaat ontstaan wanneer het een melding betreft die ook aan de externe toezichthouder gemeld zou moeten worden. Om deze vorm van belangenverstrengeling te voorkomen

¹¹ Artikel 123.

¹² Artikel 124.

¹³ Artikel 126.

¹⁴ Artikel 128.

¹⁵ Artikel 143 e.v.

is het daarom beter om de compliance officer niet als meldpunt vanuit de klokkenluidersregeling te benoemen.¹⁶

Het is wat ons betreft overigens ook niet wenselijk dat de afdeling wordt benoemd als meldpunt. Zij moeten immers onafhankelijk blijven om uiteindelijk de verschillende meldprocedures te auditen.

In de richtlijnen wordt overigens ook de suggestie gegeven om een lid van de raad van commissarissen verantwoordelijk te maken om toe te zien op meldingsregelingen, zoals de klokkenluidersregeling. Dat lijkt ons een goed voorstel.

Daarnaast worden externe, nationale toezichthouders verplicht om een meldpunt voor klokkenluidersmeldingen in te richten. DNB heeft dit meldpunt sinds 12 februari 2016 al ingericht.¹⁷

Niet nieuw, maar wel goed om in gedachten te houden

In de richtlijnen zijn een aantal principes over de inrichting van de compliancefunctie opgenomen die op zich niet nieuw zijn, maar wel de moeite waard om in gedachten te houden. Bijvoorbeeld wanneer u zelf een compliancefunctie moet (her)inrichten, auditen of evalueren.

- De compliancefunctie heeft een directe rapportagelijn naar de raad van bestuur en de raad van commissarissen.
- De compliancefunctie zou onafhankelijk van de eerste lijn moeten opereren.
- De compliancefunctie moet voldoende autoriteit, volume en bronnen hebben om de functie goed te kunnen uitoefenen.
- De compliancefunctie moet een monitoringsplan opzetten en uitvoeren om te kunnen beoordelen in hoeverre de onderneming voldoet aan wet- en regelgeving.
- De vergoeding van de compliancefunctie mag niet afhankelijk zijn van de resultaten van de onderneming.

Kanttekeningen

Bij de nieuwe richtlijnen willen we graag een paar kanttekeningen maken.

In deze richtlijnen wordt, net als in de oude richtlijnen, gesproken over 'risk culture'. Wellicht zou het mooier zijn om dit te duiden als 'sound risk culture', om zodoende meer te benadrukken dat het erom gaat zorgvuldig de risico's af te wegen.

In de regeling wordt gesproken over de 'hoofden interne control'. In de definitie staat dat hiermee het hoofd risicomanagement, hoofd compliance en het hoofd audit wordt bedoeld. In de richtlijnen worden deze functies vaak als één functiegroep gedefinieerd, terwijl er toch verschillen zijn die expliciet gemaakt mogen worden. Het zou aan te bevelen zijn om het te hebben over de tweede- en de derdelijnshoofden, dan wel de functies bij naam te noemen. Het is immers wenselijk om de controlerende taken uit de tweede lijn niet te vermengen met de taken uit de derde lijn.

Hoewel we positief zijn over de verwijzing naar het belang van organisatiecultuur, wordt er in de richtlijnen vooral verwezen naar een vrij ouderwetse aanpak van ethische standaarden. Er wordt namelijk aangegeven dat het goed is om ethische standaarden te realiseren in de organisatie, om zodoende risico's te beheersen. Hierbij worden operationeel, juridisch en reputatierisico als voorbeelden genoemd. Het is begrijpelijk dat de EBA organisatiecultuur vanuit risico-oogpunt een plaats geeft in deze richtlijnen. Het zou nog mooier zijn wanneer investeren in organisatiecultuur ook als 'business case' wordt geprofileerd. Het is immers zinvol om te investeren in een goede waardegerichte cultuur. Dat helpt medewerkers en andere belanghebbenden. Echter, wij begrijpen ook dat het niet aan de EBA is om 'organisatiecultuur' te verkopen.

Status EBA-richtlijnen

Het consultatiedocument voor de nieuwe EBA-richtlijnen is gepubliceerd in oktober van 2016. De consultatieperiode liep tot en met 28 januari 2017. De EBA heeft aangegeven dat medio 2017 de nationale toezichthouders de richtlijnen geïmplementeerd moeten hebben. Op dit moment is nog niet duidelijk wanneer de definitieve richtlijnen worden gepubliceerd en is het daardoor ook nog niet duidelijk of medio 2017 inderdaad het doel is. Na publicatie van de definitieve richtlijnen zal DNB de gelegenheid krijgen om een beleidsregel op te stellen waarin zij verklaart de nieuwe richtlijnen over te nemen in het doorlopende toezicht. We verwachten in ieder geval dat deze richtlijnen nog dit jaar in werking zullen treden.

¹⁶ Zie voor meer informatie over de meldprocedure, de rol van de vertrouwenspersoon en de compliance officer ons themanummer 'Klokkenluiden, De Compliance Officer, nummer 23, september 2016 op www.compliance-instituut.nl.

¹⁷ www.dnb.nl/over-dnb/meldpunt-misstanden/index.jsp laatst geraadpleegd op 1 mei 2017.

EBA-richtlijnen in vergelijking met andere governancerichtlijnen en codes

Naast deze EBA-richtlijnen hebben Nederlandse banken en beleggingsondernemingen te maken met andere governancecodes zoals de Code banken en de Nederlandse Corporate Governance Code. Omdat de laatste code onlangs is vernieuwd, is het interessant om de nieuwe bepalingen uit de corporate governance code te vergelijken met de EBA-richtlijnen.

Corporate Governance Code

Sinds 8 december 2016 is er een nieuwe Corporate Governance Code. Hoewel deze code alleen van toepassing is op beursondernemingen en op institutionele beleggers, houden we er rekening mee dat ook deze code als minimale norm zal worden aangeduid door DNB, net zoals dat bij de code uit 2008 het geval is geweest. Om die reden is het verstandig om ook als niet-beursgenoteerde instantie te beoordelen in hoeverre voldaan wordt aan de principes uit de code. Onderstaand hebben we een aantal bepalingen uit de nieuwe code opgenomen en deze vergeleken met de bepalingen uit de EBA-richtlijnen.

- In de herziene code is langetermijnwaardecreatie als het startpunt van corporate governance geformuleerd. Hoe het bestuur daar uitvoering aangeeft, moet jaarlijks in het bestuursverslag vermeld worden. In de EBA-richtlijnen is geen verplichting over verslaglegging opgenomen, hetgeen logisch is, omdat de EBA-richtlijnen ook op niet-beursgenoteerde ondernemingen van toepassing zijn.
- Net zoals in de EBA-richtlijnen, is ook in de herziene code aandacht gevraagd voor cultuur. "Van bestuurders en commissarissen wordt verwacht dat zij een cultuur creëren die het gewenste gedrag en integer handelen stimuleert." Hoewel het met andere woorden omschreven is, komt de strekking van deze bepaling overeen met de bepalingen over de ethische cultuur uit de EBA-richtlijnen.
- Het bestuur moet volgens de corporate governance code een regeling opstellen voor het melden van (vermoedens) van misstanden en onregelmatigheden. Waar in de EBA-richtlijnen er een commissaris benoemd moet worden die toezicht houdt op de interne meldingsregelingen, gaat de code een stapje verder. De raad van commissarissen moet toezicht houden op de wijze waarop het bestuur de meldingsregeling uitvoert. En daarnaast moet het bestuur de voorzitter van de raad van commissarissen onverwijld informeren over signalen van (vermoedens) van materiële misstanden en onregelmatigheden. Verder is geregeld dat in het geval van een vermoeden van een misstand aangaande het functioneren van een bestuurder, dit direct aan de voorzitter van de raad van commissarissen gemeld kan worden. Dit laatste is wat ons betreft niet wenselijk. Het is voor melders vaak te lastig om aan de raad van commissarissen te melden; dit wordt als een te hoge drempel ervaren. We adviseren daarom om op voor punt de modelklokkenluidersregeling¹⁸ van het Huis voor klokkenluiders te gebruiken.
- Het bestuur moet bij de verantwoording over het risicomanagement ook aangeven wanneer er materiële risico's zijn die gevolgen hebben voor de continuïteit van de onderneming. In de EBA-richtlijnen worden geen eisen gesteld over de verslaglegging.
- De raad van commissarissen krijgt zowel de benoeming als het ontslag van de leidinggevende interne auditor ter goedkeuring voorgelegd op grond van de herziene code. Op grond van de EBA-richtlijnen moet de raad van commissarissen alleen goedkeuring geven wanneer een hoofd van de interne auditdienst wordt overgeplaatst dan wel ontslagen. De code gaat op dit punt dus verder dan de EBA-richtlijnen. Bij significante instellingen moet de externe toezichthouder geïnformeerd worden over een aanstelling dan wel ontslag van het hoofd van de auditdiensten. Dit is in het geval van de nieuwe code vanzelfsprekend geen verplichting, omdat veel uitgevende instellingen geen externe toezichthouder hebben.
- In de nieuwe code wordt extra aandacht gegeven aan de diversiteit van het bestuur en de raad van commissarissen, zowel wat betreft de verhouding tussen het aantal mannen en vrouwen als met betrekking tot deskundigheid, achtergrond en competenties. De EBA heeft deze principes nader uitgewerkt in de richtlijnen inzake de geschiktheidstoetsing van bestuurders, commissarissen en sleutelfunctionarissen¹⁹. De principes van de EBA zijn verderstrekkend dan die van de code.

18 Het NCI heeft een aangepast model gemaakt voor de financiële sector, zie www.compliance-instituut.nl/wp-content/uploads/Modelregeling-Melden-misstanden-NCI-1.pdf.

19 EBA, Draft Guidelines on the assessment of the suitability of members of the management body and key function holders, 28 October 2016.

- Op grond van de code moeten instellingen een gedegen plan voor de opvolging van bestuurders en commissarissen opstellen. De EBA heeft regels van dezelfde strekking uitgewerkt in de richtlijnen inzake de geschiktheidstoetsing van bestuurders, commissarissen en sleutelfunctionarissen.²⁰
- In de nieuwe code wordt verlangd dat tenminste één commissaris afhankelijk is. Het totaal aantal onafhankelijke commissarissen moet echter altijd meer zijn dan het aantal afhankelijke commissarissen. De EBA stelt alleen als eis dat een voldoende aantal onafhankelijk moet zijn.
- Benoemingstermijn van commissarissen is volgens de code in principe een periode van twee keer vier jaar. Na een periode van acht jaar mag twee maal twee jaar verlengd worden, echter moet dit wel gemotiveerd worden. De EBA geeft hierover geen concrete richtlijnen.
- De code verwacht van commissarissen dat zij specifiek aandacht besteden aan de dynamiek en de verhouding tussen het bestuur en het onderliggende echelon. De EBA geeft hierover geen concrete richtlijnen.
- In de nieuwe code zijn de oude regels ten aanzien van belonen teruggebracht naar één regel: het beloningsbeleid van de vennootschap dient duidelijk en begrijpelijk te zijn. Over de uiteindelijk toegekende beloning wordt op een inzichtelijke wijze verantwoording afgelegd. Nieuw is dat de raad van commissarissen ook de visie van de bestuurder betreft bij het vaststellen van de hoogte en structuur van diens beloning. EBA beperkt zich niet tot één regel, zij stelt juist heel veel specifieke regels ten aanzien van de beloning. Deze regels zijn uitgewerkt in afzonderlijke richtlijnen²¹.
- De nieuwe code verlangt transparantie over de verhoudingen tussen de beloningen van bestuurders en die van werknemers. EBA geeft hier geen nadere regels over uit.

Moet u als compliance officer aan de slag?

Wanneer u als compliance officer werkzaam bent bij een bank of beleggingsonderneming, is het raadzaam om de ontwikkelingen ten aanzien van deze richtlijnen te volgen. Op dit moment zijn het nog conceptrichtlijnen, er kunnen dus nog wijzigingen worden doorgevoerd

Mogelijk zult u aanpassingen moeten doorvoeren om te gaan voldoen aan de uiteindelijk definitieve versie van deze richtlijnen. Wij zien deze richtlijnen, ondanks onze kanttekeningen, als een mooi kader voor de interne governance van banken en beleggingsondernemingen. Andere typen financiële ondernemingen kunnen deze richtlijnen ook als uitgangspunt gebruiken. Het is een prima document om de interne governance te toetsen.

Ook het gesprek over de borging van ethische waarden in de organisatiecultuur kan met deze richtlijnen (verder) gevoerd worden. En vanzelfsprekend is het verstandig om dan niet alleen naar de EBA-richtlijnen te kijken, maar evenzeer de Corporate Governance Code mee te nemen.

Hanne Wanders is compliance officer bij het Nederlands Compliance Instituut. Cora Wielenga is directeur van het Nederlands Compliance Instituut. Zij zijn beide als compliance officer gespecialiseerd in governance.

²⁰ EBA, Draft Guidelines on the assessment of the suitability of members of the management body and key function holders, 28 October 2016.

²¹ EBA, Guidelines on sound remuneration policies under Article s 74(3) and 75(2) of Directive 2013/36/EU and disclosures under Article 450 of Regulation (EU) No 575/2013, 21 December 2015.

Save the date: 28 september 2017

VCO Compliance Symposium 2017

De Vereniging van Compliance Professionals (VCO) heeft dit jaar gekozen voor een nieuwe insteek van de jaarlijkse kennisdag. Het symposium zal dit jaar in het teken staan van *verandering* en *vernieuwing*.

Compliance officers hebben continu te maken met een veranderende omgeving. Dat geldt net zo goed voor de VCO, die momenteel zelf aan veranderingen onderhevig is. Het VCO Compliance Symposium 2017 draagt dan ook als subthema: **'From old school to new school'** en staat in het teken van verandering in wetgeving en toezicht en vernieuwing op het gebied van technologie.



Tijdens deze dag zullen diverse sprekers – van toezicht-houders tot auditors en experts op het gebied van technologie – gastcolleges geven over privacy, hacking, root cause analysis en het toezien op gedrag & cultuur. Kortom: een boeiend evenement dat u niet mag missen!

Het evenement is opengesteld voor alle belangstellenden. Bent u lid van de VCO? In dat geval kunt u tegen een gereduceerd tarief aan het symposium deelnemen.

Meer informatie vindt u op de website van de Vereniging van Compliance Professionals: vco.nl.



Nu beschikbaar: inschrijven via EDU-DEX

Vanaf nu is het mogelijk om voor onze opleidingen in te schrijven via EDU-DEX.

Wie zich in het verleden nog door een wir war van websites en opleidingen moest banen om de juiste opleiding te vinden, kan nu gebruik maken van de landelijke data-standaard EDU-DEX. EDU-DEX is voor en door opleiders in het leven geroepen en verspreidt opleidingsinformatie van ruim zestig opleidingsinstituten, waaronder nu ook het onze.

Goed om te weten is dat inschrijven op één van onze opleidingen via EDU-DEX kosteloos is. Bij inschrijving via EDU-DEX wordt u direct doorgeleid naar onze website; EDU-DEX heeft namelijk geen eigen portal en houdt zich niet bezig met inschrijvingsafhandeling.

Voor meer informatie en inschrijven op één van onze opleidingen, ga naar: edu-dex.nl
Uiteraard kunt u ook nog steeds direct inschrijven via onze eigen website: compliance-instituut.nl

Governance or gaffernance¹

Een gevoel van ironie ontgaat me niet, en dan heb ik het over de politieke gang van zaken in Washington en het Witte Huis in het bijzonder. Echt, ik probeer politiek buiten de deur te houden in mijn columns, maar het zou haast onrealistisch zijn om er niet over te schrijven. Te meer vanwege het thema van dit kwartaal: 'governance'.

Wat 'governance' betreft, gaat het in ons vakgebied meestal niet over zaken die een staat aangaan, of over hoe men politiek bedrijft. Of is er wel een verband? Het begrip 'governance' is namelijk evenzeer van toepassing op landen als op bedrijven. Governance is het proces van samenwerking en besluitvorming tussen betrokkenen van een gedeeld probleem dat leidt tot de creatie, versterking of herhaling van sociale normen en instituties.² Althans, als ik Mark Bevir mag geloven. In die zin gaat het dus ook over het zijn van een goed landsbestuurder.

En het zal u vast niet ontgaan zijn, maar mijn nieuwe thuisland heeft sinds een aantal maanden een nieuw bestuur. Een bestuurder die op zijn geheel eigen wijze sociale normen en instituties op hun grondvesten doet schudden. Zijn presidentiële loopbaan is vooralsnog net zo controversieel als zijn verkiezingscampagne c.q. overwinning. En ondanks wat ik of de gangbare media ervan mag vinden, zijn er toch nog Amerikanen *that still seem to love it*.³

Veel van de aangekaarte controversie gaat over belangenconflicten. In de Amerikaanse overheid is er één instituut dat sinds 1978 op dit vlak een belangrijke rol speelt, de United States Office of Governmental Ethics, kortweg OGE. Haar missie: *"to achieve a high level of public confidence in the integrity of executive branch programs and operations"*. Ze doet dat onder meer door toezicht, normstelling en training. Ze verzamelt en publiceert onder meer overzichten van mogelijke belangenconflicten. Daartoe moeten alle,

1 A gaffe; noun 1) a clumsy social error or faux pass or 2) a blatant mistake or misjudgement.

2 Bevir, Mark (2013). Governance: A very short introduction. Oxford, UK: Oxford University Press.

3 Gallup approval ratings (in %): Reagan (53), Bush (61), Clinton (55), Bush (49), Obama (48) en Trump (41).



ja ook Trump, hooggeplaatste functionarissen jaarlijks een overzicht indienen van al hun inkomsten, geschenken, financiële bezittingen en schulden.

Sinds de nieuwe leider van de vrije wereld, hebben ze het bij de OGE een beetje drukker dan normaal. Gedurende de eerste zes maanden van Obama (tussen oktober 2008 en maart 2009) ontving de OGE 733 klachten en informatieverzoeken. Acht jaar later ontving de OGE er maar liefst 39.105 – een stijging van 5.235%. Terwijl Trump diens overzicht nog niet heeft ingediend.

Ik hoop maar dat instituties zoals het OGE in staat zullen zijn om de normen van good governance te waarborgen. Het alternatief is namelijk dat Trump met zijn 'gaffes' de nieuwe norm wordt. Governance verwordt dan eerder gaffernance.

Groetjes,

Joost

Joost Montens werkt voor AstraZeneca, een innovatief biofarmaceutisch bedrijf. Sinds februari 2015 woont en werkt hij in de Verenigde Staten. In deze column bericht hij over zijn compliance-ervaringen en bevindingen.

Ontslag en tuchtrecht banken?

Constant van Tuyll van Serooskerken

Na een trage start heeft het tuchtrecht banken inmiddels een (bescheiden) vlucht genomen. Deze trage opstartperiode is overigens begrijpelijk aangezien het tuchtrecht banken per 1 april 2015 is ingevoerd en gedragingen van voor deze periode niet onder het tuchtrecht vallen. Daarnaast is uiteraard de nodige tijd gemoed met een tuchtrechtelijke procedure: er moet een klacht door een derde worden ingediend, deze moet worden overgenomen door de professionele aanklager en vervolgens dient het inhoudelijke proces plaats te vinden. Op het moment van schrijven van dit artikel zijn er vijf inhoudelijke uitspraken gedaan door de Tuchtcommissie Banken, en één uitspraak door de hoger beroepsinstantie, de Commissie van Beroep.

Tuchtsancties kunnen worden opgelegd wegens een schending van de bancaire gedragsregels. Interessant is om na te gaan in hoeverre de Tuchtcommissie Banken, dan wel de Commissie van Beroep, bij de sanctieoplegging rekening houdt met de mogelijkheid dat een bankmedewerker reeds (op staande voet) is ontslagen en eventuele overige maatregelen die de bank heeft getroffen ten opzichte van de bankmedewerker. En als de bankmedewerker ten tijde van de sanctieoplegging nog in dienst is, komt vervolgens de vraag op in hoeverre de bank tot ontslag kan overgaan nadat de tuchtsanctie is opgelegd.¹ Voordat ik aan deze vragen toekom schets ik eerst enkele grove lijnen uit de gepubliceerde uitspraken, waarbij ik met name de (aard van de) geconstateerde normschendingen en de als gevolg daarvan opgelegde sancties behandel.

Schendingen en sancties

Op de bancaire gedragsregels is behoorlijk wat kritiek gekomen. Een van de kritiekpunten is dat ze te ruim zijn geformuleerd, zoals de gedragsregel dat een bankmedewerker de belangen van de klant centraal dient te stellen, of de gedragsregel dat een bankmedewerker open en eerlijk moet zijn over diens gedrag en zijn verantwoordelijkheid voor de samenleving moet kennen. Er was dan ook onzekerheid over de reikwijdte van de gedragsregels en welke gedragingen van bankmedewerkers gesanctioneerd zouden kunnen worden.

Inmiddels is duidelijk dat de poortwachtersfunctie die de professionele aanklager inneemt, goed werkt en dat 'onzinklachten' niet door de selectie komen. Als we kijken naar de opgelegde sancties betreffen dit gevallen waar de bankmedewerker duidelijk over de schreef is gegaan: zonder zakelijke reden bankrekeningen bekijken, ongeoorloofde belangenverstremgeling door via een klant een persoonlijke lening te laten afsluiten etc.

Wat opvalt bij het bestuderen van de uitspraken is dat het veelal meldingen betreffen die vanuit de banken zelf zijn gedaan. Hoewel er geen expliciete wettelijke grondslag is

¹ Ik bespreek de mogelijkheden hiertoe uitgebreid in, C.F.J. van Tuyll van Serooskerken, 'Tuchtrecht banken: over klachten, sancties en arbeidsrechtelijke maatregelen', *ArbeidsRecht* 2015/55.

voor een dergelijke 'klikplicht', is dit volgens de regering wel een verplichting die op banken rust.² Dit doet enigszins vreemd aan, omdat het tuchtrecht in eerste instantie bedoeld is voor, en ter bescherming van, de klanten van de bank. Daar staat tegenover dat het feit dat de uitspraken gepubliceerd worden, en de nodige media-aandacht ontvangen, denkbaar bijdraagt aan het herwinnen van het maatschappelijk vertrouwen in de sector, wat een van de doelstellingen is achter de invoering van het tuchtrecht banken.

Wat nog meer opvalt is de aandacht die de Tuchtcommissie Banken heeft voor de wijze waarop de bankmedewerker handelt nadat het kwaad is geschied. Heeft de bankmedewerker direct spijt betuigd bij ontdekking? Of heeft de bankmedewerker juist zijn gedragingen proberen te verdoezelen of goed te praten? Veel sterker dan bij een gerechtelijke procedure – waar categorische ontkenning kan lonen – lijkt spijtbetuiging en actief fouterstel een grote rol te spelen in het bankentuchtrecht, en met name bij de strafmaat. Een bankmedewerker die het rekeningnummer van een klant blokkeerde, om zo op oneigenlijke wijze met deze klant in contact te komen, maar die direct daarna zijn excuses aanbod en zich ook anderszins schuld bewust opstelde, kwam met de schrik vrij. In een andere zaak werkte het feit dat een bankmedewerker geen openheid van zaken bood richting de bank bij ontdekking van belangenverstremming juist strafverzwarend.

Bij geconstateerde schending van de gedragsregels kunnen diverse sancties worden opgelegd, zoals een berisping, het opleggen van een educatieve maatregel, een geldboete (van maximaal € 25.000,-) of een beroepsverbod (van maximaal drie jaar). De enige sanctie die de Tuchtcommissie Banken tot nog toe heeft opgelegd, is het beroepsverbod. Dit is op zich opmerkelijk, omdat dit de zwaarste sanctie is. In de gepubliceerde uitspraken is twee keer een beroepsverbod van zes maanden opgelegd en één keer van één jaar.

Het beroepsverbod is algemeen van aard. Het hangt dus niet samen met een bepaald beroep, maar met het verrichten van enige werkzaamheid in de bancaire sector. Dit lijkt voor de medewerker wel mogelijkheden te bieden om aan de slag te gaan bij een vermogensbeheerder of een kredietverstrekker, zolang het maar geen bank is.

Niettemin is een beroepsverbod een ingrijpende maatregel, temeer omdat deze sanctie wordt opgenomen in het tuchtregister – dat inzichtelijk is voor aangesloten banken – en een aantekening in dit register pas na drie jaar wordt doorgehaald.

Ontslag werknemer vooraf aan tuchtsanctie

De professionele aanklager kan bij zijn beslissing om al dan niet een klacht voor te leggen aan de Tuchtcommissie Banken, rekening houden met de omstandigheid dat de bank reeds sancties en/of maatregelen heeft opgelegd aan de bankmedewerker. Ook de tuchtcommissie kan hiermee rekening houden bij het bepalen van de strafmaat.³ In de drie zaken waarin een beroepsverbod werd uitgesproken, speelde het ontslag van de medewerker één keer een rol. Niet geheel toevallig was dit een zaak waarin de professionele aanklager het maximale beroepsverbod van drie jaar eiste. De Tuchtcommissie Banken zag in het ontslag van de medewerker, en in de langdurige opname van de medewerker in het incidentenregister en het Externe Verwijzingsregister van de bank, aanleiding om de duur van het geëiste beroepsverbod te beperken tot zes maanden.

In de andere zaken waar de bankmedewerkers beroepsverboden opgelegd kregen van zes maanden en van één jaar, eiste de professionele aanklager veel mildere straffen, namelijk een geldboete van € 500,- respectievelijk € 1.500,-. Het feit dat ook deze bankmedewerkers waren ontslagen, en de langdurige opname in het incidentenregister en Externe Verwijzingsregister, kwam in deze uitspraken niet terug in de overwegingen van de tuchtcommissie. In de ene zaak rekent de Tuchtcommissie Banken de bankmedewerker af op diens zeer lange staat van dienst (negenentwintig jaar) – de bankmedewerker had daarom beter moeten weten – en in de andere zaak wordt als verzwarende omstandigheid opgevoerd dat de bankmedewerker een leidinggevende positie vervulde, en daarom een voorbeeldfunctie richting ondergeschikten had.

Ik kan mij niet aan de indruk onttrekken dat de motivering van de Tuchtcommissie Banken een zekere willekeur kent, afhankelijk van de door de professionele aanklager geëiste strafmaat. De rode draad lijkt in ieder geval te zijn dat de

² Kamerstukken II 2013/14, 33 918, nr. 10, p. 9.

³ De juridische basis hiervoor is mijns inziens te vinden in paragraaf 3.2 van het tuchtreglement waar staat "waarbij zij in ieder geval rekening houdt met de in artikel 2.2.3 genoemde omstandigheden".



Tuchtcommissie Banken niet snel genoeg neemt met een (lage) boete als straf, maar relatief makkelijk een beroepsverbod oplegt, zij het niet voor de maximale duur van drie jaar maar voor een periode van zes maanden tot één jaar.

Ontslag werknemer na tuchtsanctie

Er zijn meerdere redenen te bedenken waarom een bank wacht met het ontslaan van een bankmedewerker tot na de tuchtprocedure, bijvoorbeeld omdat (i) de bank er niet van overtuigd is dat de medewerker kwalijk heeft gehandeld, (ii) de feiten nog onvoldoende vaststaan, (iii) de belangen van de bank en de bankmedewerker parallel lopen gedurende de tuchtprocedure, of (iv) de bank het ontslagdossier niet sterk genoeg vindt zonder tuchtrechtelijke veroordeling.

Of een bankmedewerker na de tuchtprocedure nog kan worden ontslagen, hangt af van de omstandigheden van het geval. De bankmedewerker zal niet snel ontslagen kunnen worden vanwege het enkele feit dat een tuchtsanctie is opgelegd – daarmee zou de bankmedewerker immers dubbel bestraft worden – maar de bankmedewerker kan wel ontslagen worden aan de hand van hetzelfde feitencomplex dat ten grondslag ligt aan de tuchtsanctie. De feiten en omstandigheden die ten grondslag liggen aan een zware sanctie als een beroepsverbod zullen in algemene zin strengere arbeidsrechtelijke maatregelen rechtvaardigen dan het feitencomplex dat ten grondslag ligt aan, bijvoorbeeld, een veroordeling zonder strafoplegging.

Overigens is het maar de vraag of bij een beroepsverbod veel gerechtelijke ontslagprocedures gevoerd zullen worden. Dit komt omdat de bank het loon van de bankmedewerker gedurende het beroepsverbod in beginsel niet hoeft door te betalen, aangezien de bank de bankmedewerker niet bewust op non-actief stelt, maar zich geconfronteerd ziet met het oordeel van de tuchtcommissie.⁴ Het feit dat de bankmedewerker gedurende een langere periode geen loon ontvangt, zal er naar verwachting toe leiden dat de bankmedewerker eerder bereid is een schikking te treffen met de bank over zijn ontslag.⁵ Indien een bankmedewerker echter weigert mee te werken aan een schikking over zijn ontslag, is het voor de bank mogelijk lastiger het ontslag te effectueren, omdat een van de grootste bezwaren voor de bank bij indiensthouding is weggevallen, namelijk het doorbetalen van loon.

4 Dit in afwijking van de 'Van der Gulik/Vissers'-leer van de Hoge Raad. Zie ook: p. 7/8, C.F.J. van Tuyl, t.a.p.

5 Mits hier ruimte voor is onder de beloningsregels die (onder meer) bepalen dat een ontslagvergoeding zodanig dient te zijn vormgegeven dat falen en onbetamelijk gedrag van de bankmedewerker niet mogen worden beloond (artikel 18 Regeling beheerst beloningsbeleid Wft 2014) en geen vertrekvergoeding aan de bankmedewerker mag worden toegekend bij ernstig verwijtbaar handelen of nalaten (artikel 1:125 lid 1 Wft).

Ontslag op staande voet

Gelet op het tijdsverloop, zal ontslag op staande voet doorgaans geen optie meer zijn na de tuchtprocedure. In dat geval wordt immers niet meer voldaan aan het onverwijldheidsvereiste, een van de grondbeginselen van het geven van een rechtsgeldig ontslag op staande voet. Daar komt bij dat een ontslag op staande voet een zeer ingrijpende maatregel is – de bankmedewerker krijgt geen vergoeding mee en heeft ook geen recht op WW – zodat een rechter hier zeer kritisch naar zal kijken en daarbij ook de persoonlijke omstandigheden van de bankmedewerker zal meewegen. Al met al is een ontslag op staande voet dus niet zonder risico voor de bank.

Ontslag via de rechter

Als het ontslag aan de rechter wordt voorgelegd, zal deze beoordelen of er een redelijke grond is om tot ontbinding van de arbeidsovereenkomst over te gaan. Als er geen redelijke grond is, zal de rechter de gevraagde ontbinding weigeren. De in de wet opgenomen 'redelijke gronden' die de bank naar verwachting kan aanvoeren in een ontslagprocedure die samenhangt met een tuchtrechtelijke sanctie, zijn de zogeheten 'e-grond' (verwijtbaar handelen of nalaten werknemer), de 'g-grond' (verstoorde arbeidsverhouding) en/of de 'h-grond' (overige omstandigheden).⁶ In de praktijk voeren partijen schikkingsonderhandelingen over het bereiken van een minnelijke vertrekregeling voorafgaand aan een gang naar de rechter. Ook deze schikkingsonderhandelingen worden doorgaans in sterke mate gekleurd door de verwachting van partijen of de rechter al dan niet tot ontbinding van de arbeidsovereenkomst zal overgaan.

Factoren die een rol spelen bij de beoordeling door een rechter of sprake is van een redelijke grond, zijn (onder meer) de opstelling van bank en bankmedewerker jegens elkaar, de zwaarte van de sanctie en de aard en ernst van het onbehoorlijke handelen van de bankmedewerker. Daarnaast zijn naar verwachting de volgende omstandigheden van invloed op het oordeel van de rechter: de cultuur binnen de bank (gedoogcultuur vs. actief onderricht over de gedragsregels), het interne beleid van de bank – inclusief consequente handhaving bij overtreding – en de (leidinggevende) positie van de bankmedewerker.⁷

In algemene zin is de kans dat een rechter ontbindt groter naarmate het beroepsverbod dat de bankmedewerker opgelegd heeft gekregen langer duurt. Het is praktisch niet altijd haalbaar voor een bank om een medewerker na een langdurige afwezigheid weer in diens oude positie terug te nemen: er is dan bijvoorbeeld een (permanente) vervanger aangetrokken en/of de bankmedewerker voldoet niet meer aan de (nieuwe) eisen die de functie stelt. Deze omstandigheden kunnen in mijn optiek als een (voldragen) 'h-grond' voor ontslag kwalificeren.

Conclusie

De eerste uitspraken van de Tuchtcommissie Banken bieden inzicht in de overwegingen die de tuchtcommissie ten grondslag legt aan de sanctieoplegging, en met name de zwaarste sanctie, het beroepsverbod. Opvallend is dat niet alleen de aard van de normschending een rol speelt, maar ook hoe de bankmedewerker hier achteraf mee is omgegaan.

De uitspraken bieden daarnaast inzicht in hoe de Tuchtcommissie Banken bij het bepalen van de strafmaat de maatregelen die de bank reeds jegens de bankmedewerker heeft genomen waardeert, daaronder begrepen het ontslag van de bankmedewerker. De voorzichtige conclusie kan worden getrokken dat de maatregelen van de bank met name een rol spelen als de tuchtcommissie van oordeel is dat de door de professionele aanklager geëiste straf te zwaar is en de tuchtcommissie een lichtere straf wil opleggen. In eerdergenoemde zaak betrof dit een matiging van het geëiste beroepsverbod van drie jaar naar zes maanden.

Of ontslag te effectueren is na oplegging van een tuchtsanctie hangt af van het feitencomplex dat ten grondslag ligt aan de tuchtsanctie alsmede van de overige omstandigheden van het geval. Ontslag op staande voet lijkt een gepasseerd station en ook het feit dat de bank in de meeste gevallen geen loon hoeft door te betalen zal logischerwijs niet bijdragen aan de aan te tonen noodzaak tot ontslag. Als het echter een beroepsverbod voor langere duur betreft en de bank valt geen verwijt te maken van de gedragingen van de bankmedewerker, dan lijkt een ontslag tot de mogelijkheden te behoren.

Mr. C.F.J. (Constant) van Tuyll van Serooskerken is advocaat financieel arbeidsrecht & beloningsbeleid bij Van Doorne.

⁶ Zie artikel 7:669 lid 3 BW.

⁷ Zie voor meer duiding: p. 9-12, C.F.J. van Tuyll, t.a.p.

Speakers' Corner: Sharda Poelloe

Waar is het touwtje in de compliance toolkit?



Eind 2016 deed Jan Terlouw¹ een emotionele oproep om elkaar meer te vertrouwen. Als symbool hiervoor gebruikte hij het touwtje dat vroeger uit de brievenbus hing, waarmee buiten spelende kinderen elk moment de deur konden openen en naar binnen konden komen. De achteloosheid waarmee dit werd gedaan, weerspiegelde een diepgeworteld vertrouwen in je omgeving. In de speech deed Terlouw een dringend beroep op de politiek om het vertrouwen in de maatschappij terug te brengen.

Nederland was diep geraakt door deze speech, maar naast een lawine van warme reacties was er ook kritiek. De speech zou sentimenteel zijn en niet de oplossing bieden in een wereld die in brand staat.

Ter compensatie van het gemis aan vertrouwen hebben wij veel regels, wetten, controles, etc. ingesteld om mensen 'het goede' te laten doen. We veronderstellen dat daar waar wetten ontbreken, slecht gedrag van mensen in de hand wordt gewerkt. Michael L. Michael² stelt echter dat regels en wetten niet per definitie leiden tot het gewenste gedrag, maar zelfs het tegendeel:

"One might suppose that where law is mainly absent, behavior is pretty bad. Yet it turns out to be nearly the other way around. The two areas where law is arguably the largest presence in ordinary life – driving cars and paying taxes – are probably the two areas where there is the largest amount of self-conscious cheating."

Dit betoog wordt bevestigd door professor Cools³ die zegt dat juist in de financiële sector, die van alle sectoren het meest gereguleerd is, de grootste rampen gebeuren. Tegelijkertijd constateert DNB⁴ dat er weinig voortgang wordt geboekt in het herstellen van het maatschappelijk vertrouwen in de financiële sector. De compliance officer die in veel organisaties de taak heeft om toe te zien op de naleving van wet- en regelgeving, heeft deze rampen niet kunnen voorzien, noch kunnen voorkomen. Hierdoor staat de rol van de compliance officer (weer) in de schijnwerpers.

In de nieuwe Corporate Governance Code⁵ is voor het eerst het principe cultuur opgenomen. Deze bepaling lijkt een aanknopingspunt te bieden om een dialoog tussen het bestuur en de compliance officer op gang te brengen. Dit moet leiden tot een fundamentele herijking van de reikwijdte van de compliancefunctie. Een juist evenwicht tussen regels en controle enerzijds én vertrouwen anderzijds zal centraal moeten staan. Het 'touwtje' dient onderdeel te zijn van de toolkit van de compliance officer.

1 Speech Jan Terlouw in 'De Wereld Draait Door', 30-11-2016.

2 Michael L. Michael, *Business Ethics / the law of rules*, maart 2006.

3 Kees Cools, Ziende Blind, *bankingreview*, maart 2011.

4 De Nederlandsche Bank, Staat van het toezicht 2015.

5 De Nederlandse Corporate Governance Code, 8 december 2016.

Wat is vertrouwen?

In definities van vertrouwen komen veelvuldig twee relaties⁶ naar voren: de relatie tussen *vertrouwen en verwachtingen* en de relatie tussen *vertrouwen en risico*. In een niet-perfecte wereld is er altijd gebrek aan kennis/informatie. De beschikbare informatie in combinatie met het gevoel (intuïtie), maakt dat we het verantwoord vinden om een bepaald risico te lopen. Daarbij vertrouwen we erop dat 'het goed komt', oftewel: de verwachting wordt ingevuld. Vertrouwen is daarmee een emotioneel construct ter compensatie van het gebrek aan kennis/informatie. Daarbij geldt er een verband tussen drie aspecten: de verwachte opbrengst, de waarschijnlijkheid (kans) dat de verwachte opbrengst wordt gerealiseerd en de mate van vertrouwen.

Vertrouwen is de verwachting dat mensen (en middelen) ons niet in de steek laten, ook al is dat mogelijk. De essentie van vertrouwen is dus dat je het risico accepteert dat iets anders kan lopen dan je verwacht/ hoopt.

Iedere keer dat de verwachte opbrengst uitblijft of laag is, brokkelt het gegeven vertrouwen af. Vertrouwen, verwachtingen, emotie en risico-inschatting door gebrek aan informatie zijn met elkaar verbonden. Zonder een goede risico-inschatting is het geven van vertrouwen als het autorijden zonder stuur.

Wil men vertrouwen geven dan is het van belang om goed inzicht te hebben in:

- *De intenties van de ander*. Hoe belangrijk is het voor de een om te voldoen aan de verwachtingen van de ander? In welke mate wil hij daaraan voldoen?
- *De competenties en/of middelen van de ander*. De verwachtingen moeten reëel zijn (hij moet naast de bereidheid om te willen, het ook kunnen).
- *De omstandigheden waarbinnen het realiseren van de verwachtingen zich afspeelt*. Dit onderdeel wordt treffend verwoord door Joris Luyendijk⁷: "Als je binnen vijf minuten buiten kan staan, wordt ook je horizon vijf minuten. Je loyaliteit verdampst; niemand kan ergens op bouwen".

Waarom is vertrouwen waardevol?

In de kritiek op de speech van Terlouw wordt vertrouwen als sentimenteel weggezet en zou in economisch perspectief weinig tot geen waarde hebben. Gedragseconoom

Ruben de Blik⁸ toont echter aan dat vertrouwen economische groei en ontwikkeling teweeg brengt.

De studie laat zien dat mensen met veel vertrouwen in de medemens significant meer per uur/jaar verdienen dan mensen met weinig vertrouwen. Daarnaast levert het verbeteren van het vertrouwen een significante en positieve stijging in inkomen op van 6 tot 9%.

Dit verband wordt geïllustreerd door de volgende formules van Covey & Merrill⁹:

↓ vertrouwen = ↓ snelheid ↑ kosten

Een lager vertrouwen door een gebrek aan kennis/informatie leidt tot lagere snelheid van het proces (realisatie) en hogere kosten. Het vergroten van kennis/informatie kan worden bereikt door het invoeren van regels/controles als mitigerende maatregelen op verwachtingen/risico's. Een nadeel daarvan is echter dat regels de snelheid verlagen en de kosten verhogen. Denk bijvoorbeeld aan de zorgplichtregels jegens de klant, die ertoe hebben geleid dat klanten minder snel worden bediend en de stijging van de kosten van systemen en mensen om deze controles uit te kunnen voeren.

Deze zorgplichtregels ontstonden (grotendeels) door gebrek aan vertrouwen tussen financiële instellingen en de klanten.

↑ vertrouwen = ↑ snelheid ↓ kosten

Een hoger vertrouwen leidt tot een omgekeerde beweging.

De slag naar risicomanagement

Risicomanagement is heden ten dage vrijwel altijd gericht op systemen en weinig op gedrag¹⁰, terwijl twee derde van de risico's voortkomt uit het gedrag van mensen. Bedrijven moeten meer moeite doen om de drijfveren van hun medewerkers te leren kennen. Want, hoe dichter de persoonlijke doelen van de medewerkers bij de doelen van de organisatie liggen, hoe meer vrijheid de medewerkers ervaren en hoe hoger de prestaties zijn. Dat resulteert in een hogere mate van wederzijds vertrouwen en daarmee een lager risico voor de organisatie.

6 Robert Vos en René Witte, *Vertrouwen geven en in control zijn; gaat dat samen?* Ministerie van Financiën, afdeling begrotingszaken, 28 april 2009.

7 Joris Luyendijk, *Dit kan niet waar zijn*, zevende druk, maart 2015.

8 Ruben de Blik, *Empirical Studies on Economic Impact on Trust – Proefschrift*, 21 mei 2015.

9 S. Covey & R. Merrill, *De snelheid van vertrouwen*, Amsterdam: Business Contact. 2008.

10 Kees Cools, Ziende Blind, *bankingreview*, maart 2011.

Daniel Pink¹¹ legt uit dat onze organisaties en onze levens zijn ingericht door het stimuleren van het goede (bijvoorbeeld middels bonussen) en het bestraffen van het slechte (boetes), veelal met veel wetten, regels en controles. Pink geeft zeven redenen waarom dit vaak niet effectief is.

1. Belonen en straffen kan intrinsieke motivatie verminderen.

Een beloning in het vooruitzicht stellen om een taak gedaan te krijgen, de 'als-dan-beloningen', hebben een negatief effect op de intrinsieke motivatie van mensen, doordat ze een gedeelte van hun autonomie moeten opgeven.

2. Belonen en straffen kan prestaties verminderen.

Studies op prestatiebeloningsplannen bevestigen dat hoe hoger de financiële beloning, hoe lager de behaalde resultaten.

3. Belonen en straffen kan creativiteit verminderen.

Beloningen verminderen onze focus op het probleem, waardoor de resultaten verslechteren. Uitzondering hierop zijn de algoritmische taken, waarbij de stappen naar de oplossing vastliggen.

4. Belonen en straffen kan goed gedrag verminderen.

Uit een onderzoek uit 2008 blijkt dat het betalen van bloeddonoren een negatief effect had op het aantal mensen dat bloed wilde doneren.

5. Belonen en straffen kan laksheid en onethisch gedrag bevorderen.

Een bekend voorbeeld: Omdat ouders regelmatig te laat waren met het ophalen van hun kinderen bij een kinderdagverblijf, werd een boete ingesteld voor laatkomers. Het resultaat was dat het aantal laatkomers verdubbelde ten opzichte van de periode voordat de boete was ingesteld. Ouders zagen de boete als een methode om hun schuld af te kopen.

6. Belonen en straffen kan verslavend worden.

Wanneer een beloning eenmaal is aangeboden, dient voor dezelfde taak in de toekomst ook altijd beloond te worden om de motivatie op hetzelfde niveau te houden. Na verloop van tijd worden de beloningen als normaal gezien en zullen de beloningen verhoogd moeten worden om hetzelfde effect te bereiken.

7. Belonen en straffen kan kortetermijndenken in de hand werken.

De beloningen van beursgenoteerde bedrijven is de reden waarom managers zich focussen op kortetermijnresultaten (kwartaalcijfers), waardoor economische zeepbellen ontstaan die op hun beurt tot economische crises leiden.

Pink legt uit dat het geheim van goed presteren, plezier/zin in je leven en werk ligt in de intrinsieke motivatie. Ieder mens heeft de diepe wens om zijn eigen leven te bepalen, nieuwe dingen te leren en te creëren en bij te dragen aan zinvolle zaken. Mensen willen hun talenten inzetten, gewaardeerd worden en de ruimte krijgen. Indien voldaan wordt aan deze condities zal het wederzijdse vertrouwen tussen mensen toenemen.

Vertrouwen als management tool?

Vertrouwen heeft dus, als we Covey en de Blik volgen, 'keiharde' economische waarde. Het leidt tot meer welvaart, lagere kosten, hogere snelheid van realisatie en is een goede motivator voor mensen om 'het goede' te doen. Maar hoe creëren we vertrouwen in een organisatie? Kan vertrouwen geven worden ingezet als een 'tool' voor een succesvolle organisatie? Edgar Karssing¹² beantwoordt deze vraag met 'ja' en formuleert zes concrete handvatten hoe iemand kan investeren in een vertrouwensrelatie.

Handvat 1: Denk na voordat je een belofte doet.

Stel jezelf consequent de vraag: wil ik dit echt beloven en ben ik ook in de situatie om deze belofte na te komen (ligt dit binnen je invloedssfeer)?

Handvat 2: Onthoud wat je belooft.

Wil je een belofte nakomen, dan is het van belang dat je de gedane belofte onthoudt. Juist de gebroken kleine beloften kunnen heel belangrijk zijn voor anderen.

Handvat 3: Doe wat je belooft.

Dit lijkt een open deur, maar is de 'moeder aller gedragingen'. Het is de snelste manier om vertrouwen te winnen.

Handvat 4: Pak lastige kwesties meteen aan.

Het uitstellen van lastige kwesties is niet bevorderlijk voor het vertrouwen. Als deze kwesties snel en op de juiste wijze worden aangepakt/opgelost dan wekt dat vertrouwen.

11 Daniel Pink, *Drive: de verrassende waarheid over wat ons motiveert*, elfde druk, Business Contact.

12 .D.Karssing, *De oplossing is het probleem niet! Reflectie op Ethiek, Integriteit en Compliance*, Capelle aan den IJssel: Nederlands Compliance Instituut 2011.

Handvat 5: Wees recht door zee en respectvol.

Het is vertrouwenwekkend om eerlijk te zijn, mensen te laten weten waar je staat, eenvoudige taal te gebruiken en de dingen bij hun naam te noemen.

Handvat 6: Repareer gebroken beloften.

Als je een belofte hebt gebroken, is het enige juiste dat je kunt doen: je excuses aanbieden en de geleden schade herstellen.

Wat zit er in de toolkit van de compliance officer?¹³

De taken van de compliance officer en de reikwijdte van compliance worden onder meer afgeleid van het integriteitsbeleid van de organisatie en de wet- en regelgeving die de compliance officer als aandachtsgebied heeft. Daarnaast wordt de reikwijdte bepaald door het soort vergunning, de aangeboden diensten, de producten, etc. en door de specifieke risico's die een gevaar opleveren voor de integere bedrijfsvoering van de organisatie. Dit betekent dat de doelstelling van de compliancefunctie per organisatie kan verschillen.

Echter, de doelstelling van de compliancefunctie binnen organisaties kan veelal als volgt worden verwoord: *'het bevorderen en het toezien op de naleving van interne en externe regels die relevant zijn voor de integriteit van de organisatie'*.

Doorgaans worden de taken van een compliance officer afgeleid van de compliancecyclus. Deze taken zijn: vaststellen reikwijdte, faciliteren van de compliancerisico-analyse, adviseren over beleid, uitleggen van beleid, monitoren van beleid en handhaven van beleid.

De compliance toolkit die hieruit voortvloeit, kan bestaan uit:

- Overlegstructuren;
- Een risicoanalysemethode;
- Een monitoringmethode;
- Regels en procedures;
- Een intranetsite over de van toepassing zijnde regels;
- Trainingen en voorlichting;
- Awareness-sessies (incl e-learnings);
- Advies;
- Rapportages.

Een nadere beschouwing van de toolkit leidt tot de volgende bevindingen:

- Het juridisch kader is het uitgangspunt van de taakuitoefening van de compliance officer. Dit is een logische consequentie van de bovengenoemde doelstelling van de compliance functie. Dit leidt tot meer control(e) en daardoor tot minder vertrouwen!
- Bijna alle bovengenoemde elementen uit de toolkit zijn gericht op systemen/ structuren. Dit verlaagt de intrinsieke motivatie en de creativiteit van de medewerkers.
- De onderdelen training en awareness geven ruimte tot reflectie op gedrag en cultuur. Echter, juist deze onderdelen krijgen in de dagelijkse praktijk van de compliance officer de minste aandacht.
- Er bestaat een disbalans in de werkzaamheden van de compliance officer. De taken die gejuridificeerd zijn krijgen de meeste aandacht en de taken die gericht zijn op het verhogen van de motivatie en het vertrouwen krijgen veelal minder aandacht.

Hoewel de compliance officer het bevorderen van de integriteit van de organisatie als zijn taak ziet, leidt de formele juridische invulling van deze taak juist tot het tegengestelde resultaat. Hiermee lijkt de compliance officer onderdeel van het probleem te zijn en niet de oplossing.

De compliance officer dient vertrouwen mede als tool in te zetten voor een effectieve taakuitoefening. Hierbij dient hij vertrouwen als uitgangspunt te nemen, en niet wantrouwen¹⁴:

Dus niet: 'de meeste mensen/organisaties zullen de kluit wel belazeren' of 'alleen doordat wij controleren, houden mensen/organisaties zich aan de regels'.

Maar wel: 'in het algemeen zullen mensen/organisaties zich aan de regels houden. Dit betekent uiteraard niet dat iedereen zich altijd aan alle regels/afspraken zal houden, maar wel dat het in het algemeen om uitzonderingen zal gaan'. Hiermee wordt het 'touwjtje' een onderdeel van de toolkit van de compliance officer.

Sharda Poelloe is zelfstandige risk & compliance professional. Zij heeft ruime ervaring in verschillende functies bij banken en verzekeraars.

¹³ Handboek Compliance Professional 2015-2016 hoofdstuk 2, Nederlands Compliance Instituut.

¹⁴ Robert Vos en René Witte, *Vertrouwen geven en in control zijn; gaat dat samen?* Ministerie van Financiën, afdeling begrotingszaken, 28 april 2009.

Onderzoeksresultaten over de inrichting van de compliance-functie bij Nederlandse financiële ondernemingen

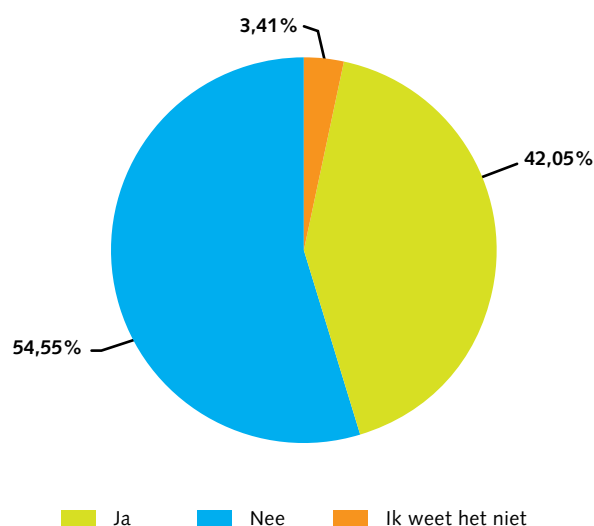
Cora Wielenga en Anne Denies

In oktober 2016 heeft de EBA nieuwe richtlijnen ter wijziging van haar bestaande richtlijnen voor interne governance gepubliceerd, die van toepassing zijn op banken en beleggingsondernemingen.¹ Dit riep bij ons de vraag op over hoe de inrichting van de compliancefunctie bij Nederlandse financiële ondernemingen er op dit moment uitziet. In hoeverre voldoen Nederlandse financiële ondernemingen al aan de nieuwe standaard die vanuit EBA is voorgesteld? Wij hebben compliance officers van banken, verzekeraars, financieel dienstverleners, beleggingsondernemingen, beleggingsinstellingen en betaalinstanties een aantal vragen voorgelegd om inzicht te krijgen in de wijze waarop de compliancefunctie nu is ingericht. De gestelde vragen zijn mede gebaseerd op de nieuwe regels van de EBA². Daarnaast hebben wij een aantal vragen toegevoegd die voortvloeien uit onze adviespraktijk. Het onderzoek is slechts op kleine schaal uitgevoerd.³ De belangrijkste uitkomsten van het onderzoek zullen in dit artikel besproken worden.

Commerciële activiteiten

Verrassend is dat in veel organisaties de bestuurder die verantwoordelijk is voor compliance dikwijls ook verantwoordelijk is voor commerciële activiteiten van de onderneming. Dit is niet wenselijk; voor banken en beleggingsondernemingen rust hier zelfs een verbod op in de nieuwe richtlijnen van de EBA. Een derde van de compliance officers bij banken geeft te kennen dat binnen hun organisatie nog steeds sprake is van deze constructie. Deze banken zullen dus nog aan de slag moeten om hier verandering in aan te brengen. Het resultaat is positiever bij de compliance officers van beleggingsondernemingen die hebben meegewerkt aan het onderzoek. Binnen deze

Is de bestuursfunctionaris die verantwoordelijk is voor compliance ook verantwoordelijk voor commerciële activiteiten in de onderneming?



1 Aan het onderzoek werkten 88 respondenten mee.

2 Zie ook het artikel 'Nieuwe governance-regels voor financiële ondernemingen' elders in deze editie.

3 Aan het onderzoek werkten 88 respondenten mee.

organisaties is de voor compliance verantwoordelijke bestuursfunctionaris niet verantwoordelijk voor commerciële activiteiten.

Rapportage

Op grond van de nieuwe richtlijnen van de EBA geldt dat de compliancefunctie direct aan het bestuur dient te rapporteren. Van de financiële ondernemingen waar direct gerapporteerd wordt aan de raad van bestuur, vindt dit in de helft van de gevallen per kwartaal plaats. De overige antwoorden lopen uiteen, van maandelijks tot jaarlijks. Wij adviseren compliance officers om minimaal één keer per kwartaal een rapportage uit te brengen aan de raad van bestuur. Het is dus een mooi resultaat dat hier bij veel ondernemingen reeds sprake van is. Wanneer slechts op jaarlijkse basis gerapporteerd wordt, loopt de raad van bestuur het risico te weinig op de hoogte te zijn van de actuele stand van zaken op compliancegebied. Dit kan ertoe leiden dat het bestuur niet adequaat kan sturen op compliancerisico's. Het onderzoek toont aan dat bijna alle compliance officers die rapporteren, ook de mogelijkheid krijgen om deze rapportage mondeling toe te lichten.

Naast directe rapportage aan het bestuur dienen banken en beleggingsondernemingen op grond van de nieuwe EBA-regels ook direct te rapporteren aan de raad van commissarissen. In het eerder verschenen artikel over de gevolgen van deze richtlijn stelden Hanne Wanders en Cora Wielenga dat deze functionarissen doorgaans al een directe rapportagelijijn hebben naar de raad van commissarissen.⁴ Gelukkig blijkt dit in 65% van de gevallen ook aan de orde te zijn. Meestal vindt rapportage eens in de drie maanden plaats en wordt de gelegenheid geboden om deze mondeling toe te lichten. Dit is prima, want zo blijft ook de raad van commissarissen op de hoogte van de actuele stand van zaken. Uit het onderzoek blijkt dat wanneer slechts één keer per jaar of helemaal niet gerapporteerd wordt, de compliance officers van mening zijn dat de raad van commissarissen niet helemaal toegankelijk is, omdat er sprake is van een te hoge drempel. Door (vaker) te rapporteren aan de raad van commissarissen zou dit gevaar weggenomen kunnen worden. Voor een deel van de ondernemingen is het overigens niet verplicht om een raad van commissarissen in te stellen.⁵

De rol van de raad van commissarissen

In de nieuwe EBA-richtlijnen wordt meer nadruk gelegd op de rol van raad van commissarissen. Uit het onderzoek is naar voren gekomen dat ongeveer de helft van de respondenten met de raad van commissarissen spreekt zonder het bijzijn van de raad van bestuur. Meestal vindt dit eens in de drie maanden of eens in het jaar plaats. Dit is zeker positief, maar mag nog groeien. Het blijkt namelijk uit ons onderzoek dat compliance officers die spreken met de raad van commissarissen zonder dat het bestuur aanwezig is, zich een stuk vrijer voelen om de raad van commissarissen op elk moment te benaderen, omdat er sprake is van een kortere lijn.

Het onderzoek toont aan dat voor de raad van commissarissen veelal een rol is weggelegd in geval van de benoeming, overplaatsing, schorsing dan wel het ontslag van de hoogstgeplaatste compliance officer. Doorgaans is deze rol van instemmende aard. Toch geeft een aantal compliance officers aan dat binnen hun onderneming de raad van commissarissen een adviserende of informerende rol heeft. In de oude richtlijnen was het alleen verplicht om de raad te informeren over de aanstelling, overplaatsing of ontslag. In de nieuwe richtlijnen wordt het voor banken en beleggingsondernemingen verplicht om de raad van commissarissen in een dergelijke situatie een instemmende rol toe te kennen. Ongeveer 20% van de banken en beleggingsondernemingen geeft te kennen dat de raad van commissarissen nog geen rol heeft met betrekking tot de benoeming, overplaatsing dan wel ontslag van de hoogstgeplaatste compliance officer. Voor deze ondernemingen is het noodzakelijk om de raad van commissarissen een rol in het benoemingsproces van het hoofd compliance te geven.

Naast de klassieke commissies in de raad van commissarissen mogen op grond van de EBA-richtlijnen ook andere commissies benoemd worden. Wij waren positief verrast door het feit dat bijna een vierde van de compliance officers aan heeft gegeven dat binnen de raad van commissarissen van hun onderneming een commissie is benoemd die gericht is op ethiek en gedrag en/of compliance. Dit is een mooi resultaat, omdat het inhoudt dat de betrokkenheid vanuit de raad van commissarissen op het gebied van ethiek, gedrag en compliance groter aan het worden is.

4 H. Wanders en C. Wielenga, 'Gevolgen van de conceptrichtlijnen over interne governance bij banken en beleggingsondernemingen', 10 januari 2017.

5 Het instellen van een raad van commissarissen is verplicht voor

structuurvennootschappen. Daarnaast kan bij statuten bepaald worden dat er een raad van commissarissen is.

Het zou mooi zijn als dit percentage de aankomende jaren nog verder zou stijgen.

Vastleggen en auditen van de compliancefunctie

De nieuwe regels van EBA verplichten het opstellen van een complianceprogramma. In een complianceprogramma, of een soortgelijk document, wordt het geheel aan activiteiten om de compliandoelestellingen van de organisatie te realiseren vastgelegd. Door een complianceprogramma op te stellen, creëert de instelling een duidelijk beeld van de wijze waarop de compliancefunctie in de brede zin van het woord is ingericht. Het is goed om te zien dat, op een enkele respondent na, iedereen aangeeft over een complianceprogramma te beschikken. De compliance officers die stellen dat hun organisatie geen complianceprogramma kent, geven allemaal aan dit wel wenselijk te vinden.

Opmerkelijk is dat een vierde van de compliance officers verklaart dat de compliancefunctie niet periodiek geaudit wordt. Ook dit is verplicht in de nieuwe richtlijnen. Bij het auditen van de compliancefunctie wordt het functioneren van de compliancefunctie onderzocht. Er wordt getoetst of de compliancefunctie voldoet aan de doelstellingen die in het complianceprogramma zijn vastgelegd. Het is wenselijk om dit op jaarlijkse basis te doen.

Three lines of defence

De meeste financiële ondernemingen werken met het 'three lines of defence'-model, waarbij het management de eerste lijn vormt, risk en compliance de tweede en de interne audit de derde lijn. De vraag of er binnen de onderneming eerstelijnscompliancefunctionarissen zijn ingesteld, is voornamelijk door compliance officers bij banken en verzekeraars positief beantwoord. Bij de financieel dienstverleners (niet zijnde banken en verzekeraars) is helemaal geen sprake van dergelijke functionarissen. Ondanks dat het niet verplicht is om eerstelijnscompliancefunctionarissen in te stellen, kan het helpen met het verwezenlijken van de compliance-doelstellingen van een organisatie om in de eerste lijn compliancefunctionarissen of -aanspreekpunten te benoemen. Er ontstaat dan namelijk een kortere lijn tussen de compliancefunctie en de eerste lijn.

De compliancefunctie wordt veelal gecombineerd met de afdeling riskmanagement, de juridische afdeling of de privacyfunctie van de organisatie. Opvallend is dat relatief veel compliance officers verklaren dat de compliancefunctie wordt gecombineerd met de afdeling audit. Audit hoort thuis in de derde lijn, waardoor het niet wenselijk is om deze functie te combineren met compliance. Op grond van de nieuwe richtlijnen van EBA is het voor sommige

De betrokkenheid vanuit de raad van commissarissen op het gebied van ethiek, gedrag en compliance wordt steeds groter

organisaties toegestaan om de compliancefunctie te combineren met de risicofunctie. Welke organisaties dit zijn, wordt beoordeeld met het oog op proportionaliteit. De interne auditfunctie mag, ongeacht de complexiteit van de organisaties, nooit gecombineerd worden met een andere risicobeheersende functie.

Onafhankelijk meldpunt

Het hoge aantal compliance officers dat aangeeft dat er een onafhankelijk meldpunt is ingericht waar medewerkers een vermoeden van een overtreding kunnen melden, is zeer positief. Een organisatie met meer dan vijftig werknemers is op grond van de Wet Huis voor klokkenluiders verplicht een onafhankelijk meldpunt in te richten waar medewerkers, buiten de standaardrapportagelijnen om, een vermoeden van een overtreding kunnen melden.⁶ Ook op grond van de nieuwe EBA-richtlijnen wordt dit meldpunt verplicht. In deze richtlijnen wordt gesteld dat dit de compliance officer, audit of een meldpunt uit de klokkenluidersregeling kan zijn. Uit het onderzoek blijkt dat in de helft van de gevallen het meldpunt een vertrouwenspersoon is. Naar onze mening is dit de beste optie, omdat de vertrouwenspersoon in de meeste gevallen geheimhouding kan toezeggen. Een ander veelgehoord antwoord is de compliance officer. Wanneer de compliance officer het meldpunt is, kan dit voor spanning zorgen, omdat de compliance officer een meldplicht aan de externe toezichthouder kent op grond van de incidentenregeling. Hierdoor kan hij geheimhouding dus niet te allen tijde garanderen. Indien sprake is van een melding op grond van de klokkenluidersregeling kan de compliance officer dan in een onwenselijke situatie terecht komen.

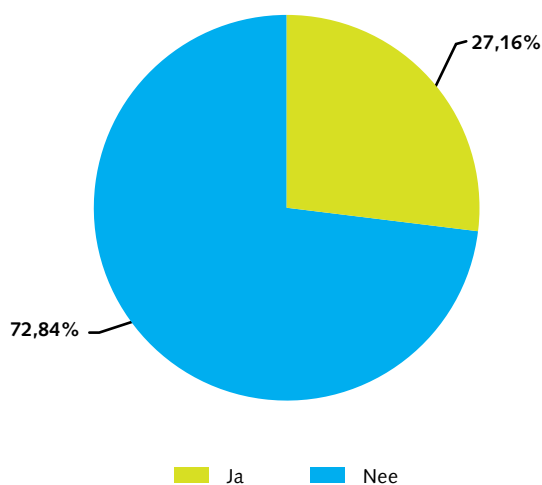
⁶ Wet Huis voor klokkenluiders.

Banken en beleggingsondernemingen met minder dan vijftig werknemers zijn op grond van de nieuwe richtlijnen overigens ook verplicht een meldpunt in de richten.

Vergoeding

Het heeft ons zeer verrast dat bijna een derde van de ondervraagde compliance officers aangeeft dat een deel van hun vergoeding afhankelijk is van de financiële resultaten van de onderneming. Voor de meeste respondenten betreft dit 1% tot 15% van de vergoeding. Een aantal compliance officers stelt echter dat hun vergoeding voor 16% of meer afhankelijk is van de financiële resultaten van de onderneming. Op grond van de nieuwe EBA-richtlijnen is dit voor zowel banken als beleggingsondernemingen verboden. In deze richtlijnen staat dat de bezoldiging van de compliance-functie niet gekoppeld mag zijn aan de resultaten van de activiteiten die zij monitoren en controleren. Gelukkig geven de meeste compliance officers van deze ondernemingen ook aan dat hier binnen hun organisatie geen sprake van is. De regel uit de EBA-richtlijnen is echter niet nieuw. Op grond van de Regeling beheerst beloningsbeleid geldt reeds dat de beloning van compliance officers bij banken onafhankelijk van de resultaten van de bedrijfsactiviteiten waar ze toezicht op houden moet zijn.⁷ De compliance officer dient onafhankelijk en objectief te zijn. Het is dan niet bevorderlijk om zijn vergoeding afhankelijk te maken van de resultaten van de onderneming. Daarom adviseren wij alle financiële ondernemingen om de vergoeding van de compliance officer niet (ook niet voor een deel) afhankelijk te maken van de financiële resultaten van de onderneming.

Is (een deel van) uw vergoeding afhankelijk van de financiële resultaten van de onderneming?



Tot slot

Ons onderzoek geeft een beeld van de manier waarop de compliancefunctie bij verschillende Nederlandse financiële ondernemingen er op dit moment uitziet. Op veel vlakken voldoen deze ondernemingen al aan de nieuwe standaard die vanuit EBA is voorgesteld. Natuurlijk is er ook ruimte voor verbetering.

De uitkomsten van het onderzoek hebben ons op een aantal vlakken positief verrast. Zo rapporteren veel compliance officers per kwartaal direct aan de raad van bestuur én aan de raad van commissarissen. Door de raad van commissarissen te betrekken bij compliance wordt de kloof tussen de compliancefunctie en de raad van commissarissen kleiner. Dit kan door middel van rapportage, regelmatig een gesprek te voeren (zonder de aanwezigheid van het bestuur) of door een commissie te benoemen die gericht is op ethiek en gedrag en/of compliance. In veel financiële ondernemingen is er op die manier al betrokkenheid van de raad van commissarissen. Daarnaast kennen de meeste ondernemingen een onafhankelijk meldpunt waar medewerkers, buiten de standaardrapportagelijnen om, een vermoeden van een overtreding kunnen melden. Veelal is de vertrouwenspersoon het meest wenselijke aanspreekpunt.

Een aantal zaken heeft verbetering nodig. Het is niet de bedoeling dat de bestuurder die verantwoordelijk is voor compliance, ook verantwoordelijkheden kent op commercieel gebied. Voor de financiële ondernemingen waar dit (nog) wel het geval is, is het raadzaam om verandering aan te brengen in de verdeling van taken onder bestuurders. Voor banken en beleggingsondernemingen is dit verplicht op grond van de nieuwe EBA-richtlijnen. Daarnaast auditen veel ondernemingen hun compliancefunctie niet en wordt de compliancefunctie nog te vaak met andere functies gecombineerd. Wij adviseren de ondernemingen die de compliancefunctie combineren met de auditfunctie, de three lines of defence strikter te handhaven. Daarnaast adviseren wij financiële ondernemingen om de bezoldiging van compliance officers niet afhankelijk te laten zijn van de financiële resultaten van de ondernemingen.

Cora Wielenga is directeur van het Nederlands Compliance Instituut. Eén van haar kennisgebieden is governance. Anne Denies heeft zowel ondernemingsrecht als financieel recht gestudeerd en is stagiaire bij het Nederlands Compliance Instituut.

⁷ Artikel 9 Regeling beheerst beloningsbeleid Wft 2014.

Het risicoconcept; een inhoudsloze mantra of een pseudoniem voor (meer) onzekerheid?

Björn Schuitemaker & Albert de Jong

De gelekte documenten van een juridisch advieskantoor die de animo voor het belangrijkste verhullingsproduct aan de kaak stellen, de verlichte sanctieregimes die voormalige schurkenstaten weer toelaten tot het internationale betalingssysteem, het referendum dat de top tien financiële centra doet wijzigen, de commerciële president die de deregulering van de financiële sector in gang zet en Bob Dylan die de Nobelprijs voor de literatuur niet ophaalt. Eén voor één voorbeelden van recente ontwikkelingen die de gemoederen bezig houden. Echter, zoals een folkzanger met een rock-'n-roll attitude al vele jaren over tijden zingt: *they are a-changin'*, met inbegrip van moraliteit.

De gemeenschappelijke noemer van voornoemde ontwikkelingen is dat ze elk effect hebben op het realiseren van doelstellingen, of – in de woorden van NEN-ISO¹ – een risico vormen. In het vervolg van deze bijdrage wordt eerst het schade- en het risicodiagram uit het oeuvre van Viaene besproken. Daarna wordt beknopt de brainstorm, de bow-tie-analyse en de Delphi-techniek uiteengezet en tot slot wordt afgesloten met de conclusie. Dit vanuit de optiek dat iedereen die zich in de discipline van compliance wil inwijden wordt geconfronteerd met een overvloed aan risico gerelateerde begrippen, variërend van witwasrisico's tot uitbestedingsrisico's, en een guideline die volgens DNB² een aanpak biedt voor het inzichtelijk maken van al deze integriteitrisico's tezamen: de systematische integriteitrisicoanalyse(SIRA).

Het schadediagram

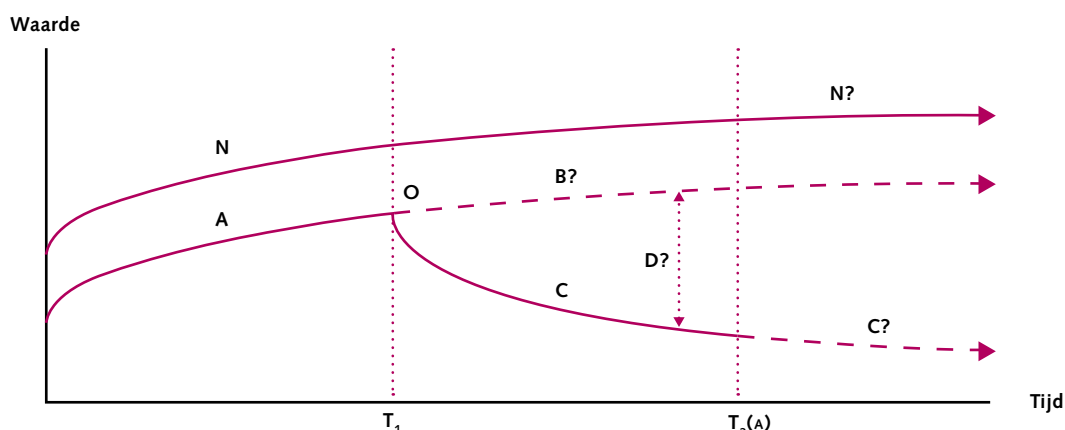
Over schade wordt meestal keurig in twee woorden gesproken, namelijk: *schade aan* (iets). Bijvoorbeeld *schade aan* de cliënten, *schade aan* de onderneming of *schade aan* de financiële markten et cetera. Het aantal schadeobjecten is hier herleid tot het inhoudsloze woord 'iets', maar is in de praktijk te verscheiden om het zinvol te kunnen benoemen. Derhalve interesseert het inhoudelijke aspect van schade ons niet in deze bijdrage. Wel interessant is het beeld dat alle beschadigde objecten gemeen hebben. Dit beeld kan visueel worden voorgesteld in het schadediagram (figuur 1).

Het schadediagram bestaat in essentie uit zeven elementen, met het waardeverlies (y-as) en het tijdsverloop (x-as) als inherente dimensies.³ Het eerste element betreft de voorafgaande toestand (A), deze geeft de waarde op

1 ISO. (2014). *ISO 19600: Compliance management systems – guidelines*. Geneva: International Organization for Standardization.

2 DNB. (2015). *De integriteitrisicoanalyse: Meer waar dat moet, minder waar dat kan*. Amsterdam: De Nederlandsche Bank.

3 Viaene, J. (2014). Inleiding tot de veiligheidstheorie. In A. van Regenmortel & K. Reyniers, *Syllabus juridische aspecten inzake welzijn op het werk* (pp. 2-38). Universiteit Antwerpen.



Figuur 1. Het schadediagram, aangepast overgenomen uit: Viaene, J. (2015). *Inleiding in de preventieleer van Jos Viaene*. In J. Buelens, K. Reyniers, I. v. Puyvelde, A. v. Regenmortel, & V. Vervliet, *Handboek welzijn op het werk: Juridische aspecten* (pp. 11). Brugge: Die Keure.

verschillende tijdstippen aan evenals de trend die daaruit voortvloeit. Het tweede element betreft de *hypothetische* voortzetting van de voorafgaande toestand (B?). Dit element is per definitie onzeker, maar kan enerzijds worden vermoed uit de trend die in A aanwezig is en anderzijds uit de vorm van het derde element: het normale waardeverloop van gelijksoortige objecten in dezelfde tijd (N). Het vierde element betreft de oorzaak (O). Dit element is doorgaans het gevolg van samenlopende factoren in tijd en ruimte⁴, of meer theoretisch geformuleerd: een onvoldoende, maar noodzakelijk deel van een voorwaarde die zelf niet noodzakelijk maar voldoende is voor het ontstaan van de schade.^{5,6} Het vijfde (C) en het zesde (C?) element hebben vervolgens betrekking op het verloop van de beschadigde toestand. Deze elementen kunnen zich acuut of geleidelijk ontwikkelen en zowel voor als na de actualiteit (a) liggen. Het zevende element betreft tot slot de schade (D?). Dit element volgt niet uit de vergelijking tussen een voorafgaande betere toestand (A) en een

daaropvolgende slechtere toestand (C), maar uit het verschil tussen de *hypothetische* toestand die zonder de schade zou hebben bestaan (B?) en de *reële* toestand die door de schade is ontstaan (C). Dit brengt met zich mee dat de omvang van de schade principieel onzeker is.⁷

Het risicodiagram

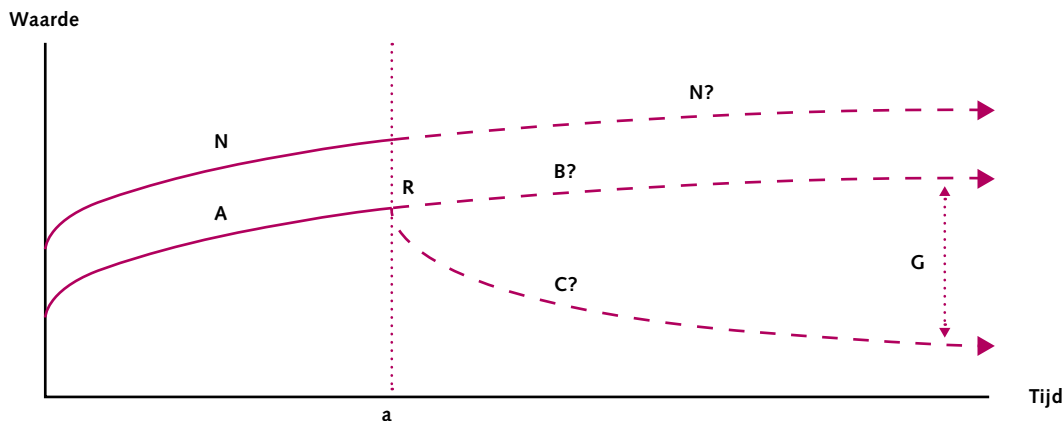
De elementen van het risicodiagram (figuur 2) zijn vrij gemakkelijk uit het schadediagram (figuur 1) af te leiden. Dit omdat de verschillen tussen de diagrammen in slechts één verandering zijn gelegen, te weten: het moment van de actualiteit.⁸ De actualiteit (a) wordt namelijk teruggedraaid tot vlak voor de oorzaak van de schade, waardoor een aantal elementen hun realiteitswaarde verliezen en daarom een andere naam krijgen. Zo staan de oorzaak (O) en het risico (R) op dezelfde plaats in het diagram, met het verschil dat de oorzaak aan het begin van een *reële* schade staat en het risico aan het begin van een *hypothetische* schade, oftewel gevaar. Het gevaar (G) is bijgevolg te definiëren als het verschil tussen het *hypothetische* verloop van het onbeschadigde waardeverloop (B?) en het *hypothetische* verloop van het beschadigde waardeverloop (C?). De elementen van het risicoconcept zijn tezamen weergegeven in het risicodiagram.

4 Viaene, J. (2014). Inleiding tot de veiligheidstheorie. In A. van Regenmortel & K. Reyniers, *Syllabus juridische aspecten inzake welzijn op het werk* (pp. 2-38). Universiteit Antwerpen.

5 Mackie, J. (1980). *The Cement of the Universe: A Study of Causation*. Oxford: Oxford University Press.

6 Zo is kortsluiting in de betekenis van: a) noodzakelijke voorwaarden niet de oorzaak, omdat andere oorzaken eveneens tot brand kunnen leiden, b) voldoende grond niet de oorzaak aangezien branden niet ontstaan wanneer de andere voorwaarden van de branddriehoek niet worden beantwoord en c) verzameling van voorwaarde wel de oorzaak (Mackie, 1980).

7 Viaene, J. (2014). Inleiding tot de veiligheidstheorie. In A. van Regenmortel & K. Reyniers, *Syllabus juridische aspecten inzake welzijn op het werk* (pp. 2-38). Universiteit Antwerpen.



Figuur 2. Het risicodiagram, aangepast overgenomen uit: Viaene, J. (2015). *Inleiding in de preventieleer van Jos Viaene*. In J. Buelens, K. Reyniers, I. v. Puyvelde, A. v. Regenmortel, & V. Vervliet, *Handboek welzijn op het werk: Juridische aspecten* (pp. 15). Brugge: Die Keure.

Het risicoconcept wordt overigens in de regel uitgelegd als het product van waarschijnlijkheid en consequenties⁹, waarbij de taalpurist zal opperen dat de term waarschijnlijkheid refereert aan de Engelse term 'likelihood'. Deze Engelse term duidt in tegenstelling tot de term 'probability' niet op de statistische kans, maar op de kans die op veronderstellingen is gebaseerd.¹⁰ Vervolgens kan de waarschijnlijkheidsfactor nog worden genuanceerd als de samenloop van dreigingen (T) en kwetsbaarheden (V). Dit betekent dat risico's zich manifesteren wanneer een kwetsbaarheid door een dreiging wordt benut.¹¹

De risicoanalysetechnieken

Een goed begrip van voorgaande risicoterminologie is onder meer van belang voor de keuze van een adequate risicoanalysetechniek. Thans wordt veelal een afgeleide of combinatie van de brainstorm of de Delphi-techniek gehanteerd voor het uitvoeren van de SIRA. Deze technieken lenen zich uitstekend voor het identificeren van

risico's.¹² Echter, voor de risicoanalyse en -evaluatie zijn aanvullende technieken nodig zoals bijvoorbeeld de bow-tie-analyse. In het vervolg van deze paragraaf worden de brainstorm, de Delphi-techniek en de bow-tie-analyse kort toegelicht.

Volledigheidshalve wordt opgemerkt dat de risico-beoordeling uit drie processen bestaat, namelijk: risico-identificatie, risicoanalyse en risico-evaluatie. Daarbij heeft: het risico-identificatieproces betrekking op het onderkennen van de risico's, het risicoanalyseproces op het begrijpen van de aard van het risico en het vaststellen van het risiconiveau en het risico-evaluatieproces op het vergelijken van de resultaten van de risicoanalyse met de (vooraf gedefinieerde) risicoattitude van de organisatie om vast te stellen of het risico acceptabel is.¹³ Deze risicobeoordeling wordt overigens voorafgegaan door het vaststellen van de context en gevolgd door het behandelen van het risico. Het laatste refereert aan handelingsperspectieven, zoals bijvoorbeeld het vermijden, verminderen, overdragen of accepteren van het (rest)risico.¹⁴

8 Viaene, J. (2015). *Inleiding in de preventieleer van Jos Viaene*. In J. Buelens, K. Reyniers, I. v. Puyvelde, A. v. Regenmortel, & V. Vervliet, *Handboek welzijn op het werk: Juridische aspecten* (pp. 9-19). Brugge: Die Keure.

9 Hillson, D. (2006). *The risk management universe: A guided tour*. London: British Standards Institution.

10 ISO-IEC. (2009). *ISO/IEC 31010: Riskmanagement – Risk assessment techniques*. Geneva: International Organization for Standardization.

11 International Monetary Fund. (2001). *Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) – Report on the Review of the Effectiveness of the Program*. Washington: IMF.

12 ISO-IEC. (2009). *ISO/IEC 31010: Riskmanagement – Risk assessment techniques*. Geneva: International Organization for Standardization.

13 ISO. (2009). *Risk management – principles and guidelines*. Geneva: International Organization for Standardization.

14 ISO. (2009). *Risk management – principles and guidelines*. Geneva: International Organization for Standardization.

Risikoanalyse techniek	Risicobeoordeling				
	Risiko-identificatie	Risikoanalyse			
		Waarschijnlijkheid	Consequentie	Risiko-niveau	Risiko-evaluatie
Brainstorm	SA ¹⁵	NA ¹⁶	NA	NA	NA
Delphi	SA	NA	NA	NA	NA
Bow-tie-analyse	NA	SA	A ¹⁷	SA	A

Tabel 1. Toepasbaarheid van drie risicoanalysetechnieken.¹⁸

BRAINSTORM

De brainstorm refereert in de volksmond aan elk type groepsdiscussie. Echter, om te stimuleren dat het voorstelingsvermogen wordt getriggerd door de gedachtegangen en de stellingen van andere deelnemers, behoort de brainstorm bepaalde randvoorwaarden te beantwoorden.

Deze randvoorwaarden zijn volgens ISO-IEC¹⁹:

- Een aantal thema's²⁰ en scenario's worden voorafgaand aan de brainstorm voorbereid.
- De doelstellingen worden vooraf gedefinieerd en de spelregels worden toegelicht.
- De initiatiefnemer begint met het delen van zijn gedachtegang, waarna de deelnemers ideeën verkennen.
- De ingevingen worden niet ter discussie gesteld om het vrije denken te stimuleren.
- De organisator introduceert een nieuw thema wanneer de discussie dreigt uit te putten of teveel dreigt af te dwalen van de doelstelling.
- De ingevingen die uit de brainstorm voortkomen worden vastgelegd.

Bij de brainstorm ligt het accent op het voorstellingsvermogen van de deelnemers, waardoor deze techniek zich in het bijzonder leent voor het identificeren van risico's en beheersmaatregelen wanneer nieuwe producten, diensten,

klanttypen, afzetkanalen of jurisdicties et cetera worden aangesproken. De brainstorm heeft evenwel als nadeel dat de deelnemers onvoldoende kennis en ervaring kunnen hebben om tot adequate inzichten te komen, de volledigheid moeilijk is aan te tonen vanwege het relatief ongestructureerde karakter, en de brainstorm door bepaalde deelnemers kan worden gedomineerd vanwege groepsprocessen.²¹

DELPHI-TECHNIEK

Een andere techniek die sterk leunt op het identificeren van risico's is de Delphi-techniek. Deze techniek is in essentie een schriftelijke brainstormmethode die uit een drietal vragenlijstrondes bestaat. In de eerste ronde wordt de deelnemers gevraagd om op een aantal ongestructureerde vragen te reageren. Bijvoorbeeld: 'Op welke wijze kan non-compliance zich manifesteren op het gebied van (inter)nationale sanctieregelgeving?' Uit deze ronde kunnen de scenario's worden gedestilleerd die vervolgens in een Likert-vragenlijst²² kunnen worden vertaald voor de tweede ronde. Tijdens deze ronde wordt de deelnemers gevraagd om hun antwoorden te motiveren. De individueel gegeven antwoorden zullen voor bepaalde scenario's (sterk) verschillen, waardoor de deelnemers in de derde ronde wordt gevraagd om de vragenlijst opnieuw in te vullen voor de vragen die het meest uiteenlopend werden beantwoord. Echter, ditmaal hebben de respondenten informatie over de gemiddelde scores op elk vraag, de spreiding van de antwoorden en de motiveringen die de andere deelnemers bij de antwoorden hebben gegeven. De Delphi-techniek laat met andere woorden toe om consensus over de materie te verkrijgen, doordat de deelnemers individueel

15 Strongly applicable.

16 Not applicable.

17 Applicable.

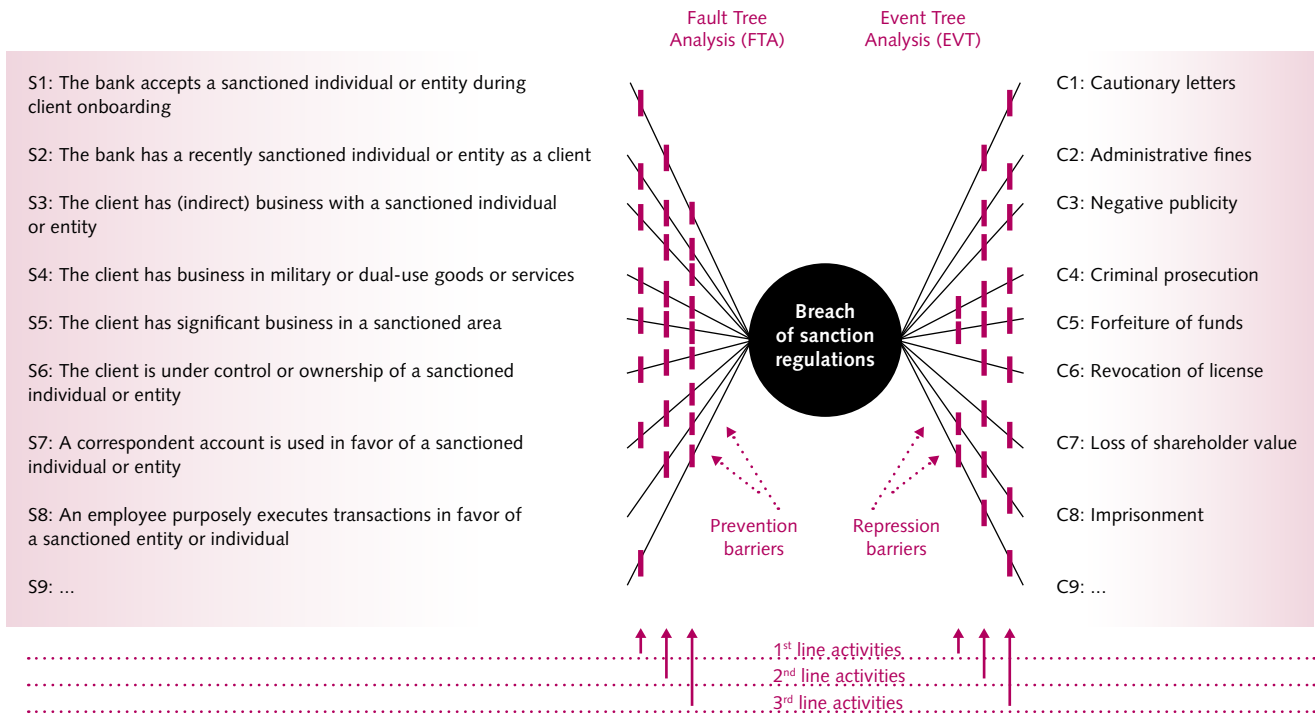
18 Aangepast overgenomen uit ISO-IEC (2009). ISO/IEC 31010: *Riskmanagement - Risk assessment techniques*. Geneva: International Organization for Standardization.

19 ISO-IEC. (2009). ISO/IEC 31010: *Riskmanagement - Risk assessment techniques*. Geneva: International Organization for Standardization.

20 Voorbeelden van integriteitthema's zijn: witwassen, terrorisme-financiering, sanctieregelgeving, corruptie, (interne) fraude, agressieve belastingplanning, marktmanipulatie en cybercrime (DNB, 2015).

21 ISO-IEC. (2009). ISO/IEC 31010: *Riskmanagement - Risk assessment techniques*. Geneva: International Organization for Standardization.

22 Bij een likert-schaal geeft de respondent aan in hoeverre hij het eens is met de stelling, bijvoorbeeld op een vijfpuntsschaal van 'helemaal mee eens' tot 'helemaal mee oneens'.



Figuur 3. Voorbeeld van een bow-tie-diagram, toegepast op sanctiescenario's voor een handelsbank.

hun opinies delen en tegelijk kennis hebben van de opinies van de andere deelnemers. Desgewenst kunnen meerdere rondes worden geïntroduceerd.²³

BOW-TIE-ANALYSE

In aanvulling op de brainstorm of de Delphi-techniek kan de bow-tie-analyse worden gebruikt voor het uitvoeren van de risico-evaluatie en risicobeoordeling. De bow-tie-analyse combineert in feite de 'fault tree analysis' (FTA)²⁴ met de 'event tree analysis' (EVT)²⁵ en genereert als output een eenvoudig diagram waarin zowel de faalpaden (failure pathways) als de beheersmaatregelen (barriers) zijn aangegeven om de gevolgen van (hypothetische) schade te voorkomen dan wel te beheersen.²⁶ Ter illustratie is in figuur 3 een bow-tie-diagram opgesteld voor het SIRA-thema 'sanctieregelgeving'.

De barrières in de bow-tie-analyse (figuur 3) bestaan bijvoorbeeld uit pre-event transaction monitoring (links) en post-event transaction filtering (rechts). Andere voorbeelden aan de *preventieve zijde* zijn: het verkrijgen van inzicht in de eigendoms- en zeggenschapstructuur tijdens het client-onboarding-process, of het controleren van het type goederen, de eind-gebruiker en de vrachtroute et cetera bij het verlenen van documentaire kredieten. Andere voorbeelden aan de *repressieve zijde* zijn: audit trails, sanctieclausules, meldingen, voluntary-self-disclosures of schikkingen. Op de barrières aan beide zijden kan vervolgens het three-lines-of-defence-principe worden toegepast. De hoofdlijnen hiervan zijn weergave in figuur 4.

In een laatste stap kan eventueel nog de effectiviteit van de barrières worden bepaald aan de hand van de layer of protection analyses (LOPA), zodat de schaarse bedrijfsmiddelen aan de meest kritische layers of protection worden toegewezen.²⁷

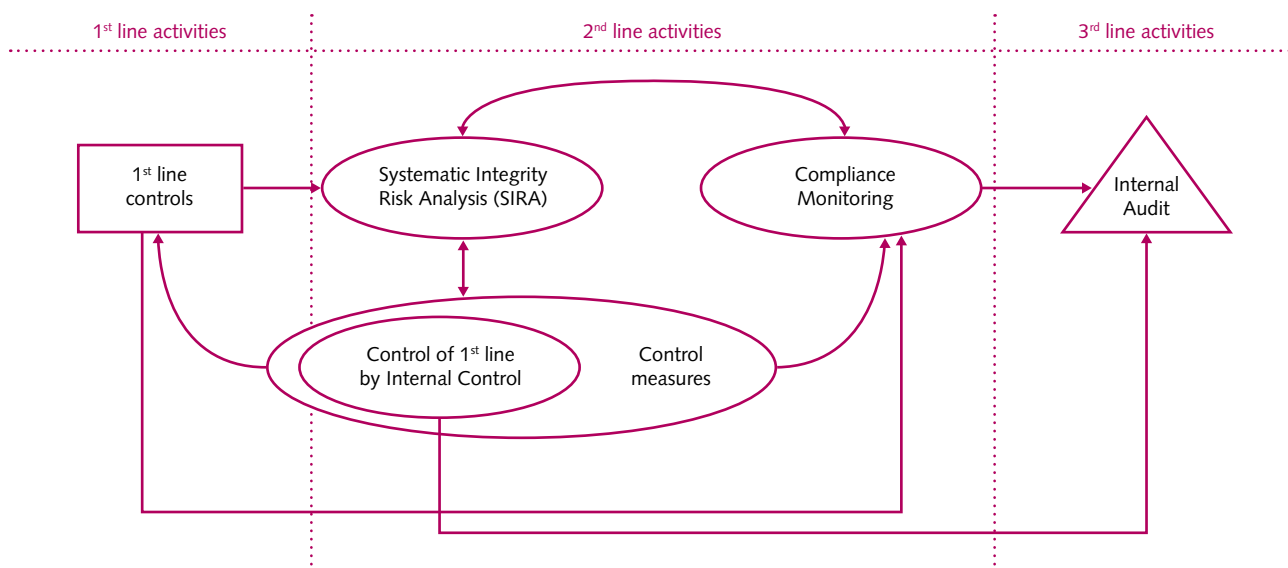
23 ISO-IEC. (2009). ISO/IEC 31010: *Riskmanagement – Risk assessment techniques*. Geneva: International Organization for Standardization.

24 Hierbij wordt voor een bepaalde ongewenste gebeurtenis een foutenboom geconstrueerd; deze bestaat uit logische poorten, een reeks gebeurtenissen die tot het top event leiden en uit basisoorzaken waarvan de faalkansen beschikbaar zijn.

25 Hierbij wordt vanuit een gebeurtenis vertrokken, waarna systematisch alle mogelijke combinaties en gevolgen worden onderzocht.

26 ISO-IEC. (2009). ISO/IEC 31010: *Riskmanagement – Risk assessment techniques*. Geneva: International Organization for Standardization.

27 ISO-IEC. (2009). ISO/IEC 31010: *Riskmanagement – Risk assessment techniques*. Geneva: International Organization for Standardization.



Figuur 4. SIRA- en compliance monitoring cyclus in het three-lines-of-defence model.

Conclusie

Risico's hebben effect op het behalen van geformuleerde doelstellingen, wat betekent dat ze zonder positieve dan wel negatieve consequenties überhaupt niet bestaan. Echter, het begrip risico dreigt abusievelijk synoniem te raken met een aantal aanverwante begrippen, terwijl een goed begrip van de risicoterminologie van belang is voor iedereen die zich in de discipline van compliance wil inwijden. Deze terminologische verwarring is voornamelijk ingegeven door het gemis aan het principiële respect voor het tijdselement. De term 'oorzaak' (O) refereert namelijk aan reële schades en de term risico's (R) aan schades die zich kunnen voordoen of zich zelfs in het geheel nooit voordoen (G). Daarbij is het van belang om te onderkennen dat (hypothetische) schades volgen uit de vergelijking tussen enerzijds de hypothetische toestand zonder schade en anderzijds de reële dan wel hypothetische toestand met schade. Daarnaast is het van belang om te onderkennen dat objecten die niet aan een waarde of tijd zijn onderworpen geen schade kunnen leiden; deze objecten kunnen enkel veranderen.

De voorgaande theoretische beschouwing helpt bij het kiezen van een gedegen risicoanalysetechniek. Momenteel wordt voor het uitvoeren van de systematische integriteitsrisicoanalyse (SIRA) veelal een afgeleide of combinatie van de brainstorm of de Delphi-techniek gebruikt, terwijl deze technieken enkel toepasbaar zijn op het eerste proces van de risicobeoordeling, namelijk de risico-identificatie.

Een techniek die zich goed leent voor het uitvoeren van de overige processen (risicoanalyse en -evaluatie) is de bow-tie-analyse. Deze analysetechniek geeft een eenvoudig overzicht van alle geïdentificeerde scenario's, met inbegrip van de preventieve barrières die een bepaalde scenario kunnen voorkomen en de repressieve barrières die de gevolgen van een bepaald scenario kunnen beperken.

Overigens bleek uit de risicodefinitie dat risico's uit drie factoren bestaan, namelijk: dreiging, kwetsbaarheid en consequentie. Op de eerste factor hebben financiële ondernemingen weinig invloed, daar dreigingen afhankelijk zijn van macroculturele of -economische ontwikkelingen en bovendien het domein van diverse overheidsorganisaties vormen. De andere twee factoren kunnen daarentegen worden beïnvloed door middel van preventieve en repressieve beheersmaatregelen. Beheersmaatregelen kunnen met andere woorden de kwetsbaarheid of de consequentie verminderen. Als vanzelfsprekend is een combinatie eveneens mogelijk.

Björn Schuitemaker is junior compliance officer bij het Nederlands Compliance Instituut, met als aandachtsgebieden: customer due diligence (CDD), witwassen, terrorismefinanciering, agressieve belastingplanning en (inter)nationale sanctieregelgeving. Albert de Jong is senior compliance officer bij het Nederlands Compliance Instituut, met als aandachtsgebied integere bedrijfsvoering. Daarnaast is hij belast met de coördinatie van de dienstverlening aan de pensioenfondsen.

Compliance highlight: PE-bijeenkomsten raad van bestuur en raad van commissarissen

Permanente educatie (PE) is voor iedere raad van bestuur en raad van commissarissen van essentieel belang. Maar het gedegen vormgeven en uitvoeren van een PE-programma zorgt regelmatig voor de nodige hoofdbreken. We assisteren u graag hierbij.

We kunnen het gehele PE-programma opzetten en uitvoeren. Of u kunt PE-bijeenkomsten bij ons afnemen. In overleg met u maken we gebruik van onze standaard-programma's of ontwikkelen we PE-programma's op

maat. Een PE-bijeenkomst kan op ieder gewenst moment incompany georganiseerd worden, met uw eigen raad en bij u op locatie.

Wilt u meer informatie?
Cora Wielenga helpt u graag.

☎ 088 99 88 100
☎ 06 20 49 27 49
✉ c.wielenga@compliance-instituut.nl

07 september	Toezichtrecht voor niet-juristen
12,13 september	Update Compliance
14 september	Themamiddag MiFID II voor beleggingsondernemingen (verwacht)
27 september	Themamiddag Privacy in de zorg
27 september	Update Compliance Trust
28 september	VCO Compliance Symposium
10 oktober	Introductie Compliance
12 oktober	LCO Zorg Module 4: De toezichthouders
12 oktober	Themamiddag Pensioenen (verwacht)
19 oktober	Themamiddag Trust (verwacht)
23, 24, 25 en 26 oktober	Leergang Dutch Caribbean
7 november	Masterclass Zorgplicht (verwacht)
15,16 november	Functionaris Gegevensbescherming Zorg
21 november	Compliance & Integriteit voor HR professionals
22 november	Competentietraining
23 november	LBW Module 2: Bestrijding witwassen & terrorismefinanciering in de praktijk
28,29 november	Opleiding Privacy Officer
29,30 november	LCP Module 5: Compliance Risk Management
30 november	LBW Module 3: CDD-beleid en gedifferentieerd cliëntenonderzoek
06 december	LCO/LCP Module 2: Compliancefunctie en integere bedrijfsvoering
12 december	LBW Module 4: Transactiemonitoring
14 december	Nationaal Compliance Congres (verwacht)
21 december	Themamiddag FinTech (verwacht)
	LBW: Leergang Bestrijding witwassen & terrorismefinanciering
	LCO: Leergang Compliance Officer
	LCP: Leergang Compliance Professional

Vertrouwens- persoon

Wij kunnen voor uw organisatie optreden als externe vertrouwenspersoon. Onze medewerkers zijn hiervoor opgeleid, zowel op het beid van integriteit, als op het gebied van ongewenste omgangsvormen.

www.compliance-instituut.nl

Recruitment en detachering



Wilt u zich als ervaren compliance professional verder ontwikkelen in een uitdagende functie? Of bent u op zoek naar nieuwe, tijdelijke opdrachten op het gebied van compliance? Wij komen graag met u in contact.

Annemarie Pierik

088 99 88 100

06 83 59 98 47

pierik@compliance-instituut.nl

Susan Tjong

088 99 88 100

06 53 98 03 95

tjong@compliance-instituut.nl

www.compliance-instituut.nl/recruitment