de Compliance Officer
nummer 15, september 2014

DNB's 'Good practices bestrijden corruptie' onder de loep

Geschikt of niet?

Dorothé Beernink: Compliance Officer Equens

Kees Cools: 'De aarde biedt genoeg voor iedereen, maar niet voor ieders hebzucht'

Nederlands compliance Instituut

Inhoud

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 compliancetaken.

Redactie:
José Hooghiemstra (interviews), Sharon Karsten (bureauredactie) en Cora Wielenga (eindredactie)
Tel 088 99 88 100 E-mail: redactie@complianceofficer.nl
Aan deze editie werkten verder mee: Adriaan van Verseveld, Bernadette Ouwerkerk, Marit Klapwijk, Tom van Middelkoop, Bart Peters en Sacha Spoor
Fotografie: Wilco van Dijen
Vormgeving: Tangram Studio
Druk: Kapsenberg & Van Waesberge 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 3.100
ISSN 1878-7991

www.complianceofficer.nl

Eed/belofte: tijd voor een goed gesprek

Heeft u de eed of belofte al afgelegd? Voor bestuurders en commissarissen was dit al sinds 1 januari 2013 een verplichting. Vanaf volgend jaar geldt deze verplichting voor veel meer mensen in de financiële sector. Eigenlijk kunnen we de aankomende uitbreiding verdelen in drie groepen. De eerste groep bestaat uit mensen die vanaf volgend jaar voor het eerst aan de geschiktheidstoets moeten voldoen. Dit zijn personen die onder het eerste echelon een leidinggevende functie uitoefenen en het risicoprofiel van de financiële onderneming kunnen beïnvloeden.

De tweede groep bestaat uit medewerkers die het risicoprofiel van de onderneming wezenlijk kunnen beïnvloeden en medewerkers die zich rechtstreeks bezig houden met het verlenen van financiële diensten. Voorbeelden van mensen die het risicoprofiel van de onderneming kunnen beïnvloeden zijn bijvoorbeeld leden van de kredietcommissie of individuele handelaren. Ondernemingen kunnen deze groep gelijk trekken met de zogenaamde 'risk identified staff', die zij op basis van beloningsregels uit 2011 moeten aanwijzen. Ondernemingen mogen hier overigens ook van afwijken. Bij de medewerkers die zich rechtstreeks bezig houden met het verlenen van financiële diensten, denken we natuurlijk al snel aan de medewerkers die klanten adviseren, de zogenaamde klantmedewerkers. Maar de verplichting om de eed/belofte af te leggen reikt verder dan alleen de klantmedewerker. Ook de medewerkers die klanten slechts informeren over producten, bijvoorbeeld in het geval van execution only dienstverlening, zijn verplicht om de eed/belofte af te leggen.

De derde groep mensen bestaat uit alle bankmedewerkers. De NVB heeft verzocht om de zelfregulering, die alle bankmedewerkers zal verplichten om een eed-belofte af te leggen, op te nemen in de Wft.

Wat kan er gebeuren wanneer bestuurders en commissarissen de eed/belofte niet afleggen? Voor bestuurders en commissarissen kan dit leiden tot een hertoetsing met uiteindelijk het risico dat ze door de toezichthouders worden heengezonden. Wat gebeurt er wanneer organisaties de eed/belofte niet volgend jaar realiseren? In dat geval kunnen DNB en AFM bijvoorbeeld dwangsommen of bestuurlijke boetes opleggen.

Ik sluit niet uit dat DNB en AFM handhavend zullen optreden. Bestuurders en commissarissen hebben deze verplichting al sinds 2013. En nog steeds zijn er organisaties waar bestuurders en commissarissen de eed/belofte niet hebben uitgesproken, omdat ze deze verplichting afdoen als onzinnige 'window dressing'. Hoe zal dan straks binnen die organisaties het afleggen van de eed/belofte door de medewerkers worden ervaren? Juist door zo te handelen wordt het een afvinkexercitie, terwijl je als organisatie er juist je winst uit kunt halen. Het afleggen van de eed/belofte is juist hét moment om weer met elkaar in gesprek te gaan over de onderliggende waarden van de organisatie. Op het moment dat je dat gesprek goed voert met elkaar, kun je als organisatie een hoop tijd besparen op het implementeren en monitoren van allerlei regels. Ik adviseer organisaties om de eed/belofte aan te grijpen voor een goed gesprek. En hulde aan die organisaties die dat al hebben gedaan. Organisaties waar het gesprek al is gevoerd en waarin de eed/belofte is uitgesproken tijdens een officiële ceremonie. Gelukkig kan het zo ook.

Cora Wielenga

Kees Cools:

‘De aarde biedt genoeg voor iedereen, maar niet voor ieders hebzucht’

Met deze uitspraak van Gandhi begint *Kees Cools*, partner bij Strategy& en hoogleraar Corporate finance en governance aan de Universiteit van Tilburg (TIAS School for Business and Society) zijn oratie 'Gandhi in governance' op 20 juni 2014. Hij onderzocht de zestien grootste Amerikaanse banken op oorzaken van de financiële crisis. Als grote risicofactoren duidt hij de omvang van banken, de solvabiliteit, extreme financiële prikkels en gedrag: ijdelheid, narcisme en burgerlijke staat van CEO's. Met name zijn bevinding dat CEO's van bescheiden sociaal-economische komaf een risicofactor vormen, kreeg veel commentaar. Zijn conclusie is dat governance niet in staat is perverse drijfveren en motieven van bestuurders te corrigeren. Nederigheid en waarheid spreken (het Griekse parrèsia) noemt hij als twee cruciale factoren die kunnen helpen de gedragseffectiviteit van boards te versterken. José Hooghiemstra ging met hem in gesprek over wat zijn conclusies betekenen voor compliance en hoe deze vormgegeven kunnen worden binnen ons huidige financieel bestel.

Compliance gaat ondermeer over corporate governance. U zegt eigenlijk dat het niet werkt. Klopt dat? 'Dat is wel de essentie. Om precies te zijn: als het er op aan komt, werkt het niet. Met "als het er op aan komt" bedoel ik: wanneer de drijfveren en motieven van bestuurders en mensen in verantwoordelijke posities niet aansluiten bij de doelen van de wetgever of de onderneming, er geen enkele regel, code of controlesysteem is die daartegen bestand is. Het heeft allemaal te maken met drijfveren (waar ga ik voor) en waarden en normen (waar sta ik voor). Als die voor iedereen anders zijn, dan is compliance kansloos. Neem als extreem voorbeeld van controle een gevangenis. Daar zijn de drijfveren en de doelen van de gevangenen tegengesteld aan die van de leiding van de instelling; gevangenen willen eruit, de directie wil ze erin houden. Gevolg: maximale controle, dikke muren, camera's, prikkeldraad. Toch ontsnapt er elke dag ergens in de wereld een gevangene, zelfs bij 24 uur per dag controle.'

Hoe bent u er zo toe gekomen dit te gaan onderzoeken? 'De start was mijn boek "Controle is goed, vertrouwen nog beter" (2005). Daar kwam dit onderwerp min of meer toevallig uit de analyses van de 25 grootste boekhoudschandalen (Enron, Worldcom, Ahold, etc.) naar voren. Sindsdien heeft het mijn belangstelling. Ik wist voorheen nauwelijks wat corporate governance was. Toen ik werd gevraagd om lid te worden van de eerste "corporate governance monitoring commissie" met Jean Frijns, ben ik er dieper ingedoken. Er was bovendien nog niet eerder dergelijk onderzoek naar gedaan. Ik vind het intellectueel, maar ook maatschappelijk een heel intrigerend en een belangrijk onderwerp. Ik citeer in mijn oratie President Bush, die bij het ondertekenen van de Sarbanes-Oxley wetgeving – bedoeld om schandalen als Enron voorgoed te voorkomen – zei: "The era of low standards and false profits is now finally over..." Handtekening eronder en klaar: de illusie van de wetgever. Die is kansloos, echt kansloos'

Is het niet eigenlijk het verhaal over mens zijn en verkeren met elkaar? 'De morele mens heeft op een gegeven moment bedacht: "We moeten ordening aanbrengen." Zarathustra (Iraanse profeet en stichter van religieuze beweging uit de 14de eeuw BC, red.) is de eerste filosoof waarvan men zegt dat hij expliciet onderscheid maakte tussen goed en kwaad en dat heeft geproblematiseerd. Dit soort denken is in het licht van de

menselijke evolutie eigenlijk heel jong. Ja, het is wel mens zijn, maar het is ook mens zijn wat kansloos is. Een soort onmogelijke opgave vooralsnog. De governance problemen zijn niet minder geworden sinds de eerste governance schandalen bij de oprichting van de VOC 400 jaar geleden.'

> Uiteindelijk gaat het om 'waar ga ik voor, waar sta ik voor'

Heeft uw oratie veel kritiek opgeroepen? 'Ik heb commentaar gekregen, maar ik krijg ook verzoeken van CEO's en raden van bestuur, omdat men zich blijkbaar realiseert dat hier een probleem zit. Bij een grote bank ben ik bijvoorbeeld uitgenodigd om met hun kredietverstrekkers te kijken naar het gedrag van klanten die kredieten vragen. Eén punt van kritiek is mij door Eli Leenaarts van ING aangegeven; dat ik naast de solvabiliteit ook naar de liquiditeit moet kijken.'

Is het niet gevaarlijk op basis van afkomst en cultuur een prognose van toekomstig gedrag te maken? Dat ligt heel dicht bij discriminatie. 'Het gaat niet over prognoses, het gaat over risico's. Er zijn natuurlijk mensen die zeggen: "Twintig jaar geleden zou je hierom zijn verketterd." Maar ik publiceer slechts resultaten van onderzoek. Het zou te gek zijn dat ik die uitkomsten niet zou mogen publiceren. Het lijkt me juist goed dat dergelijk onderzoek er is. Hiermee kunnen maatschappelijke risico's hopelijk verkleind worden. Risico's komen deels voort uit achterstelling. In Australië is er expliciete wetgeving die universiteiten verplicht om mensen uit lagere milieus te beschermen door maatregelen te treffen die achterstelling voorkomen. Aangenomen dat het onderzoek zorgvuldig is uitgevoerd en dat de uitkomst klopt, dan is dit juist een oproep om er iets aan te gaan doen! Er met zijn allen over te spreken, nader te bekijken hoe het zit en vooral ook om hier nog meer onderzoek naar te doen. Dit is tenslotte maar één onderzoek. Als straks blijkt dat andere soortgelijke onderzoeken andere resultaten geven, dan zat ik blijkbaar bij de 5% uitzonderingen. Alhoewel, ik ben nu bezig met een vergelijkbaar onderzoek bij Europese banken. Dat is nu voor een belangrijk deel klaar, maar op hoofdlijnen lijken de resultaten identiek.'

Roept het product 'geld' die hebzucht op? 'Nee, daar zit het niet in. De bestuurders verdienen niks aan het product geld. Zij willen carrière maken, status, macht en een hoog inkomen. Waarom wil men een hoog inkomen? Omdat inkomen primair bijdraagt aan status. Het gaat dus niet zozeer om het kunnen kopen van bijvoorbeeld een derde huis, maar meer om met dat derde huis te kunnen pronken. Geld heeft een externe werking, niet zozeer een interne. Er is blijkbaar behoefte om te etaleren. Het maakt niet uit of je status, macht en geld creëert met het verkopen van kruidenierswaren, olie of melkproducten. Ik heb destijds de top 25 boekhoudschandalen onderzocht. Daar zat geen bank bij. Hebberigheid ja, maar het had niets met de aard van het bedrijf te maken.'

Welk beeld had u van de CEO's van de banken die u onderzocht heeft, heeft u ze ook persoonlijk gesproken? 'Bij het Amerikaanse bankenonderzoek heb ik niemand gesproken. Dat is in zekere zin ook wel de kracht van het onderzoek. Het onderzoek is gebaseerd op publieke informatie die voor iedereen inzichtelijk is. Iedereen kan zien dat er hoge bonussen worden uitbetaald, dat het narcisten lijken te zijn, dat ze voortdurend zichzelf op de voorgrond zetten. Het is extreem zichtbaar en toch gebeurt het!'

Dat is wellicht ook wel het benauwende. Het is openbaar, maar het gaat gewoon door. 'Een journalist van het FD vroeg mij onlangs naar de lessen van Imtech (elektronisch installatiebedrijf welke door grote fraude in moeilijkheden is geraakt, red.). Deze zaak heeft alle ingrediënten in zich van eerdere schandalen met narcistische bestuurders. De interessante vraag is dus niet wat er nou precies gebeurd is, maar waarom het steeds weer gebeurt, ondanks regels en codes. De titel boven zijn artikel was: "Een mens leert, maar de mens niet". Zo is het. Mensen hebben persoonlijke ervaringen, ze scheiden, gaan failliet, worden ontslagen. Heftige ervaringen die ze meenemen voor het leven, maar na de dood is die ervaring weg. Dan begint het weer opnieuw. Het einde van een mens is ook het einde van die emotionele ervaring.'

U heeft in wezen een vrij negatief mensbeeld? 'Mijn mensbeeld is niet negatief, het is wat het is. Er is niets negatiefs aan. De constatering dat het steeds terugkomt is ook niet negatief. Mijn analyse over afkomst

is ook niet negatief. Het zijn gewoon de feiten. Ik probeer het te begrijpen en dan kom ik uit bij zo'n uitspraak als "een mens leert, maar de mens leert niet."'

U heeft toch ook gezegd: Goed bestuur is tegen de natuur? 'Het past niet bij wat we zijn. Ieder van ons zit in een voortdurende titanenstrijd tussen Darwin en Gandhi. "Darwin" staat voor de evolutionaire, natuurlijke selectie en het primaten gedrag in ieder van ons, dat al ruim drie miljard jaar oud is. Gandhi's morele mens is maar 3000 jaar oud. Het ene is de natuur waar wij evolutionair vandaan komen, het andere is gecreëerd en kunstmatig en eigenlijk tegen de natuur. We willen wel, maar we kunnen vaak niet.'

Toch is het wonderlijk, want die impuls om het goede te willen komt toch ook ergens vandaan? 'Dat weet ik niet, dat is de vraag. Mijn hypothese is dat dat pas gekomen is toen de mens wat vrije tijd kreeg en tijd had om daar over na te denken. Toen de mens niet meer dag en nacht bezig hoefde te zijn om voor voedsel te zorgen en zich te beschermen tegen de natuurlijke vijanden om ons heen. Moraal, daar gaat tijd overheen, daar moet je over nadenken, daar moet je op kunnen reflecteren en een bepaalde mate van intelligentie voor hebben. Beide ontbraken ons voor die tijd. Menselijke moraal is luxe.'

Toch wordt er in onze wereld wel op ingezet. De Algemene Rechten van de Mens, de mens moet gered worden, wij willen een zorgzame maatschappij. Hoe ziet u de wereld verder gaan? 'Het is echt een wankel evenwicht en heel fragiel. Ik heb eens ooit gelezen dat als overal in de wereld de elektriciteit acht dagen uitvalt, we weer terug in de oertijd zijn en elkaar de hersens in slaan. Acht dagen maar. We lopen heel veel risico dat we weer terugvallen. Los van alle oorlogen en wat er gebeurt in de wereld. We moeten beseffen dat het fragiel is, maar dat we ook door moeten. Dat is ook zo met compliance. Compliance gaat tegenwoordig veel over soft controls. Het is nu even modieus, maar het raakt wel de essentie. Het heeft echter weinig zin ben ik bang. Het grote probleem ligt in het feit dat de compliancemensen die zich daarmee bezig houden, allemaal onder de directie vallen en sterk afhankelijk zijn. Moet je voorstellen dat de compliance officer de directie gaat aanspreken op hun gedrag. Dat gebeurt niet! De CEO is uiteindelijk wel verantwoordelijk, maar die heeft andere drijfveren en dat is het probleem, die wil dat vaak helemaal niet als het er op aan komt.'

Ik hoor dat compliance groeit. Steeds meer kracht krijgt binnen organisaties. U zegt dat dat niet zo is? 'Wat ik bedoel is dat het wel gebeurt, maar vaak bij mensen die het niet nodig hebben. Bij mensen waar het niet goed zit komt de tegenkracht niet van een compliance officer en ook niet van het hoofd compliance.'

Wat is die tegenkracht? 'Bij een CEO zijn dat drie mensen: de eerste is de eerste echtgenote, de tweede een sterke CFO en de derde zijn de puberende kinderen. Dat zijn de mensen die dichtbij staan en durven te zeggen wat ze vinden. Echter, er zijn nogal wat CFO's die door de knieën gaan, want die willen zelf graag CEO worden of tenminste niet als permanente lastpost worden ervaren. De eerste vrouw wordt ingeruild voor een "trophy wife" en puberende kinderen gaan op een gegeven moment de deur uit en klaar. Het moet van de commissarissen komen, daar ligt het begin van een oplossing. De laatste zin van mijn oratie luidt: "Het evolutionaire tekort van kleine zielen is de kracht van de kudde."'

Wat bedoelt u daar precies mee? 'We hebben een paar grote zielen als Mahatma Gandhi (Mahatma betekent "grote ziel") en dan de kleine zielen, dat zijn wij allemaal. De kracht van de kudde zou parrèsia moeten zijn (waarheid spreken). Het is moeilijk waarheid te spreken bij een raad van commissarissen, omdat je al snel een outcast wordt als je het niet eens bent en te kritisch bent. Je bent al snel niet coöperatief, je bent niet loyaal, je kent de regels van het spel niet. Mensen zijn daarom niet oprecht. Er is geen moed om waarheid te spreken, omdat we dan uit de kudde vallen en dan zijn we alleen, dan overleven we niet. Vroeger letterlijk, maar nu sociaal niet. We moeten dus diezelfde kudde herdefiniëren. We spreken voortaan af dat parrèsia heel belangrijk is. Wij gaan elkaar aanspreken en we spreken af dat, als iemand echt een afwijkende mening heeft, wij ernaar luisteren en dat juist waarderen in plaats van dat wij van hem of haar een outcast maken. Met andere woorden: als je de waarheid spreekt, lig je niet meer uit de kudde, maar dan maak je juist deel uit van de kudde. De kudde is dan geherdefiniëerd. Levinas (Joodse filosoof, 20ste eeuw) zag de Ander als een weerloos schepsel dat een appèl doet op zijn verantwoordelijkheid. Wij moeten het niet hebben van discipline door het opleggen van regels en principes gelijk voor iedereen. Als je elkaar aankijkt, contact maakt in de kudde en dan gezamenlijk optrekt, dan werkt het wel. Dat is mijn visie. Het gaat fout in het gedrag en het moet dus gecorrigeerd worden in het gedrag zelf. Niet met andere instrumenten.'

Krijgt u hier gehoor voor en hoe gaan we dat vorm geven? 'Journalisten vinden het allemaal machtig interessant. Ook veel jongere commissarissen. Alleen, diegenen waar het met name voor bedoeld is, zijn de laatsten die er echt wat mee gaan doen. Bij commissarisopleidingen worden dit soort boodschappen steeds meer gewaardeerd. De mensen waar het echt om gaat, dat zijn de commissarissen en bestuurders bij de grotere ondernemingen. Diegene die het het meeste betreft, zijn waarschijnlijk de laatsten. De jeugd heeft de toekomst!'

Is er uit de variabelen uit uw onderzoek (financiële karakteristieken, beloningen van bestuurders, kwaliteit van de governance en persoonlijke kenmerken van CEO's) af te leiden dat één variabele een grotere invloed heeft op het label 'slechte' of 'goede' bank? 'De persoonlijke kenmerken van CEO's. De rest komt er uit voort; narcisme, het gedrag, de persoonlijkheid. En dan de onderlinge dynamiek in boards. Waar je vandaan komt is van invloed daarop en dat kan weer verder gestimuleerd worden door die bonussen. Uiteindelijk gaat het om "waar ga ik voor, waar sta ik voor".'

Is het ook niet ken u zelve, wie ben ik? 'Ja, maar dat is de eerste vraag. Van Erik van de Loo heb ik geleerd dat nederigheid drie kenmerken heeft. De eerste is zelfreflectie, de tweede is openstaan voor de ander en de derde is beseffen dat je onderdeel bent van iets groters. Dat grotere kan je gezin zijn of het bedrijf waar je werkt. Je bent maar een passant. Het bedrijf is er straks nog steeds en jij bent vertrokken. Er zijn drie vragen voor een mens: wat kan ik, wat wil ik, wie ben ik. Wat kan ik is je CV, daar kijkt iedereen naar bij elke benoeming. Die andere twee komen bijna niet aan bod. Wat wil ik zijn je drijfveren en wie ben ik zijn je normen en waarden. Daar gaat het vaak fout. We moeten veel meer focussen op de laatste twee vragen. Het is zelfs zo dat de CV zelfs een contra-indicator is. Het blijkt dat mensen die een carrière maken drie keer zo veel tijd besteed hebben in hun carrière aan het politieke spel, dan gewoon met hun eigen werk binnen hun eigen bedrijfsonderdeel bezig te zijn. Als dat zo is, dan zijn die mensen die carrière hebben gemaakt politiek handig, maar niet goed. Dat is aangetoond in een 30 jaar oud onderzoek van Fred Luthans, een Amerikaanse hoogleraar. Fantastisch.'

Wat is uw advies aan organisaties en speciaal aan compliance officers, over wat zij met uw onderzoek kunnen doen? 'Ze moeten eerst bedenken: hoe zit het bij ons in elkaar? Heeft de directie een luisterend oor? Zo niet, dan moeten ze contact zoeken met kritische geesten binnen de onderneming en met commissarissen. Ze kunnen ook heel praktische zaken afspreken, bijvoorbeeld over het jaarlijks in kaart brengen wat medewerkers vinden en voelen. Goed afspreken wat er gemeten wordt en hoe. Dit vervolgens aankaarten bij de directie en RvB. De RvB moet onderkennen en weten dat hun gedrag de belangrijkste factor is. Als het daar fout gaat, wordt het daaronder nooit meer gecorrigeerd. Een RvC moet daarbij betrokken zijn en eigenlijk ook leidend zijn, anders gaat het niet lukken. Compliance officers moeten er voor waken dat zij niet in dezelfde val trappen als President Bush. We hebben het allemaal afgevinkt en toch ging het mis; we stonden er bij en keken er naar.'

DNB en AFM beoordelen de geschiktheid van bestuurders en commissarissen van onder toezicht staande instellingen. In hoeverre zou uw onderzoek de geschiktheidstoetsingen van DNB en AFM kunnen helpen? 'Gedrag primair inzetten als toetsing. DNB is al een tijdje bezig met het nadenken en sturen op gedrags- en cultuuraspecten van financiële instellingen. Ze hebben ook al een slag gemaakt, niet langer focussen op bekwaamheid maar kijken naar geschiktheid. Bekwaamheid is je CV, geschiktheid is al die andere factoren. DNB is in dat opzicht goed bezig. Tegelijkertijd worden ze echter gedwongen of dwingen ze zichzelf, mede door de politiek, om meer op regelgeving te focussen.'

Is het niet eens tijd om de enorme hoeveelheid regelgeving over boord te gooien? 'De Code Tabaksblat moet eigenlijk de prullenbak in en we moeten een nieuwe code schrijven. De huidige code is teveel gebaseerd op regels en voorschriften en zou veel meer op de gedragsleest geschoeid moeten worden.'

U denkt dus dat het gaat lukken. Nu de economie weer aantrekt gaat niet iedereen weer gezellig voort op de oude weg? 'Goede vraag, maar het lijkt te gaan lukken hier en daar. We zijn de afgelopen tijd een eind opgeschoten. Tien jaar geleden en daarvoor gebeurde er helemaal niets op dit gebied. Het gaat stapje voor stapje. Journalisten pikken het op en via opleidingen en commissarisopleidingen wordt het doorgegeven. Je openstellen voor de "moed tot waarheid spreken". Ik hoop stiekem wel eens dat het om de paar jaar ergens zichtbaar mis gaat. Niet zo radicaal als destijds rond de eeuwwisseling en ook niet zoals in de financiële crisis, maar op kleine schaal. Dat houdt iedereen alert en dat is hard nodig!'

Geschiktheidstoetsingen: Koorddansen zonder zekering?

Cora Wielenga

Kent u de reclamecampagne van Defensie nog? Geschikt/ongeschikt? In korte spotjes werd duidelijk gemaakt welke kwaliteiten je geschikt maken om bij Defensie succesvol te zijn. Een heerlijke eenvoudige weergave van een selectieproces. De werkelijkheid is minder zwart-wit. Het beoordelingsproces is immers al lastig bij het werven van eigen personeel, laat staan als je dit als externe partij uitvoert. Toch beoordelen DNB en AFM de geschiktheid van bestuurders en commissarissen en kunnen zij besluiten om hen 'heen te zenden'. Dit is een nuttige bevoegdheid bij slecht bestuur of toezicht, maar wanneer is daar sprake van? Toezichthouders moeten balanceren tussen het weren van een ongeschikte bestuurder en het gevaar om onterecht een benoeming van een bestuurder te blokkeren.

Het toetsingsproces is sinds 2011 een aantal veranderd en aangescherpt. Om het toetsingsproces voor organisaties en externe toezichthouders te verbeteren, wordt er nu meer verwacht van onder toezichtstaande instellingen. Ondernemingen moeten nu bijvoorbeeld beter motiveren waarom een bepaalde bestuurder of commissaris geschikt is. In dit artikel behandel ik de huidige regels over geschiktheid en blik ik vooruit op de aanstaande wijzigingen. Waar van toepassing geef ik suggesties.

Huidige regels

Bij het bespreken van de huidige regels behandel ik op wie de regels van toepassing zijn, wat de toetsing inhoudt, wanneer de toetsing uitgevoerd moet worden, wanneer welke toezichthouder moet toetsen en wat de uitkomsten daarvan kunnen zijn. Als laatste licht ik de verplichting van doorlopende geschiktheid toe.

Wie wordt getoetst?

De geschiktheidsregels zijn momenteel van toepassing op de volgende personen[1]:

- beleidsbepalers (bestuurders) en overige beleidsbepalers (bijvoorbeeld plaatsvervangende bestuurders);
- leden van organen die belast zijn met het toezicht op het beleid en algemene zaken van een financiële onderneming. Hiermee worden leden van een raad van commissarissen en een raad van toezicht bedoeld. Maar ook de algemeen bestuurders bij onderlinge verzekeraars;
- dagelijkse beleidsbepalers van organisaties die meer dan 10% aandelen- of zeggenschapsbelang houden in een Nederland gevestigde financiële onderneming;
- vertegenwoordiger van een levensverzekeraar of schadeverzekeraar met zetel in Nederland die zijn bedrijf uitoefent door middel van een buiten Nederland gelegen bijkantoor.

Voor de leesbaarheid van het artikel heb ik het vanaf nu over de toetsing van de bestuurders en commissarissen, omdat dit de grootste groep is op wie deze regels van toepassing zijn.

Wat wordt getoetst?

Wat houdt geschiktheid eigenlijk in? Geschiktheid bestaat volgens de Beleidsregel geschiktheid 2012 van DNB en AFM uit kennis, vaardigheden en professioneel gedrag. De geschiktheid van een bestuurder of commissaris blijkt in ieder geval uit de opleiding, werkervaring en competenties van de persoon. In de praktijk moeten bestuurders en commissarissen doorlopend laten zien dat zij kennis, vaardigheden en professioneel gedrag adequaat en zorgvuldig toepassen.

Wanneer wordt getoetst?

De geschiktheidseis is een doorlopende eis. De geschiktheid wordt niet alleen voorafgaand aan de benoeming van de bestuurder of commissaris getoetst, maar ook tijdens het uitoefenen van de functie indien daar aanleiding voor is.

1 Zie voor een overzicht van het juridisch kader per type onderneming <www.compliance-instituut.nl/pagina/publicaties_medewerkers_nederlands_compliance_instituut>.

Een aanleiding voor een hertoetsing kan zijn dat een bestuurder of commissaris een andere functie binnen de raad krijgt. Bijvoorbeeld op het moment dat een lid voorzitter wordt of dat één van de RvC-leden lid wordt van de auditcommissie.

Een andere aanleiding voor hertoetsing voor DNB en AFM is dat er feiten bekend worden waardoor twijfel ontstaat over de geschiktheid. Bijvoorbeeld bij een fusie of bij zorgen over het bedrijfsmodel of de organisatiecultuur.

Leden van visitatiecommissies van pensioenfondsen worden overigens niet getoetst voorafgaande aan de benoeming. Zij moeten op grond van de Pensioenwet wel deskundig zijn, maar worden alleen getoetst wanneer daar aanleiding voor bestaat. Leden van andere toezichthoudende organen van pensioenfondsen worden wel door DNB voorafgaand aan de benoeming getoetst op geschiktheid.

Attentiepunt:
- Denk bij wijzigingen van rollen van bestuurders of commissarissen aan een melding aan DNB of AFM zodat er zonodig een hertoetsing kan plaats vinden.

Hoe wordt getoetst?

Ondernemingen zijn verantwoordelijk voor het aanstellen van geschikte bestuurders en commissarissen. Dit betekent dat zij zelf eerst moeten vaststellen in hoeverre de bestuurders en commissarissen die zij voordagen bij DNB en AFM geschikt zijn en dit gemotiveerd aangeven.

Ondernemingen moeten bij aanvragen een geschiktheidsmatrix[2] voor de gehele raad invullen. Deze matrix moet de kennis en ervaring van alle bestuurders of commissarissen aangeven. De matrix moet de sterke én de zwakke plekken binnen de raad tonen.

Naast de motivering en de geschiktheidsmatrix moet de onderneming het functieprofiel, het CV en de procedure van werving- en selectie aanleveren. Voor banken geldt daarnaast dat zij de uitkomsten van het assessment moeten meesturen.[3] Voor andere ondernemingen wordt dit op prijs gesteld, maar is dit niet verplicht.

DNB en AFM verrichten aan de hand van de ingezonden informatie en de al bij de toezichthouders beschikbare informatie bureauonderzoek. Daarnaast worden referentgesprekken en een interview met de kandidaat gevoerd.

In de toetsing worden de volgende criteria meegenomen:
- kennis, vaardigheden en professioneel gedrag;
- functie bestuurder;
- collectief;
- omvang van de organisatie;
- risicoprofiel van de organisatie.

Doordat bij de toetsing van een bestuurder het collectief wordt beoordeeld, kan het voorkomen dat een bestuurder die op zich geschikt is voor de functie wordt afgewezen, omdat het collectief behoefte heeft aan andere competenties.

Attentiepunt:
- Beoordeel als organisatie niet alleen de geschiktheid van de te benoemen persoon, maar ook de geschiktheid van het collectief en verwoord dit in de motivering richting DNB of AFM.

Welke toezichthouder?

De vergunningverstrekkende toezichthouder voert de toetsingen uit. Dat betekent bijvoorbeeld dat DNB bestuurders en commissarissen van een trustkantoor toetst. De AFM toetst bestuurders en commissarissen van bijvoorbeeld een beleggingsinstelling.

Voor banken en verzekeraars zijn zogenaamde 'dubbele poortjes' ingesteld. Dit betekent dat DNB als vergunningverstrekkende toezichthouder de geschiktheid beoordeelt van de bestuurder of commissaris. Wanneer DNB oordeelt dat de persoon geschikt is, wordt de toetsing voorgelegd aan AFM. De AFM heeft de bevoegdheid aan DNB kenbaar te maken dat ze de toetsing steunen of dat zij een 'bindende aanbeveling' afgeven. Een bindende aanbeveling betekent dat de kandidaat op dat moment door AFM niet geschikt wordt bevonden en dat DNB dit vervolgens moet opvolgen.

Uitkomsten

Logischerwijs zijn er als gevolg van de toetsing verschillende uitkomsten mogelijk. Allereerst natuurlijk 'geschikt' en 'niet geschikt'. Daarnaast kan het gebeuren dat de bestuurder of de commissaris besluit zich terug te trekken. Als laatste mogelijkheid kunnen DNB en AFM in uitzonderingsgevallen instemmen met benoemingen waarbij zij een voorschrift afgeven. Dit betekent dat de bestuurder of commissaris binnen een bepaalde periode nog kennis moet opdoen.

2 Deze matrix is afgeleid van de Beleidsregel geschiktheid 2012.

3 EBA Guidelines on the assessment of the suitability of members of the management body and key function holders, EBA/GL/2012/06.

Wanneer dit voorschrift niet tijdig wordt opgevolgd, kan de toezichthouder alsnog een negatieve beslissing nemen.

Doorlopende geschiktheid

Meer dan voorheen wordt sinds 2012 actief getoetst op doorlopende geschiktheid. Dit betekent dat voor bestuurders en commissarissen meer aandacht komt te liggen op o.a. de volgende onderwerpen:

- moreel ethische verklaring;
- permanente educatie;
- antecedentmeldingen;
- (zelf)evaluatie;
- beschikbaarheid.

Moreel ethische verklaring

Sinds 2013 zijn alle bestuurders en commissarissen verplicht een moreel ethische verklaring af te leggen, oftewel de eed of belofte. Deze verplichting is in de Wft ondergebracht bij de geschiktheidseis van bestuurders en commissarissen. Wanneer een bestuurder of commissaris zich niet houdt aan de eed of belofte, of deze niet eens aflegt, kunnen DNB en AFM een hertoetsing starten.

Permanente educatie

Bestuurders en commissarissen zijn op grond van verschillende governancecodes[4] verplicht om een programma van permanente educatie op te zetten en uit te voeren. De educatie heeft betrekking op relevante ontwikkelingen binnen de financiële sector, op corporate governance in de sector, op de zorgplicht jegens de klant, integriteit, het risicomanagement, financiële verslaggeving en audit. Voor banken en beleggingsondernemingen is permanente educatie overigens per 1 augustus 2014 een wettelijke verplichting.[5]

Attentiepunt:

- Waarborg dat een programma van permanente educatie is opgezet en wordt uitgevoerd.

Antecedentmeldingen

Ondernemingen zijn wettelijk verplicht wijzigingen in antecedenten van bestuurders en commissarissen te melden bij DNB of AFM. Dit betreft toezichtantecedenten, strafrechtelijke antecedenten, financiële antecedenten en fiscaal bestuursrechtelijke antecedenten. De bestuurders en commissarissen hebben de plicht om wijzigingen in persoonlijke antecedenten te melden bij de onderneming. DNB en AFM registeren deze meldingen in de 'bestuurdersmonitor'. Het doel van de bestuurdersmonitor is het verkrijgen van een totaalbeeld van antecedenten om de doorlopende geschiktheid van bestuurders en commissarissen te beoordelen. Sommige antecedenten kunnen leiden tot hertoetsing.

Toezichtantecedenten zijn toezichtmaatregelen die DNB en AFM opleggen. Een toezichtmaatregel die gericht is aan de financiële onderneming wordt geregistreerd bij alle bestuurders en commissarissen van die financiële onderneming, ongeacht welke bestuurder of commissaris feitelijk verantwoordelijk was voor de overtreding.[6]

Antecedenten tellen zwaarder mee in de beoordeling wanneer blijkt dat onderneming het antecedent niet zelf heeft gemeld.[7] DNB en AFM hebben toegang tot verschillende niet openbare bronnen, zoals de belastingdienst. Een voorbeeld zijn zwartspaarders die gebruik hebben gemaakt van de inkeerregeling. Bestuurders en commissarissen die gebruik hebben gemaakt van de inkeerregeling behoren dit als antecedent te melden bij DNB of AFM. Zo niet, dan krijgen ze te maken met minimaal een hertoetsing.

Attentiepunt:

- Verifieer bij bestuurders en commissarissen of de plicht om antecedenten te melden bekend is. Verifieer minimaal jaarlijks of er zich in het afgelopen jaar wijzigingen in de antecedenten hebben voorgedaan.

(Zelf)evaluatie

Op grond van verschillende governancecodes[8] zijn bestuurders en commissarissen verplicht periodieke (zelf)evaluatie uit te voeren. DNB en AFM verwijzen hiernaar en mogen bij een hertoetsing de uitkomsten van de periodieke (zelf) evaluatie opvragen en meenemen in de toetsing.

Attentiepunt:

- Waarborg dat bestuurders en commissarissen periodiek (onafhankelijk) geëvalueerd worden.

4 Code Banken, Governance Principes en Code Pensioenfondsen.

5 Implementatiewet richtlijn en verordening kapitaalvereisten.

6 DNB & AFM, Informatiebulletin toetsingen versie mei 2012 A.

7 Idem.

8 Code Banken, Governance Principes en Code Pensioenfondsen.

Beschikbaarheid
Bestuurders en commissarissen moeten voldoende beschikbaar zijn om de taken goed te kunnen uitoefenen. Per 1 januari 2013 zijn nieuwe regels van kracht, die leiden tot een beperking van het aantal toezichthoudende functies van een bestuurder of commissaris. Een commissaris mag niet meer dan vijf commissariaten bij grote NV's, BV's of stichtingen voeren. Het voorzitterschap van een RvC of een 'one-tier board' telt daarbij dubbel.[9]

Bestuurders van grote NV's, BV's of stichtingen mogen slechts bij twee van dergelijke andere rechtspersonen lid zijn van de RvC. Verder mogen ze geen voorzitter zijn van een RvC of van een one-tier board. Deze verplichtingen zijn van toepassing op de benoemingen en herbenoemingen na 1 januari 2013.
Bovengenoemde verplichtingen zijn overigens niet van toepassing op grote coöperaties. Hoewel het geen wettelijke verplichting is, adviseer ik om deze regels ook voor bestuurders en commissarissen van coöperaties in acht te nemen.

Per 1 augustus 2014 zijn er overigens voor 'significante banken' en 'significante beleggingsondernemingen' nog aanvullende regels in de Wft[10] van kracht geworden. Bestuurders daarvan mogen niet meer dan twee commissariaten vervullen. Deze verplichting is dus alleen nieuw voor een significante bank met de rechtsvorm coöperatie, oftewel de Rabobank. Een andere nieuwe verplichting is van toepassing op de commissarissen van significante banken en beleggingsondernemingen. Zij mogen niet meer dan vier commissariaten voeren. Dit betekent een aanscherping op de huidige regels uit het BW.

Attentiepunt:
- Waarborg dat bestuurders en commissarissen voldoende beschikbaar zijn en verifieer daartoe dat het aantal commissariaten dat zij voeren.

Toekomstige regels
De bestaande geschiktheidseis wordt per 1 januari 2015 uitgebreid naar personen die werkzaam zijn bij een bank of verzekeraar en daar als leidinggevende onder het eerste echelon grote invloed uit kunnen oefenen op het risicoprofiel van de financiële onderneming. Te denken valt aan leidinggevenden die verantwoordelijk zijn voor grote financiële transacties, juridische zaken, compliance, risicomanagement en audit. Het gaat dus niet om de medewerkers die werkzaam zijn op deze afdelingen.

DNB zal het toezicht op deze groep risicogebaseerd inrichten. Dit betekent dat DNB in eerste instantie alleen toezicht houdt op de interne processen ten aanzien van geschiktheidstoetsingen bij ondernemingen. Pas wanneer DNB signalen krijgt over de onderneming of bepaalde personen, zal DNB de desbetreffende personen uitgebreid toetsen op geschiktheid.

Voor de doorlopende geschiktheidseis is het nog niet helemaal duidelijk wat DNB van ondernemingen verwacht. Is het bijvoorbeeld de bedoeling dat voor deze groep ook een programma van permanente educatie wordt ingericht? Moeten deze functionarissen onverwijld melding maken van wijziging in antecedenten? Het lijkt mij van wel, maar op grond van de memorie wordt dat nog niet duidelijk. Wat wel helder is opgenomen, is dat deze groep functionarissen ook de eed/belofte zal moeten afleggen.

Attentiepunt:
- Organisaties moeten beoordelen of zij met de bestaande screeningsprocedures voldoen aan de aankomende wijzigingen.

Afsluitend
Het is mijn ervaring dat het onderwerp 'geschiktheid' niet in de top-tien-prioriteiten-lijst van compliance officers staat. Dat is op zich niet verbazingwekkend, als we kijken naar wat er allemaal op organisaties afkomt. Toch ben ik van mening dat dit onderwerp meer aandacht behoeft dan het nu krijgt. Geschikt bestuur en intern toezicht is immers ontzettend belangrijk voor organisaties. Zeker met het oog op de recente en aanstaande wijzigingen adviseer ik organisaties hier meer aandacht aan te besteden. Het is overigens helemaal niet noodzakelijk dat dit onderwerp op het bordje van de compliance officers komt te liggen. Waar mogelijk zal het in de meeste organisaties beter thuis horen bij de secretaris van de raad van bestuur. Echter in die organisaties waar er geen secretaris is benoemd, kan het de verantwoordelijkheid van de compliance officer zijn.

Cora Wielenga is directeur van het Nederlands Compliance Instituut. Voor meer informatie kunt u contact met haar opnemen. Tel. 088 99 88 100 of c.wielenga@compliance-instituut.nl.

9 BW2.
10 Door de inwerkingtreding van de Implementatiewet richtlijn en verordening kapitaalvereisten.

Speakers' Corner:
Sacha Spoor

De rol van de vertrouwenspersoon in het integriteitsbeleid

Op 10 juni 2014 organiseerde het NCI een themamiddag over de rol van de vertrouwenspersoon in het integriteitsbeleid. De opkomst was hoog, de deelnemers hadden uiteenlopende soorten functies en kwamen uit verschillende organisaties. De opzet van de middag was interactief; de deelnemers hebben zelf veel input geleverd over een aantal onderwerpen gerelateerd aan het vertrouwenspersoonschap. Dit artikel is een korte weerslag van die middag, met daarin de bijdragen van mijzelf als inleider op deze themamiddag en van de deelnemers.

Hoe ziet integriteitsbeleid eruit?
Effectief integriteitsmanagement is veel meer dan het afvinken van lijstjes. Zeker indien men beseft dat integriteit als levend thema voortdurend in beweging is. Het is bovendien een onderwerp dat veel aspecten van het werk raakt en een brede benadering vraagt.
In de praktijk zie je dat integriteit door velen wordt neergezet als het tegendeel van fraude, corruptie, belangenverstrengeling en andere ondeugden; oftewel, integriteit betekent dat je handelt conform de regels. Integriteit is in dat geval vooral een hygiënefactor en integriteitsmanagement is gericht op het voorkomen van misstanden.

Een hanteerbare, bredere en ook positiever geformuleerde definitie van integriteit, die recht doet aan veel associaties en in ieder geval de kern van thematiek goed samenvat is: zorgvuldig, uitlegbaar en standvastig handelen.[1]
Zorgvuldig betekent dat medewerkers steeds opnieuw kritisch en systematisch reflecteren op hun kernverantwoordelijkheden en zich voortdurend vragen stellen als: Hoe doe ik mijn werk goed? Doe ik recht aan de situatie? Houd ik in voldoende mate rekening met de rechten, belangen en het welzijn van alle belanghebbenden?
Uitlegbaar betekent dat medewerkers kunnen aangeven hoe hun handelen past bij hun kernverantwoordelijkheden en kerntaken, bij de kernwaarden regels, richtlijnen, wetten en andere bindende voorschriften van hun organisatie.
Zorgvuldig verwijst naar de manier waarop een standpunt wordt ingenomen, uitlegbaar naar de uitkomst, naar het standpunt zelf.

Standvastig handelen betekent dat medewerkers hun rug recht houden bij weerstanden en verleidingen; dat ze niet onverantwoord handelen omdat dit de weg van de minste weerstand is.

Integriteitsmanagement is dus meer dan alleen voldoen aan wet- en regelgeving en het beperken van allerlei soorten risico's; integriteit is meer dan alleen de relatiegeschenken, uitnodigingen en andere bijzaken in het werk.

1 Edgar Karssing, De oplossing is het probleem niet. Reflecties op ethiek, integriteit en compliance, Capelle aan den IJssel: NCI, 2011.

Rollen in het integriteitsbeleid

Effectief en evenwichtig integriteitsbeleid bestaat uit 6 onderdelen en bewaakt de samenhang hiertussen[2]:

1. Beleid, regels, procedures, wetten etc.
2. Normen en waarden
3. Cultuur
4. Visie en voorbeeldgedrag management
5. Incidenten
6. Evalueren en rapporteren

De vertrouwenspersoon maakt onderdeel uit van punt 5: 'Incidenten'.

Uit onderzoek[3] bij overheidsorganisaties blijkt dat 61% van de geënquêteerde ambtenaren het liefst een vermoeden van een misstand bij hun eigen leidinggevende aankaart. Als tweede meldinstantie wordt de vertrouwenspersoon genoemd, waar 20% naar toe zou gaan met een vermoeden van een misstand. Slechts 8% gaat naar het formele meldpunt van de organisatie (de integriteitsfunctionaris/ compliance officer). In de private sector zijn de cijfers vergelijkbaar; gemiddeld genomen wordt de helft van de vermoedens van misstanden intern aanhangig gemaakt (publiek 47%, privaat 52%). De meerderheid heeft dit via de directe leidinggevende gedaan.[4]

Deze wijze van melden is wat wij de 'snelweg' noemen; medewerkers moeten bij hun leidinggevenden terecht kunnen met dilemma's, met problemen of bij vermoedens van een overtreding. Het management is verantwoordelijk voor het oppakken en afhandelen van problemen. Er moet echter ook een 'vluchtstrook' georganiseerd worden. Dit voor het geval men niet terecht kan bij de leidinggevende, bijvoorbeeld omdat hij niets met de melding doet of omdat het over de leidinggevende zelf gaat. Daarvoor is de vertrouwenspersoon-functie in het leven geroepen, als de 'vluchtstrook' van de organisatie.

Rol van de vertrouwenspersoon

Uit het onderzoek Luisterend Oor[5] – maar ook uit de praktijk – blijkt dat de belangrijkste rol van de vertrouwenspersoon bestaat uit een luisterend oor zijn, hieraan wordt het meeste tijd besteed. Verder biedt de vertrouwenspersoon ondersteuning, geeft hij informatie en verwijst hij door naar instanties die de de betrokken medewerker verder kunnen helpen. Daarnaast geeft de vertrouwenspersoon voorlichting in de organisatie en adviseert hij het management over beleids- en procesmatige integriteitszaken (dus niet over individuele casussen).

Aan welke taak besteedt de vertrouwenspersoon integriteit de meeste tijd?

• Luisterend oor bieden	62%
• Advies aan melder	8%
• Voorlichting in organisatie	8%
• Bemiddeling in lopende zaken	6%
• Advies aan leidinggevenden en management	3%
• Onderzoeken van de (vermoede) misstand	1%
• (Advisering omtrent) de afdoening	1%
• (Betrokkenheid bij) ontwikkelen integriteitsbeleid	4%
• Registratie en/of jaarverslag	1%

De vertrouwenspersoon heeft de belangrijke taak de medewerker die bij hem komt te wijzen op de mogelijkheden die er zijn om een probleem of dilemma aan te pakken, of waar/hoe een melding te doen en hem hierover te informeren. Dit doet hij veelal in een persoonlijk gesprek. In dit gesprek hoort de vertrouwenspersoon niet alleen aan, maar houdt hij de medewerker ook een spiegel voor en biedt hij de mogelijkheid tot reflectie.

Profiel van een vertrouwenspersoon

Uit de themamiddag rolde het volgende profiel van de vertrouwenspersoon:

- Empatisch vermogen (van nature over beschikken en verder uitbouwen middels opleiding).
- Ervarenheid/wijsheid/volwassenheid (onafhankelijk van leeftijd).
- Laagdrempelig en bekend (bijv. makkelijk vindbaar op intranet).
- Voorlichting kunnen geven met diverse werkvormen (presentatie, spel) en bij diverse doelgroepen (introductie nieuwe medewerker, managementopleiding).
- Flexibel (op 3 manieren: als persoon, in tijd en bijv. op vrije dagen/'s avonds/in het weekend beschikbaar zijn).
- Bevlogen (dit is de basis voor het vertrouwenspersoonschap!).
- Sterk gevoel voor integriteit (van nature over beschikken en verder uitbouwen middels opleiding).

---

2 Zie voor meer informatie ook: <www.integriteitoverheid.nl/dossiers/integriteitsmanagement.html>.

3 'Luisterend Oor', onderzoek naar het interne meldsysteem integriteit binnen de Nederlandse overheid – VU&BIOS 2012.

4 'Veilig misstanden melden op het werk', Evaluatie Onderzoeksraad Integriteit Overheid en Adviespunt Klokkenluiders, evenals 'Besluit Melden Vermoeden van Misstand Rijk en Politie' en 'Tijdelijk Besluit Commissie advies- en verwijspunt Klokkenluiden', Berenschot, juli 2014.

5 'Luisterend Oor', onderzoek naar het interne meldsysteem integriteit binnen de Nederlandse overheid – VU&BIOS 2012.

Een opleiding is essentieel voor de vertrouwenspersoon, omdat er een aantal dingen aan- of afgeleerd moeten worden:
- Conflictbeheersing (ook al ben je geen bemiddelaar, hier moet de vertrouwenspersoon wel kennis van hebben).
- Gespreksvaardigheden.
- Omgaan met emoties.
- Psychische problematiek herkennen en weten wanneer en waarnaar je doorverwijst.

Na de opleiding moet ook nog een aantal zaken geregeld zijn:
- Intervisie en uitwisseling met collega-vertrouwenspersonen.
- Up to date blijven van vakgebied en nieuwe ontwikkelingen/wetten etc.
- Op de hoogte zijn wat er speelt in de organisatie, wat er verandert (en daarop inspelen).
- Diversiteit van vertrouwenspersonen (jong/oud/culturele achtergrond/man/vrouw/intern/extern etc.) om de drempel zo laag mogelijk te maken.

Combinatiefunctie compliance officer en vertrouwenspersoon

In de financiële wereld is een belangrijk vraagstuk of de functie van compliance officer gecombineerd kan worden met de functie van vertrouwenspersoon. Dat lijkt heel praktisch en efficiënt, waarbij twee vliegen in één klap kunnen worden geslagen. Om dit vraagstuk te beantwoorden, zetten we een stapje terug.

Het onderdeel incidenten van het integriteitsbeleid bestaat uit een aantal taken:
- Het (vertrouwelijk) ondersteunen van medewerkers bij integriteitdilemma's, bij adviesvragen (over bijv. regelingen en procedures) en bij vermoedens van een schending of overtreding.
- Het innemen van de melding van een incident (loketfunctie) en het verkrijgen van de benodigde informatie (intake).
- Het onderzoeken van de melding in opdracht van het management en hierover rapporteren.
- Het afhandelen en adviseren over, dan wel het opleggen van een straf.

De taken met betrekking tot incidenten betreffen dus niet alleen wetgeving, niet alleen juridische, imago- of financiële risico's, maar ook dilemma's, meldingen en adviesvragen. Het bespreken van deze laatste zaken kunnen ook een preventieve functie hebben en 'erger' voorkomen.

De rol van de compliance officer kan als volgt worden beschreven:

De compliance officer is de toezichthouder voor wat betreft de naleving, beheersing en implementatie van wet- en regelgeving. Hij analyseert periodiek de compliancerisico's en vormt hierover een eigen onafhankelijk oordeel. De compliance officer is de stimulator van cultuur en gedrag. Met zijn actieve en sturende participatie in de volledige managementcyclus (PDCA-cyclus) ten aanzien van de compliance met wet- en regelgeving, ondersteunt hij actief het lijnmanagement bij hun integrale verantwoordelijkheid voor de naleving op de wet- en regelgeving.[6]

De compliance officer staat dicht bij de organisatie en dat zou de (perceptie van) onafhankelijkheid als vertrouwenspersoon kunnen belemmeren. Daarnaast moet de compliance officer het beleid en de regels van de organisatie uitdragen, deze bewaken en er toezicht op houden. Het bedrijfsbelang staat hierbij hoog in het vaandel en dit kan botsen met het (individuele) medewerkersbelang waarvoor de vertrouwenspersoon staat.

De rol van de vertrouwenspersoon bestaat vooral uit luisteren, meedenken, klankborden en adviseren. Een belangrijke component hierbij is de vertrouwelijkheid: de medewerker kan in vertrouwen een gesprek voeren zonder dat hij bang hoeft te zijn dat hij de regie kwijt raakt.

De combinatie van de functies compliance officer en vertrouwenspersoon levert een aantal spanningsvelden op. Enerzijds voor de compliance officer (het scheiden van conflicterende rollen) en anderzijds voor de medewerker (het kan gevoeld worden als een drempel om het gesprek aan te gaan).
De compliance officer is aangesteld om te zorgen voor de naleving van wet- en regelgeving. Dit kan een drempel vormen voor collega's om vertrouwelijk te sparren over hun dilemma en wellicht angst voor een 'wijzend vingertje' geven. Dat laatste hoeft niet te gebeuren; veel compliance officers kunnen hun verschillende rollen wel scheiden, maar de perceptie van de medewerker kan anders zijn.

Daarnaast is de compliance officer vaak de aangewezen persoon om het onderzoek naar een mogelijk incident of overtreding uit te voeren. Een vertrouwelijk gesprek over een meldenswaardig incident dat de medewerker eigenlijk

6 Uit de beschrijving van de inrichting van het opgedragen toezicht, Rabobank, 2012.

niet wil melden, kan een dilemma opleveren voor de vertrouwenspersoon die ook compliance officer is. Vanuit die laatste functie zal hij zich geroepen voelen om toch iets te doen, terwijl de vertrouwenspersoon dit niet hoeft of zal willen. Het is dus maar de vraag of deze functies te combineren zijn en of dit in het belang van de medewerker – en in het belang van de compliance officer of vertrouwenspersoon – is.

Bij een niet-combinatiefunctie kan de vertrouwenspersoon de medewerker laten bepalen wat hij wil. Het organisatiebelang weegt vanzelfsprekend ook mee, maar in principe weegt het medewerkersbelang het zwaarst (behoudens wettelijke verplichtingen). Van een compliance officer wordt waarschijnlijk een andere afweging verwacht en zal het organisatiebelang meestal het zwaarst wegen.

Combinatiefunctie vertrouwenspersoon integriteit en vertrouwenspersoon ongewenste omgangsvormen

In de meeste organisaties is er al enige jaren een vertrouwenspersoon ongewenste omgangsvormen aanwezig. De vertrouwenspersoon integriteit bestaat echter nog niet zo lang en de meeste organisaties zijn er nog niet zo lang mee bezig. Een actueel vraagstuk is of dit twee verschillende functies zijn die gescheiden moeten worden gehouden, of dat deze functies juist vergelijkbaar zijn en daardoor gecombineerd kunnen worden.

In de praktijk blijkt dat men vooral de verschillen tussen de vertrouwenspersoon integriteit (VPi) en de vertrouwenspersoon ongewenste omgangsvormen (VPo) ziet. De belangrijkste zaken die steeds weer genoemd worden:

- Bij de VPo is de medewerker het slachtoffer, bij de VPi is de medewerker slechts omstander.
- Bij de VPo betreft het de medewerker zelf, bij de VPi betreft het de organisatie.
- De VPo is emotioneler en raakt mensen; de VPi is zakelijk en afstandelijk.
- Bij Ongewenste Omgangsvormen bepaalt de klant en hij heeft altijd de regie. Bij integriteit moet hiervan soms van afgeweken worden.
- De VPo bestaat op basis van arbo-wetgeving, voor de VPi zijn er geen verplichtingen.

Er zijn inderdaad verschillen te benoemen tussen beide vakgebieden en de inrichting van de functies. Dit is vooral historisch zo gegroeid; de VPo bestaat al sinds de jaren '80 en de Vpi pas sinds deze eeuw. In de praktijk zie je de vakgebieden echter steeds meer naar elkaar toe groeien en bij veel organisaties worden ongewenste omgangsvormen zelfs als een uitingsvorm van een integriteitschending gezien. Ongewenste omgangsvormen vallen daarmee dus onder integriteit; in de praktijk zijn het allebei uitingsvormen van ongewenst gedrag. Er komen ook steeds meer VPio's (combinatie van de functie VPo en VPi) en minder Vpi's, wat te merken is aan het animo voor de verschillende vertrouwenspersoonopleidingen. Naast praktische en financiële overwegingen vanuit de organisatie, kiezen vertrouwenspersonen vaak ook uit principiële overwegingen voor de combinatie.

Ik ben al jaren uitgesproken voorstander van de combinatiefunctie van VPi en VPo (dus VPio), net als de deelnemers van de themamiddag, zo bleek uit hun reacties. De belangrijkste reden hiervoor is dat de rol in beide gevallen precies hetzelfde is, namelijk vooral die van luisterend oor. Het maakt niet uit naar wat voor soort probleem de vertrouwenspersoon luistert, daar wordt geen onderscheid in gemaakt. Dit voorkomt de vervelende situatie dat hij medewerkers moet doorsturen naar een andere vertrouwenspersoon.

Medewerkers kiezen de vertrouwenspersoon vaak op gevoel, het soort type dat ze aanspreekt en niet op het soort probleem dat ze hebben (integriteit of ongewenste omgangsvormen). Dat onderscheid is vaak ook lastig te maken. Het is vervelend om je hele verhaal te vertellen aan een vertrouwenspersoon, om vervolgens te horen dat je bij de verkeerde zit! De combinatiefunctie voorkomt dit; er is één loket en je zit altijd goed. Tenzij het over arbeidsconflicten gaat, een veel gehoord onderwerp van gesprek...

Belangrijk hierbij is om de vertrouwenspersoon goed op te leiden en toe te rusten voor zijn taak. Er zijn verschillende regels en procedures voor ongewenste omgangsvormen en integriteit. De vertrouwenspersoon moet de relevante regels en procedures op beide vakgebieden kennen en kunnen toepassen. Het onderscheidingsvermogen ligt nu bij de vertrouwenspersoon (i.p.v. bij de medewerkers); die zal de goede weg moeten kiezen. Daartoe is een goede opleiding onontbeerlijk. Vertrouwenspersoonschap is echt een vak dat serieus genomen moet worden en dat je er niet zomaar even bij kunt doen!

Drs. Sacha Spoor (1968) is sinds 2008 als senior advisor en trainer verbonden aan het European Institute for Business Ethics (EIBE) van Nyenrode Business Universiteit.

DNB's 'Good practices bestrijden corruptie' onder de loep

Ruud van der Mast

In 2013 heeft De Nederlandsche Bank (DNB) een thema-onderzoek uitgevoerd bij banken en verzekeraars. Het onderzoek richtte zich op corruptie en de bestrijding hiervan in de financiële sector. Uit dit onderzoek is gebleken dat marktpartijen behoefte hebben aan meer informatie en houvast om corruptie effectief te kunnen voorkomen en bestrijden. Op 6 maart 2014[1] kwam DNB tegemoet aan deze oproep met de publicatie van een aantal 'good practices'. In dit artikel beschouwen we de good practices van DNB vanuit een compliance-oogpunt.

Het document heeft geen formele juridische status, maar als toezichthouder zal DNB, naar verwachting, kritisch zijn ten aanzien van organisaties die de good practices in de wind slaan. Als compliance officer adviseer ik u dan ook de good practices goed te bestuderen en wanneer wordt besloten om hiervan af te wijken, dit goed te onderbouwen.

DNB heeft het document onderverdeeld in twee delen:

I. Beheersen corruptierisico
II. Maatregelen

Voor het gemak houd ik deze verdeling in dit artikel aan.

I. Beheersen corruptierisico

Teneinde de corruptierisico's goed te kunnen beheersen beveelt DNB aan allereerst een risicoanalyse uit te voeren om inzichtelijk te krijgen welke risico's de organisatie precies loopt. DNB onderscheidt daarbij de volgende risico's:

- geografisch risico;
- sectorrisico;
- product-/transactierisico;
- *third party*-risico;
- het risico 'persoonlijke netwerken en belangen'.

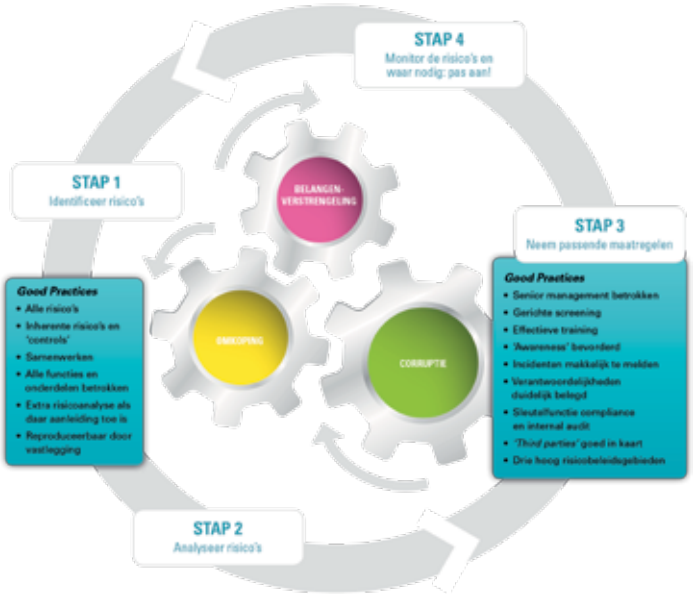
Om de aanbeveling ten aanzien van de risicoanalyse kracht bij te zetten wordt verwezen naar de wettelijke plicht voor het uitvoeren van een systematische risicoanalyse, vastgelegd in artikel 10 Besluit prudentiële regels Wft (Bpr). Helemaal vrijblijvend is deze analyse dus niet.

1 <www.toezicht.dnb.nl/7/50-230098.jsp>

Om van analyse naar daadwerkelijke beheersing te gaan beveelt DNB aan een 4-stappenplan te volgen.

1. Identificeer risico's
2. Analyseer risico's
3. Neem passende maatregelen
4. Monitor de risico's en waar nodig: pas aan!

In dit stappenplan worden de eerder genoemde, veel voorkomende risico's in kaart gebracht en toegelicht. De lezer kan bij een aantal risico's direct een link leggen met risico's die ook worden onderscheiden bij klantintegriteit. Hier kijken we bijvoorbeeld ook naar product-, sector-, transactie- en geografische risico's. Het is dan ook passend om bij het beoordelen van klantintegriteit tevens het corruptierisico in te schatten; DNB ziet bijvoorbeeld bij *private banking* een hoger risico vanwege de nauwe klantrelatie. Het corruptierisico beperkt zich echter niet tot de doelgroep klanten, maar is ook van toepassing op *third parties* en medewerkers.



Figuur: In de 'good practices' presenteert DNB onder andere een risicobeheersingscyclus die wordt voorgesteld als standaard voor alle banken en verzekeraars. Een standaard die deze marktpartijen in staat zou moeten stellen passende maatregelen te nemen om risico's in relatie tot corruptie en omkoping te beheersen.

De *good practices* die DNB ten aanzien van de compliancerisicoanalyse beschrijft zijn, in mijn opinie, niet baanbrekend te noemen. *Good practices* als betrokkenheid senior management, bepalen van *risk appetite*, periodiek uitvoeren van een analyse en reproduceerbare vastlegging zal veel organisaties bekend in de oren klinken. Mogelijk is het voor een aantal organisaties wel nieuw om de specifieke risico's ten aanzien van corruptie in deze analyse op te nemen waar het op dit onderwerp eerder beperkt was tot risico's ten aanzien van belangenverstrengeling. Wanneer u zich afvraagt welke risico's dan opgenomen moeten worden, geeft het document van DNB een goede aanzet.

II. Maatregelen

Na het uitvoeren van de risicoanalyse is in beeld welke risico's daadwerkelijk beheerst moeten worden en kunnen passende maatregelen geïmplementeerd worden. Hierbij denkt DNB aan maatregelen op het gebied van organisatie, cultuur, governance, *third party*-risico en andere beleidsgebieden. Het is uw rol als compliance officer om het bestuur over deze maatregelen te adviseren.

Ten aanzien van cultuur beschrijft DNB het belang van de betrokkenheid van hoger management, het inrichten van een incidenten- en klokkenluidersregeling en het creëren van awareness bij verschillende (maar wel alle!) doelgroepen. Het risico op corruptie is hoger naarmate een functie meer mandaat bevat, maar om corruptie en belangenverstrengeling effectief te bestrijden dient de gehele organisatie op de hoogte te zijn van de risico's en hoe deze te signaleren.

Voor het creëren van awareness geeft DNB een aantal *good practices* zoals zij deze tijdens haar onderzoek bij marktpartijen is tegengekomen. Hoewel een aantal nuttige tips en voorbeelden wordt genoemd, zijn deze (awareness-)maatregelen niet nieuw voor de sector. De winst zit hem juist in het daadwerkelijk toepassen van deze maatregelen in plaats van het voor kennisgeving aannemen.

DNB geeft op het gebied van cultuur ook een *good practice* ten aanzien van het uitvoeren van (pre) employment screening. Dit specifieke voorbeeld is interessant, omdat het verder gaat dan wat gebruikelijk is in de sector. DNB benoemt expliciet het gevaar van bepaalde persoon-

lijkheidskenmerken en stelt voor om deze kenmerken en risico's in kaart te brengen en te analyseren tijdens de sollicitatieprocedure. Hierdoor kan een beter beeld gevormd worden over het karakter van de sollicitant; een nadeel is dat dit veel tijd kost. Vanuit praktisch oogpunt zou dit daarom met name een goede maatregel zijn voor integriteitsgevoelige functies en dient deze *best practice* risicogebaseerd te worden toegepast.

Op het gebied van governance adviseert DNB om de taken, verantwoordelijkheden en managementinformatie onder de loep te nemen bij het vaststellen, implementeren, reviewen, monitoren en updaten van beleid en procedures. DNB deelt hierbij expliciet een rol toe aan senior management, compliance en audit. Compliance wordt hierbij geacht om minimaal twee keer per jaar aan het bestuur en de raad van commissarissen te rapporteren over het beleid en incidenten ten aanzien van corruptie.

Ten aanzien van het *third party*-risico is DNB meer specifiek in de aanbevelingen. Vermoedelijk omdat de analyse van dit risico voor veel organisaties relatief nieuw is. DNB adviseert marktpartijen in hun *third party*-beleid onder andere een kwalificatie en classificatie van de risico's, een relation due diligence, een escalatiemogelijkheid, een *right to audit*, een 4-ogen principe en een betalingsmonitoring op te nemen. Beschouwend zijn dit essentiële maatregelen om het corruptierisico te kunnen beheersen. Veel organisaties hebben er al voor gekozen om hun CDD-beleid uit te breiden naar een RDD beleid waarin de 'C' van *customer* wordt vervangen door een 'R' van *relation*. Effectief betekent dit dat er ook een integriteitsonderzoek en risicoclassificatie plaatsvindt bij het aangaan van relaties met bijvoorbeeld samenwerkingspartners om, onder andere, het corruptierisico te kunnen beheersen.

Als laatste beschouw ik het advies van DNB met betrekking tot het drietal hoogrisicobeleidsgebieden. Dit zijn:

1. *'Gifts, hospitality & entertainment',*
2. 'donaties, liefdadigheid en sponsoring' en
3. de 'persoonlijke netwerken en belangen'.

Het corruptierisico bij deze onderwerpen is hoog. Daarom geeft DNB gedetailleerde *good practices* om het corruptierisico te beheersen. Hoewel de aanbevelingen ook hier niet baanbrekend zijn, is wederom de grote winst te behalen in het daadwerkelijk doorvoeren van deze *good practices* in de eigen organisatie. Ik adviseer compliance officers dan ook om aan de hand van de aanbevelingen van DNB het huidige beleid te reviewen en waar nodig aan te passen of uit te breiden.

Overwegend

Hoewel de aanbevelingen in het document 'Good practices bestrijden corruptie' voor veel organisaties bekend in de oren zouden moeten klinken, is het goed dat DNB haar aanbevelingen op een rijtje heeft gezet. Het is mijn ervaring dat veel organisaties wel weten hoe het zou moeten, maar dat de daadwerkelijke uitvoering moeilijk of niet te realiseren is.

DNB geeft een nuttig overzicht van de belangrijkste risico's die in het kader van corruptie kunnen worden onderscheiden. Deze risico's kunnen marktpartijen toevoegen aan hun compliancerisicoanalyse voor zover deze nog niet uitgebreid was met corruptierisico's. De analyse van deze risico's zal echter door elke instelling afzonderlijk uitgevoerd moeten worden en hier kunnen de *good practices* prima voor worden gebruikt.
Mijn advies is dan ook om het document kritisch te bestuderen en de relevante *good practices* op te volgen.

Ruud van der Mast is directeur bij het Nederlands Compliance Instituut. Voor meer informatie kunt u contact met hem opnemen. Tel. 088 99 88 100 of vandermast@compliance-instituut.nl.

Is de auditor de controleur aan het monitoren...

Adriaan van Verseveld

Controle... Monitoring... Audit... Spraakverwarring... Allemaal hetzelfde of toch niet?

Tijdens Module 5 van de Leergang Compliance Professional komen deze begrippen aan bod. Vele malen is mij, als docent verbonden aan deze module, de vraag gesteld wat de verschillen zijn tussen deze termen. In deze bijdrage schep ik hier graag wat duidelijkheid in.

Om een goed beeld van de begrippen te krijgen is het van belang om inzicht te hebben in het 'three lines of defence-model', dat tegenwoordig vrij algemeen gebruikt wordt om de beheersing van de organisatie in te richten. Het model van three lines of defence is erop gebaseerd dat de eerste lijn verantwoordelijk is, dat de tweede lijn, bestaande uit o.a. compliance, risk en legal, ondersteunend is aan de eerste lijn en dat de derde lijn zich onafhankelijk een oordeel vormt over het functioneren van de eerste en de tweede lijn. In elk van de drie lijnen komen werkzaamheden voor die in het normale taalgebruik als controlerend worden gezien. Ze verschillen echter van aard en daarom is het van belang onderscheid te maken tussen de begrippen controle, monitoring en audit.

Eerste lijn: controle

De term controle is van toepassing op de activiteiten die in de eerste lijn (of beter gezegd: binnen de normale bedrijfsvoering) worden ondernomen, om te bezien of de werkzaamheden worden uitgevoerd op een manier die past bij de opdracht en in lijn zijn met de werkinstructies. R.W. Starreveld hanteert de volgende definitie voor het begrip controle.

'Controle omvat het geheel van maatregelen om:

- *vast te stellen of hetgeen in de onderneming wordt verricht in overeenstemming is met gegeven opdrachten, respectievelijk of daarvan bij de uitvoering op gegronde motieven is afgeweken, en*
- *te constateren dat op de verschillende hiërarchische niveaus gedelegeerde bevoegdheden op de juiste wijze zijn gehanteerd.'*[1]

1 R.W. Starreveld, O.C. van Leeuwen en H. van Nimwegen, Bestuurlijke informatieverzorging deel 1: algemene grondslagen, Groningen: Noordhoff Uitgevers 2002.

Het doel van controle is om vast te stellen dat gewerkt wordt zoals is afgesproken en dat fouten tijdig kunnen worden hersteld. Het zijn dus activiteiten of processen om tijdige identificatie en bijstelling van fouten te bewerkstelligen.

Tweede lijn: monitoring
Monitoring vindt doorgaans plaats binnen de tweede lijn. Monitoring kan (bezien vanuit de optiek van de compliance officer) worden omschreven als:

'Het op systematische wijze verzamelen van overtuigende informatie over de naleving van interne en externe regels, om vast te stellen in hoeverre de organisatie voldoet aan interne en externe regels.'

Op basis hiervan kan over de naleving gerapporteerd en geadviseerd worden aan het management.

Compliance monitoring richt zich dan ook primair op de naleving van wet- en regelgeving en interne regels en daarnaast ook op de cultuuraspecten binnen de organisatie. Het gaat hierbij om de activiteiten of processen met als doel de tijdige identificatie en bijstelling van de oorzaak van fouten.

Derde lijn: audit
Een audit vindt in beginsel plaats vanuit de derde lijn, oftewel de interne auditafdeling (en bij het ontbreken van een auditafdeling door een externe auditor). Audit richt zich primair op de interne beheersing en betrouwbaarheid van de processen. De taakopdracht van de auditafdeling wordt in artikel 5.3 van de Code Banken als volgt gedefinieerd:

'5.3 De interne auditfunctie heeft tot taak te beoordelen of de interne beheersmaatregelen in opzet, bestaan en in werking effectief zijn. Daarbij ziet zij onder meer op de kwaliteit en effectiviteit van het functioneren van de governance, het risicobeheer en de beheersprocessen binnen de bank. De interne auditfunctie rapporteert over de bevindingen aan de raad van bestuur en de auditcommissie.'

Bij audit gaat het erom dat een afdeling die 'niet direct bij de normale bedrijfsvoering' is betrokken, op basis van haar onafhankelijke onderzoek, een redelijke zekerheid kan verschaffen aan de raad van bestuur over de kwaliteit van de bedrijfsvoering binnen de financiële instelling. Hierbij dient te worden opgemerkt dat de auditor strikt genomen enkel een verifiërende en signalerende functie heeft.2

Verschillen
Als belangrijkste verschillen tussen controle, monitoring en audit kunnen worden genoemd:
- Controles worden doorgaans uitgevoerd door speciaal daartoe aangewezen medewerkers binnen de normale bedrijfsvoering (de eerste lijn). Monitoring wordt door de tweede lijn uitgevoerd en audit door de interne auditafdeling (derde lijn).
- Controle richt zich met name op een juiste invulling van processen en werkinstructies ('de fout'). Compliance monitoring daarentegen richt zich primair op de naleving van wet- en regelgeving en interne regels ('de oorzaak van de fout'). Audit richt zich primair op de interne beheersing en betrouwbaarheid van de processen.

Tenslotte: In reactie op de vraag zoals beschreven in het begin, krijgen we vaak terug dat de begrippen monitoring, controle en audit allemaal hetzelfde zijn, namelijk controlewerkzaamheden die de eerste lijn alleen maar weerhouden van het echte werk.

Gelukkig onderkennen veel mensen wel het nut van deze systematiek van drie defensielijnen. Op deze manier kunnen we gezamenlijk een beheerste en integere bedrijfsvoering nastreven door elkaar scherp te houden op gemaakte fouten en de oorzaken ervan.

Adriaan van Verseveld is senior compliance officer bij het Nederlands Compliance Instituut. Voor meer informatie kunt u contact met hem opnemen. Tel. 088 99 88 100 of vanverseveld@compliance-instituut.nl.

2 J. Hoving en W.M.L. Keulemans, Risicomanagement: Grondslagen voor een integrale en interdisciplinaire aanpak, NIBE-SVV eerste druk, 2008.

Opzetten van een privacyrisicoanalyse: be prepared!

Marit Klapwijk

Op 12 maart 2014 heeft het Europees Parlement haar standpunt over de Algemene Verordening Gegevensbescherming gepubliceerd (eerste lezing) en het gewijzigde voorstel is toen met grote meerderheid aangenomen. Hoewel het nog even zal duren voor de verordening daadwerkelijk in werking treedt, is het verstandig om hier nu al op te anticiperen. In deze verordening staan veel ingrijpende veranderingen op het gebied van privacy, die een grote impact zullen hebben op de bedrijfsvoering. Door de verordening komt privacy bij veel organisaties (weer) hoger op de agenda te staan.

Daarnaast heeft het initiatief van ING om in de toekomst klantgegevens voor commerciële doeleinden te verstrekken aan derden veel stof doen opwaaien. De discussie over 'big data' is hierdoor in een versnelling gekomen. Gegevensbescherming en big data zijn onderwerpen die door de Verordening en door initiatieven van het bedrijfsleven meer in de belangstelling komen te staan Daarom wil ik in deze bijdrage een aantal handige tips bespreken voor het maken van een privacyrisicoanalyse.

Waarom nu?

Zoals al aangestipt laat de Algemene Verordening Gegevensbescherming nog even op zich wachten. Toch is het aan te raden nu al een inventarisatie van privacyrisico's te maken. Het maken van een risicoanalyse op basis van slechts de Wbp en de gedragscode is al zeer tijdrovend. De winst die de organisatie kan behalen met de privacyrisicoanalyse is dat de organisatie nu al een beeld heeft van hoe deze ervoor staat op het gebied van de verwerking van persoonsgegevens. Dat is nuttig omdat in de verordening een Privacy Impact Assessment verplicht is gesteld. De risicoanalyse die dan al is gemaakt, maakt het maken van deze impact assessment dan ook veel gemakkelijker, omdat de bedrijfs- en verwerkingsprocessen al in kaart zijn gebracht.

De Algemene Verordening Gegevensbescherming

Hoewel de exacte inhoud van de verordening nog niet bekend is, zijn er wel een aantal onderwerpen waarvan de kans groot is dat deze in de verordening terug zullen komen. Alleen de exacte invulling ervan is nog niet bekend. Een aantal voorbeelden zijn:

- verplichting tot het aanstellen van een privacy officer;
- verhoging van de boetes tot € 100.000.000,- of 5% van de wereldwijde jaaromzet;
- verplichting tot het uitvoeren van een Privacy Impact Assessment;
- melden van datalekken binnen 72 uur;
- 'right to erasure': recht om gegevens te laten wissen;
- oestemming CBP nodig voor doorgifte persoonsgegevens aan overheidsorganen buiten de EU;
- zelfstandige verantwoordelijkheid van bewerkers.

Het CBP

In Nederland houdt het College bescherming persoonsgegevens toezicht op de Wet bescherming persoonsgegevens en zal straks eveneens toezicht gaan uitoefenen op grond van de Algemene Verordening Gegevensbescherming.

Wetgeving
Op het moment dat je als organisatie een privacyrisico-analyse wil uitvoeren, is het verstandig om de huidige wetgeving als uitgangspunt te gebruiken. In dit geval zijn dat de Wbp en eventuele van toepassing zijnde gedragscodes.

Gedragscodes zijn niet vrijblijvend
Het CBP kan op verzoek een goedkeurende verklaring afgeven voor een bepaalde gedragscode. Deze gedragscode vormt dan een nadere uitwerking van de bepalingen uit de Wbp. Het CBP houdt een register bij van gedragscodes waar het een goedkeurende verklaring voor heeft afgegeven, waaronder bijvoorbeeld de Gedragscode verwerking persoonsgegevens financiële instellingen. Deze gedragscode is van toepassing op banken die lid zijn van de Nederlandse Vereniging van Banken (NVB), aangesloten zijn bij Rabobank Nederland en op verzekeraars die lid zijn van het Verbond van Verzekeraars. De bepalingen uit deze gedragscode zullen daarom ook moeten worden meegenomen in de risicoanalyse indien deze van toepassing is.

Hulpmiddelen
Het CBP heeft op haar website een aantal handige hulpmiddelen staan om een risicoanalyse te maken of aan de hand waarvan de risicoanalyse opgezet kan worden:

- De Quickscan: is bedoeld voor het bevorderen van het privacybewustzijn in de organisatie en het bepalen van de plaats van de organisatie op de kwaliteitsschaal van de gegevensverwerking.
- WBP Zelfevaluatie: is bedoeld voor het verkrijgen van inzicht in het toepassen van de Wbp in de organisatie en het nader bepalen van de plaats van de organisatie op de kwaliteitsschaal van de gegevensverwerking.
- Raamwerk Privacy Audit: is bedoeld als basis voor het beoordelen van de kwaliteit van de bescherming van persoonsgegevens over de gehele verwerking. Hier hoort ook een handreiking bij.

Daarnaast heeft ook het Verbond van Verzekeraars voor hun leden een Model Zelfevaluatie ontwikkeld op basis van de Gedragscode verwerking persoonsgegevens financiële instellingen. In deze zelfevaluatie zijn de normen uit de Wbp en de gedragscode verder uitgewerkt en specifiek voor verzekeraars aangepast. Aan de hand daarvan kan men direct het risico benoemen wat hieruit voort vloeit.

Voor compliance officers van verzekeraars is de opzet dus iets gemakkelijker te maken, maar voor andere compliance officers biedt naar mijn mening de WBP Zelfevaluatie het meeste houvast. Het Raamwerk Privacy Audit is geschikter voor compliance officers die al audit ervaring hebben of de internal auditors binnen de organisatie. De Quickscan is te globaal om een risicoanalyse mee op te zetten.

Verschillende risicocategorieën
De meeste risico's uit een privacyrisicoanalyse zijn te verdelen in reputatierisico's en toezichthouderrisico's. Hierbij kan bij reputatierisico gedacht worden vanuit het klantperspectief of het risico dat de organisatie in het (landelijke) nieuws komt door verkeerd gebruik of verlies van persoonsgegevens. Het toezichthouderrisico bestaat uit bijvoorbeeld een onderzoek, een dwangsom of een boete van het CBP. Waar bij het bepalen van de impact in de risicoanalyse mijns inziens ook rekening mee gehouden moet worden, is het soort gegevens dat verwerkt wordt. Bijzondere gegevens zoals strafrechtelijke en medische gegevens vereisen bijzondere aandacht. Bij verlies van deze gegevens bestaat ook het risico dat klanten hiervoor gecompenseerd willen worden.

Ik adviseer organisaties om nu al met de privacyrisicoanalyse te beginnen. De Verordening lijkt nog ver weg, maar gezien de hoeveelheid aan extra werk die de Verordening de organisaties brengt, ben je als organisatie al snel te laat gestart.

Marit Klapwijk is junior compliance officer bij het Nederlands Compliance Instituut. Voor meer informatie kunt u contact met haar opnemen. Tel. 088 99 88 100 of klapwijk@compliance-instituut.nl.

Aankomende wetswijzigingen voor trustkantoren

Tom van Middelkoop

De nieuwe Regeling integere bedrijfsvoering (Rib) treedt, naar verwachting, op 1 januari 2015 in werking. De huidige Rib is een toezichthouder-regeling. Bij de evaluatie van de Wet toezicht trustkantoren (Wtt) in 2010 was één van de aanbevelingen om de toezichthouderregeling te veranderen in een ministeriële regeling. De nieuwe regeling is een ministeriële regeling geworden. De aanscherping heeft in het bijzonder effect op de inrichting van de compliancefunctie en de auditfunctie.

De controlefunctie wordt in de huidige Rib impliciet genoemd in artikel 7. Het vernieuwde artikel 7 stelt dat het trustkantoor zorg dient te dragen voor een onafhankelijke en effectieve uitvoering van de auditfunctie ten aanzien van haar werkzaamheden en de compliance-functie. De auditfunctie heeft als taak de controle op de naleving van de wet en het procedurehandboek door het trustkantoor en de uitvoering van de compliancefunctie. De uitvoering van werkzaamheden, compliance en audit moeten van elkaar zijn gescheiden. Een bestuurder mag geen auditfunctie uitoefenen en men moet de onafhan-kelijkheid van de compliancefunctie waarborgen.

De compliancefunctie monitort het trustkantoor op naleving van de Wtt, de onderliggende regeling en het eigen procedurehandboek. Naar gelang er meer afstand is tussen de compliancefunctie en de uitvoering van werkzaamheden, zal de auditfunctie minder intensief kunnen zijn. Voor de vereiste intensiviteit van de audit-functie zijn verder de complexiteit en het risicoprofiel van de dienstverlening van belang.

Wijzigingen Wwft per 1 januari 2015

Door de Wijzigingswet financiële markten 2015 wordt de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) gewijzigd. Een aantal wijzigingen hebben gevolgen voor de Trustsector.

Melden onsuccesvol cliëntonderzoek of beëindigen relatie

De voorgestelde wijzigingen in de Wwft legt trustkantoren enkele verplichtingen op wanneer een cliëntonderzoek niet succesvol kan worden volbracht en men daardoor afscheid neemt van de relatie of deze niet accepteert. Indien bijvoorbeeld de uiteindelijk belanghebbende of het doel van de zakelijke relatie niet kan worden vastgesteld én er indicaties van betrokkenheid bij witwassen of terrorismefinanciering zijn, moet een melding worden gedaan bij de Financiële inlichtingen eenheid (FIU-NL). Van deze verplichting waren trustkantoren tot nog toe uitgezonderd.

Verificatie identiteit van instellers, trustees, vennoten en beheerders

Artikel 11 van de Wwft schrijft voor aan de hand waar-van de identiteit van een cliënt wordt geverifieerd. Die bepaling houdt op dit moment nog geen rekening met de sinds 1 januari 2013 geldende bepalingen voor de identificatie en verificatie van instellers en trustees, vennoten en de personen bevoegd met het beheer van een personenvennootschap. Met de wijziging wordt bewerkstelligd dat de eisen van artikel 11 ook op hen van toepassing zijn.

Implementatie vierde witwasrichtlijn

De vierde witwasrichtlijn, die vermoedelijk begin 2015 in werking zal treden, bevat verschillende wijzigingen. Na vaststelling van deze richtlijn zal duidelijk worden of en op welke punten de Nederlandse wetgeving aangepast zal moeten worden. In de nieuwe richtlijn is er zowel sprake van binnenlandse als buitenlandse PEP's. Daarnaast is het ook van toepassing op niet-politieke functies, zoals bestuurders van internationale organisaties of onder-nemingen die een prominente publieke functie vervullen.

Laatste ontwikkelingen

Uit de wetgevingsbrieven op het terrein van de financiële markten blijkt dat het Ministerie van financiën van plan is de Wtt meer in lijn te brengen met de Wft en de Wwft.

Voorbeelden die genoemd zijn:

- Normen voor beheerste en integere bedrijfsvoering invoeren in de Wtt, naar model van artikel 3:17 Wft. Dit houdt in dat de bedrijfsvoering van trustkantoren zich moet richten op het beheersen van de risico's die het bedrijf van trustkantoor meebrengen.
- Invoering van de verplichting van minimaal twee dagelijks beleidsbepalers, naar model van artikel 3:15 Wft.
- Risicogebaseerde cliëntidentificatievereisten, naar model van de Wwft.

DNB en het Ministerie van financiën zijn in overleg over de volgende – voor trustkantoren nieuwe – handhavingsmaatregelen:

- Verruiming van de mogelijkheden van DNB om boetes en dwangsommen te publiceren.
- Bij structureel niet voldoen aan wettelijke normen en gebrek aan manieren om naleving af te dwingen, de mogelijkheid om de vergunning in te trekken.

Tom van Middelkoop is werkzaam bij het Nederlands Compliance Instituut. Voor meer informatie kunt u contact met hem opnemen. Tel. 088 99 88 100 of vanmiddelkoop@compliance-instituut.nl.

2 oktober	Themamiddag Actualiteiten Compliance & Governance bij pensioenfondsen en pensioenuitvoerders
7 oktober	LCP Module 4
9 oktober	Themamiddag Actualiteiten Compliance Trustsector
28, 29 & 30 oktober	LCO/LCP Module 3
29 & 30 oktober	LCP Module 5
4 november	LCP Competentietraining
4 november	LCOZ Module 1
5 november	LCO/LCP Module 2
11 november	LCOZ Module 3
11 november	LCP Module 4
11 november	LBW Module 2
13 november	Themamiddag Bitcoins en andere virtuele valuta
18 november	Update Compliance Verzekeraars 2014
18 november	LCOZ Module 3
18 november	LBW Module 3
19 november	Themamiddag Anti-corruptie
20 november	Nationaal integriteitscongres
25 november	LCOZ Module 4
25 november	LBW Module 4
27 november	Introductie Compliance
27 november	Themamiddag Moreel Ethische Verklaring
2 december	LCOZ Module 5
9 december	LCP Module 4
11 december	Nationaal Compliance Congres
16, 17 & 18 december	LCO/LCP Module 3
17 & 18 december	LCP Module 5

LCO: Leergang Compliance Officer
LCOZ: Leergang Compliance Officer in de Zorg
LCP: Leergang Compliance Professional
LBW: Leergang Bestrijding witwassen & terrorismefinanciering

Dorothé Beernink:

‘Uiteindelijk draait toch heel veel om gedrag’

Dorothé Beernink is sinds 2013 de enthousiaste Chief Compliance Officer van Equens SE. José Hooghiemstra praat met haar over haar werkgebied, de risk based benadering en de activiteiten van Equens: verwerking van betalingsverkeer. Een wereld waar we iedere dag meerdere malen mee te maken hebben, maar eigenlijk maar heel weinig van weten.

Wat doet Equens? 'Equens SE is een van de grootste betalingsverwerkers in Europa. Wij zorgen voor de verwerking van meer dan 10 miljard girale betalingen en bijna 5 miljard toonbankbetalingen en geldopnames transacties per jaar. Onze organisatie is in 2006 ontstaan uit een fusie tussen het Nederlandse Interpay en het Duitse Transaktionsinstitut für Zahlungsverkehrsdienstleistungen A.G. Sinds onze oprichting hebben we hard gewerkt aan het uitbouwen en versterken van onze Europese marktpositie, wat bijvoorbeeld blijkt uit de volledige integratie van onze Italiaanse dochteronderneming per 1 januari jl. We zijn een zelfstandige en commerciële organisatie. Naast ons hoofdkantoor in Utrecht hebben we vestigingen in Stuttgart, Frankfurt, Helsinki, Rome, Milaan en Londen.'

Waar staan jullie in het rijtje van de payment processors in de wereld? 'Onze ambitie is bij de Europese top drie te horen en we komen aardig in die richting. Er is concurrentie in verschillende vormen. In Nederland doen bijvoorbeeld CCV en Atos aan processing en er zijn andere grote spelers in Europa en daarbuiten. Met de komst van de uniforme Europese betaalmarkt SEPA (Single Euro Payments Area) is het een heel ander speelveld geworden, met internationale concurrentie. Dat betekent natuurlijk voor ons weer een hele uitdaging. Dynamiek is hier wel aanwezig!'

Hoe hebben jullie de crisis beleefd? 'Onze grootste klanten zijn de banken en in steeds meer gevallen ook corporates die rechtstreeks hun transacties bij ons kunnen aanleveren. De gevolgen van de economische crisis voelen we duidelijk. Banken zijn sterk gericht op het reduceren van kosten. Dat merken wij als service provider natuurlijk ook. Zelf hebben we ook de nodige wijzigingen doorgevoerd om efficiënter te kunnen werken. Kostenbeheersing blijft voorlopig een belangrijk punt, zowel vanuit het bankperspectief maar ook voor ons.'

Er vallen veel ontslagen bij de banken en verzekeringsbedrijven. Geldt dat ook voor jullie sector? 'In de financiële sector hebben al de nodige reorganisaties plaatsgevonden en ook in de toekomst zal ongetwijfeld nog het nodige veranderen. SEPA heeft het hele speelveld veranderd. Iedereen had een verandering verwacht qua kostendruk, maar niet de mate waarin die druk zou toenemen. Deze veranderingen vereisen van ons een flexibele houding . Wij implementeren diverse kostenbesparende programma's, gericht op efficiënter werken en optimalisering van onze bedrijfsvoering.'

Je hebt een imposante titel: manager Risk Management, Information Security & Compliance. Dit zijn drie werkgebieden waar bij andere bedrijven drie mensen voor nodig zijn. Leg eens uit. 'De afdeling waar ik voor werk staat bekend als center Risk Management. Deze term is wat verwarrend, want risicomanagement is ook een proces en voor ons een belangrijk aandachtsgebied. Wij zijn company-wide verantwoordelijk voor risicomanagement, informatiebeveiliging, business continuity en compliance. Wij zitten dus in de tweede "line of defence". De rollen binnen onze afdeling zijn verdeeld om goed focus te kunnen houden. Zo hebben we een Chief Information Security Officer (die tevens Chief Risk Officer is), een Chief Business Continuity Officer (tevens onze Chief Operating Officer) en ikzelf ben de Chief Compliance Officer. Naast mijn taak als Chief Compliance Officer stuur ik een team aan met experts.'

Hoe is compliance ingericht binnen dit geheel, hoe geef je het vorm? 'We hebben de scope van compliance gedefinieerd als wetten, regels, standaarden en ethische principes. De rules en regulations van de card schemes zoals Mastercard en Visa maken ook onderdeel uit van deze scope. We hebben het dus over wetgeving zoals Wft, card schemes rules en regulations, maar ook bijvoorbeeld de UK Bribery

> Het speelveld verandert, dus ook de compliance-eisen veranderen

Act, de locale wet- en regelgeving in de landen waar wij werkzaam zijn en uiteraard onze Code of Conduct.
Om dit zo goed mogelijk te kunnen doen zijn compliance officers werkzaam in de verschillende bedrijfsonderdelen en samen vormen we de compliance-organisatie. Iedere compliance officer heeft zijn eigen "expertise", zodat we ons totale werkgebied kunnen afdekken. De 'business' is heel belangrijk; zij doen het werk. Wij zorgen onder andere voor ondersteuning ,support en advies, maar de implementatie wordt door de business gedaan. De samenwerking is dus cruciaal.'

Jullie opereren heel internationaal en dat lijkt me ingewikkeld. 'Soms zorgt een situatie voor een spagaat, maar dat maakt het ook wel weer erg leuk. De uitdaging is: hoe houden we onze focus op alle gebieden? Compliance op zich is al ingewikkeld genoeg. We werken daarom heel nauw met Legal samen. Zij volgen de veranderingen in de wetgeving en wij vertalen dat naar de praktijk. Zo zijn er bijvoorbeeld in Italië een aantal specifieke wetten die voor ons van toepassing zijn, die volgen we dus op de voet. Daarnaast heeft Nederland natuurlijk ook specifieke wetgeving zoals de Wft. De veranderingen van de card scheme rules en regulations worden door Compliance gemonitord en samen met de organisatie wordt dan de impact bepaald. Ook vanuit de Europese commissie komen er nieuw regels en richtlijnen die we samen met Legal volgen. Ik verwacht dat de Europese commissie in de loop van de komende jaren weer veel zal veranderen.'

Compliance wordt als zeer complex ervaren, mede door de toenemende regelgeving die de crisis met zich mee brengt. Daarnaast wordt men opgeroepen om meer vanuit waarden te werken en minder vanuit wet- en regelgeving als startpunt. Leeft dat bij jullie? 'Wij hebben met elkaar een gedragscode (Code of Conduct) opgesteld. Wat verwachten wij van de medewerker en wat mag de medewerker van Equens verwachten? Uiteindelijk draait heel veel om gedrag. Je kunt wel zeggen dat je ergens aan moet voldoen, maar alleen het zeggen lost niets op, daar gaat niemand harder door lopen.'

Hoe stuur je dat dan aan? 'We hebben een verplicht e-learning programma ontwikkeld. De e-learning bestaat uit drie onderwerpen namelijk Compliance in algemene zin, de Code of Conduct en de "Gift, entertainment and anti-bribery policy". Daar hoort uiteraard ook een certificaat bij. Hierdoor onderstrepen we ook het belang wat we daaraan hechten. Verder hebben we een compliance game gespeeld met alle managementteams. Een elektronisch vragenspel met vragen als: "Wat doe je als je voor iets wordt uitgenodigd?" Om de collega's nog wat meer te prikkelen hebben we een competitie element toegevoegd, dat werkte heel positief! De collega's met de meeste punten kregen een prijs. Zo hopen we meer bewustheid te creëren over compliance.'

Je zit nu zo'n anderhalf jaar in deze rol. Heb je het gevoel dat je compliance goed neer hebt kunnen zetten? Hoe zag het er daarvoor uit? 'Voor Equens is compliance uiteraard belangrijk. Veel compliance-aspecten zijn een vanzelf sprekendheid omdat we dat al jaren doen. Maar het speelveld verandert, dus ook de compliance-eisen veranderen. Mijn belangrijkste focus was het neerzetten van de compliance-organisatie en daarmee ook compliance-awareness vergroten. Door de samenwerking met bijvoorbeeld Legal te intensiveren zijn we in staat om beter onze toegevoegde waarde aan de business te laten zien. Door namelijk in een vroegtijdig stadium aan te geven welke eisen er op ons afkomen, kunnen we gezamenlijk beter inspelen op wat er nodig is om compliant te blijven.'

Heb jij een aantal compliance officers ter plekke? 'Ja, een aantal compliance officers zijn werkzaam in de business waarbij er nu een functionele rapportage lijn is naar mij. We overwegen op dit moment meer centralisatie, waarbij de compliance officers ook hiërarchisch aan mij gaan rapporteren. Door te centraliseren kunnen we efficiënter werken en de werkgebieden ook beter verdelen. Om het risico van de ivoren toren te vermijden, zullen de compliance officers ook fysiek een aantal dagen in de week bij de business zitten. Met deze opzet hopen we een goede balans te bereiken.'

Jullie zijn een afwikkelonderneming. Wat is dat precies en waarom waren jullie bezig met een vergunningaanvraag? 'Wij zijn verantwoordelijk voor de achterkant van het girale betalingsverkeer. Als je naar de winkel gaat en je koopt iets, moeten die transacties geaccordeerd worden, bij de juiste persoon afgeschreven en bij de juiste persoon bijgeschreven worden. In dat gehele traject (of een deel daarvan) is een afwikkelonderneming werkzaam. Als gevolg van de gewijzigde Wft, per 1 januari 2014, hebben we nu formeel een vergunning van DNB nodig. Op basis van het verleden hebben we nu een tijdelijke vergunning verkregen, maar we moeten wel aan de nieuwe vergunningseisen voldoen. Aangezien dit nieuw is, brengt dit ook soms onduidelijkheden met zich mee. Maar dat is dan ook weer de uitdaging. We zijn er erg druk mee bezig geweest de afgelopen maanden. Per 1 augustus is alles ingediend dus we zijn benieuwd.'

Hoe zie jij het geheel van wetgeving, monitoring en processen die compliance met zich mee brengt? 'Het is logisch dat de crisis een groeiende hang naar regelgeving heeft gebracht, maar het geeft geen enkele garantie. Het is een beetje een golfbeweging. Na een crisis neemt de regelgeving toe, dan zwakt het geleidelijk af tot de volgende crisis en dan neemt het weer toe. Nu zie je een meer principle based benadering ten opzicht van rule based, maar beiden hebben voor- en nadelen.'

Het lastige blijft dat principle based niet te kwantificeren is, het heeft met houding, moraliteit en ethiek te maken. 'Verschil in interpretatie maakt afstemmen ook lastig. Bij principle based mag je het eigenlijk zelf bepalen, maar toch ook weer niet; er zijn immers maatstaven waaraan je moet voldoen. Ik denk dat helemaal principle based niet bestaat. Bij helemaal rule based stop je met nadenken en dat is nooit goed! Wij richten ons hier meer op de "risk based" of "outcome based" benadering. Dit betekent dat de focus ligt bij wat die regel eigenlijk beoogt. Is er überhaupt wel een risico? Waarom veel energie stoppen in iets wat eigenlijk geen risico is? We kijken waar het risico zit en wat de impact is als er wat gebeurt. Deze benadering lijkt me veel effectiever. Voor ons is continuïteit, veiligheid en betrouwbaarheid van onze business heel belangrijk, daar ligt de focus. Door op een risk-based manier ernaar te kijken zorgen we voor de juiste focus en aandacht.'

Dus jullie zetten daar bewust op in? Is dat nieuw binnen dit bedrijf? 'Het is iets wat groeit. Wanneer je het vaak met elkaar hebt over waarvoor we staan en waarvoor we het doen, dan kun je als compliance niet achter blijven. Wij proberen onze beleidszaken zo risk based mogelijk aan te pakken.'

Wat dat betreft hebben jullie natuurlijk minder risicovolle klanten. 'Due diligence is natuurlijk belangrijk. We zeggen niet dat we dat niet doen, maar het dient wel in balans te zijn. Je kunt je energie maar één keer uitgeven. Ik ben dan, als compliance, liever betrokken bij de ontwikkeling van nieuwe diensten en bekijk wat dat betekent en welke regelgeving belangrijk is. Wij hebben bijvoorbeeld te maken met MasterCard, Visa en andere schemes en die leggen veel regels op, waaronder regels rondom Customer Due Diligence. Daarvan wil je van tevoren weten wat de impact is. Ik onderzoek liever dát, dan dat we minutieus op een regel controleren die niets oplevert en die ook geen risico voor ons vormt.'

Kun je ons de verhouding tussen PaySquare en Equens uitleggen? Wat doet PaySquare en wat doet Equens? 'PaySquare is een dochteronderneming van Equens. Equens is een processor van (betaal)transacties, PaySquare is een zogenoemde "acquirer" (een bank of instelling die betalingsverkeer aanbiedt aan retailers (red.)). PaySquare heeft een betaalinstellingsvergunning, maakt het mogelijk dat winkeliers bepaalde betaalproducten kunnen accepteren en verzorgt de relatie tussen de winkelier en de acquirer. De acquirer PaySquare staat helemaal los van Equens, maar gebruikt wel de processor Equens om de betaaltransacties te verwerken. PaySquare kent een andere dynamiek, een ander risicoprofiel en een ander aandachtsgebied, maar tegelijkertijd kunnen we elkaar versterken.'

Bestaat die scheiding al lang? 'PaySquare is al langere tijd een dochter van Equens. Voorheen regelden ze ook nog Maestro en MasterCard issuing. Dit is nu bij ICS[1] ondergebracht. De acquirer PaySquare is met name creditcard gericht, met merken als Visa, MasterCard, JCB, UP en Diners. De organisatie is vertegenwoordigd in verschillende landen in Europa. Zo timmeren we internationaal aan de weg.'

1 International Card Services, dochter van ABN Amro Bank N.V.

> Soms zorgt een situatie voor een spagaat

Het is wel ingewikkeld allemaal. 'Voor een buitenstaander zeker, terwijl vrijwel iedereen onze systemen toch elke dag meerdere malen gebruikt en niet zonder ons zou kunnen! Buitenstaanders weten eigenlijk heel weinig van die wereld. Het is ook wel logisch, want je hebt er als consument ook niets mee te maken, het verloopt allemaal via de bank. Daarachter zitten wij, als transactie processor. Een acquirer doet zaken met winkeliers. Het zijn werelden die je niet ontmoet als consument.'

Maar het is wel een heel belangrijk proces, want als hier wat mis gaat, dan merk je dat als klant onmiddellijk. 'Inderdaad, daarom zijn onze business continuity en veiligheid essentieel. Er is constante zorg en aandacht om het betalingsverkeer vlekkeloos te laten verlopen en fraudeurs voor te zijn. Zeker niet makkelijk in de huidige tijd met al het elektronisch betalingsverkeer. Het is voor ons bedrijf een van de belangrijkste aandachtsgebieden. Wij zetten vol in op informatiebeveiliging. Daarvoor zijn we gecertificeerd, zodat we zeker weten dat alles goed geregeld is.'

Hoe zijn de compliance verantwoordelijkheden over beide afdelingen/ tussen beide entiteiten geregeld? Kun je aangeven in hoeverre ook de meer generieke (regulatory) compliance onderwerpen op de agenda van PaySquare staan? Denk bijvoorbeeld aan het beloningsbeleid, awareness of corporate governance. 'Vanuit compliance hebben we ook PaySquare in onze portefeuille dus we hebben een speciale compliance officer "acquiring" die voor dat stuk verantwoordelijk is. Vanuit mijn rol als Chief Compliance Officer heb ik bilateraal overleg met de CEO van PaySquare en elk kwartaal wordt in het Management Team de compliance rapportage gepresenteerd.'

Wat is wat jou betreft het belangrijkste compliance-onderwerp voor Equens voor 2015? 'Het belangrijkste aandachtspunt is de Wft. Het is nieuw voor ons en we moeten het goed inbedden in de organisatie. Verder staat de voortgaande professionalisering van de compliance organisatie hoog op de lijst.'

Hoe beleven de medewerkers van Equens compliance? 'Aan de ene kant is het vanzelfsprekend, omdat ze vanuit informatiebeveiliging gewend zijn met standaarden te werken. Door bijvoorbeeld e-learning en presentaties krijgt men er steeds beter beeld bij en dat maakt het leuker.'

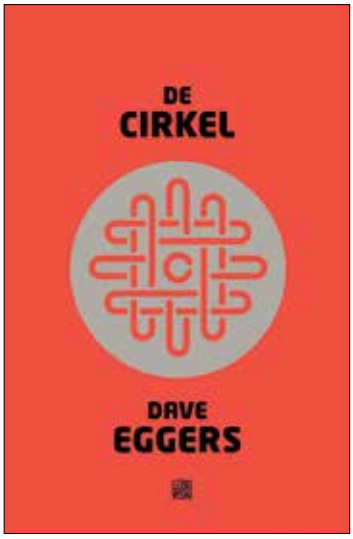
Melden ze zelf ook dingen, worden ze daar actiever in? 'Het is nog even zoeken naar de goede weg. Wij hebben met name informatie beveiligingsprocedures. Wanneer is er dan precies sprake van een compliance-incident en hoe ga je daar dan mee om? Met deze vraagstukken zijn we aan de slag gegaan, om zo te zorgen dat de medewerkers er meer gevoel bij krijgen. De vertaling naar de business en de samenwerken met de business is voor ons ook in 2015 heel belangrijk.'

Tot slot, je bent nu manager Risk Management, Information Security & Compliance, hoe is dat gegaan? Wat voor achtergrond heb je? 'Ik ben begonnen bij de ABN AMRO Bank en was betrokken bij het opzetten van het callcenter in allerlei functies. Het callcenter was een soort speeltuin waar je alles kon bouwen en opzetten. Daarna ben ik bij Operations gaan werken, dat was wel even wennen. Bij Operations heb ik mijn expertise ingezet om diverse servicedesken te centraliseren en verder te professionaliseren. Toen aanvankelijk de fusie ABN AMRO Bank en Fortis niet doorging ben ik op pad gegaan. Zo kwam ik bij Operations Equens terecht, en nu bij Risk Management/Compliance. Ik heb een brede bedrijfskundige achtergrond en ik heb mij verder verdiept in verandermanagement. Ik vind het heerlijk, verandering en verder studeren. Ik ben nu bezig met het "international diploma in compliance"[2]. Nieuwe uitdagingen zijn altijd spannend. Ik ben geen behoudend type, mij moet je niet iets laten consolideren zonder verandering. Daarom zit ik hier zo goed, er gebeurt genoeg en dat maakt het ook zo leuk!'

2 International Compliance Association: <www.int-comp.org>.

De Cirkel van Dave Eggers

Bart Peters



Oorspronkelijke titel: The Circle
Dave Eggers, Uitgeverij Lebowski (2013)
ISBN 978-9-048-81863-1

Een paar jaar geleden las ik het boek 'Wat is de Wat' van de jonge Amerikaanse schrijver Dave Eggers. Deze recensie gaat niet over dát boek (een boeiend en meeslepend geschreven boek over een jonge Soedanees die Darfur ontvlucht, overleeft in Kenia en een nieuw bestaan vindt in Amerika), maar het was wel de aanleiding voor mij om ook het boek 'De Cirkel' van dezelfde schrijver te lezen.

Op internet kwam ik over 'De Cirkel' tegen: 'Een must-read voor iedereen met internet'. Nu vermoed ik dat er geen enkele compliance officer meer is die internet niet gebruikt, maar ik denk dat dit boek juist 'een must-read' is voor compliance officers die zich interesseren voor thema's als privacy en het gebruik van social media.

Persoonlijk ben ik geen privacy-fetisjist en in discussies hierover heb (of moet ik zeggen had?) ik soms de neiging om de kant te kiezen van mensen die zeggen dat goedwillenden geen privacy nodig hebben. Met het aloude argument dat wie niets te verbergen heeft, geen behoefte zou moeten hebben aan de bescherming van zijn privacy.

Dit boek heeft mij wat dat betreft een spiegel voorgehouden en een nieuw licht geworpen op de maatschappelijke discussie over privacy, social media en de machtspositie van grote bedrijven als Facebook, Google en Twitter.

Een boekrecensie mag niet leiden tot een spoiler alert en dus zal ik de verhaallijn niet teveel uit de doeken doen. Het boek beschrijft goed hoe de komst van internet ons beeld van privacy verandert of minimaal dreigt te veranderen. Mensen gooien hun complete leven online, in dit boek nog veel meer dan wij nu gewend zijn, maar als lezer realiseer je je voortdurend dat de beschreven werkelijkheid misschien niet zo heel ver af ligt van de werkelijkheid anno 2014. De argumenten die gebruikt worden om vergaande privacy-beperkingen te bepleiten, lijken soms erg op de argumenten die nu vaak al geaccepteerd worden. Het gaat dan bijvoorbeeld om het bestrijden van kindermisbruik, terrorisme en criminaliteit, maar bijvoorbeeld ook om het bevorderen van transparantie door politici. In dit – Orwelliaans te noemen – boek wordt dit debat meer en meer gedomineerd door de tegenstanders van privacy, belichaamd door een bedrijf (De Cirkel) dat je kunt zien als een Facebook 3.0. Het bedrijf dreigt uiteindelijk ook een rol te krijgen in het betalingsverkeer, criminaliteitsbestrijding, het continu in beeld brengen van politici en zelfs het organiseren van de verkiezingen. Kortom: een organisatie die als een soort octopus haar tentakels heeft in de gehele maatschappij. Je voelt als lezer de beklemming die dat oplevert... Personen die zich verzetten tegen de, op het oog nobele, motieven van De Cirkel, worden neergezet als stoorzender, rebel of zelfs vijand van de maatschappij.

Een boeiend verhaal waarin de hoofdpersoon die bij De Cirkel gaat werken en dit van binnenuit beleeft, uiteindelijk overwint (of niet…?). Het boek daagt de lezer uit nog eens goed na te denken over thema's die nu al actueel zijn en wellicht in de toekomst nog meer. Aan de lezer tenslotte om te bepalen of dat een schrikbeeld is...

Nationaal Compliance Congres 2014

11 december 2014

Met aandacht voor ondermeer:

- Verdraaide organisaties: een nieuw paradigma voor compliance officers?
- Visie van DNB op anti-corruptie
- Samenwerking tussen HR & Compliance
- Resultaten van het AFM en DNB onderzoek naar verandervermogen
- Privacy governance in de praktijk
- Vierde witwasrichtlijn
- Vernieuwde Code Banken en het tuchtrecht

Nederlands Compliance Instituut

www.nationaalcompliancecongres.nl

Leading in compliance