VU magazine

Compliance & Integriteit

nr.1 jaargang 4 | april 2013

Intern Toezicht

Over macht, dwang en sancties

License to operate van de CO

Vertrouwen : hoe doe je dat ?

Nieuwe rollen voor Compliance en IAD

VU VRIJE UNIVERSITEIT AMSTERDAM

Inhoud

Column: Steven ten Have

Stimuleren of waarborgen van gewenst gedrag: hoe doe je dat? En waarom? Hoe voorkom je dat het middel verwordt tot doel.

Intern toezicht in relatie tot de 1e lijn

Compliance is gedrag en voor het grootste gedeelte rechtstreeks gekoppeld aan de activiteiten van de 1e lijn. Compliance is dus de verantwoordelijkheid van de 1e lijn.

(Her)oriëntatie op de kerntaken van de compliancefunctie

Over de nieuwe rol van de compliancefunctie sinds de economische crisis en de diverse schandalen. Naast kerntaken ruimte voor advisering.

De interne accountant: van controleur naar regisseur

Wat is het nieuwe profiel van de Internal Auditor? De spin in het GRC net, de regisseur die gebruik maakt van andere onafhankelijke interne deskundigen.

Extern toezicht op interne beheersing

Niet teveel nadruk op de plaats van compliance in de defensielinies, maar op de inhoud van compliance.

Voorwoord

De postdoctorale opleiding Compliance & Integriteit Management van de VU heeft een vaste plaats gevonden in de harten van de compliance gemeenschap, zowel binnen de financiële instellingen als binnen de industrie. Dit doet ons deugd. Nog nooit waren er in januari al zoveel concrete belangstellenden. Natuurlijk hopen wij dat dit leidt tot een groot aantal aanmeldingen voor leergang IX. De splitsing tussen de financiële en niet-financiële organisaties in het derde blok blijft deels gehandhaafd. We hebben ervaren dat studenten bepaalde onderwerpen zo belangrijk vinden dat zij de voorkeur hebben dat deze colleges – zoals bijvoorbeeld het college over extraterritoriale werking van het Amerikaanse en Britse recht - niet gesplitst worden. Wij nemen de commentaren van onze studenten altijd ter harte, want ons doel is ieder jaar weer de colleges zo goed mogelijk aan te laten sluiten bij de behoeften en de praktijk van onze studenten.
Ook de behoefte aan communicatie met onze alumni en de buitenwereld hebben wij destijds onder de loep genomen. Hier hebben we echter in al die tijd geen wijzigingen aangebracht. Meer dan drie jaar geleden kwamen wij naar buiten met het VU Magazine. Zie hier het eerste nummer van de vierde jaargang! Het blijkt dat er voor ons Magazine een klein plaatsje is in de enorme hoop van Magazines, folders en brochures. Door de inhoud toegankelijk te houden en dicht te koppelen aan de opleiding voldoen wij blijkbaar toch aan een behoefte. Het Magazine wordt gelezen! Ditmaal hebben we als onderwerp ‘Intern Toezicht’ genomen. Het sluit aan bij het symposium dat de VU dit jaar samen met DNB en Deloitte organiseert op 27 mei aanstaande. De kerndocenten geven in dit Magazine hun visie op de rol van toezicht in de diverse defensielijnen van een organisatie. Daarnaast hebben we ook weer onze vaste rubrieken zoals de column en de ervaringen van een alumnus. Wij wensen u veel leesplezier en heten u alvast graag welkom op ons symposium van 27 mei 2013!

Sylvie C. Bleker-van Eyk, programmadirecteur Postgraduate opleiding Compliance & Integriteit Management

Column

Steven ten Have

Voer voor psychologen (en sociologen)

Voor veel psychologen is het begrip compliance verbonden met het onderwerp sociale invloed. Daarbij gaat het om de wijze waarop mensen de overtuigingen, gevoelens en het gedrag van anderen beïnvloeden. Sociale invloed kent verschillende vormen: conformiteit, compliance, gehoorzaamheid. De basis voor beïnvloeding varieert. Bij conformiteit gaat het om aanpassing aan een groepsnorm. Bij compliance om een reactie op een expliciet of impliciet verzoek van anderen. Bij gehoorzaamheid gaat het om een reactie op een bevel of opdracht van een hiërarchisch of anderszins hoger gestelde. Een vierde vorm is *persuasion* waarbij men zich bewust richt op het beïnvloeden van overtuigingen en gevoelens van anderen. Als het gaat om het stimuleren of waarborgen van gewenst gedrag zijn alle vier, al dan niet gecombineerd, nuttig. Voorbeeldgedrag, socialisatie, psychologische contracten, organisatiestructuren, campagnes. Het zijn stuk voor stuk nuttige gereedschappen. Ze zijn (vaak) een noodzakelijke-maar-niet-voldoende-voorwaarde voor het realiseren van gewenst gedrag. Niet meer, niet minder. Het ontbrekende deel wordt gevormd door het antwoord op de vraag wat gewenst gedrag is.

Het vakgebied compliance gaat over leiderschap en management: de goede dingen doen en die dingen goed doen. Echt leiderschap verlicht de rol van het management. Als de goede dingen vanzelfsprekend of aansprekend zijn, doet de bal het werk. Dan hoeft de organisatie niet in de touwen gehouden te worden. Met macht en dwang, hiërarchie en sancties. Antoine de Saint-Exupery zei het al: *'Wanneer je een schip wilt bouwen, breng dan geen mensen bij elkaar om het hout te slepen, het werk voor te bereiden en de taken te verdelen. Maar leer mensen te verlangen naar de eindeloze zee.'* Met gereedschap is niets mis. Sterker nog, het is vaak hard nodig. Maar niet zelden verwordt het middel tot doel. Onderzoek van Schaffer en Thomson[1] naar veranderprogramma's leert dat deze mislukken als ze 'activiteitengericht' zijn. In plaats van resultaatgericht. Vraag maar eens in je eigen organisatie: hoe staat het hier met het onderwerp compliance? Helaas. De meeste mensen zullen vertellen over waar ze in de organisatie allemaal wel niet mee bezig zijn. In plaats van over dat wat men wil bereiken. Of belangrijk vindt. Laat staan, over het *waarom*, betekenis en zingeving.

Compliance is een onderwerp dat *by nature* (te) veel met de punt naar achteren speelt. Defensief, control. Zoals innovatie en leren onderwerpen zijn die met de punt naar voren spelen. Toekomstgericht, vernieuwend. Compliance zou je in ieder geval toewensen dat het ook met de punt naar voren leert spelen. Zonder de defensie te verwaarlozen. Dat het meer gaat over *positive deviants* dan over de afwijkingen waar auditors (*by nature*) zo gek op zijn. *Positive deviants* zijn mensen die 'ongewoon' of ander, maar succesvol *en* gewenst gedrag laten zien. Het zijn de mensen die verlangen naar de zee. Of het vuur. En zich dan autonoom, vooral intrinsiek gemotiveerd, *self propelling* manifesteren als scheepsbouwers of hittezoekende raketten. Ze zien en zijn het gewenste gedrag voordat het beleid is. Wat wil je nog meer?

Steven Ten Have is hoogleraar Strategie en Verandering aan de Vrije Universiteit Amsterdam, partner bij TEN HAVE Change Management en commissaris bij ABN AMRO en CITO

1 Schaffer, R. & H. Thomson (1992), Succesful Change Programs Begin with Results, *Harvard Business Review*, january-february, p. 80-89

Dr. Sylvie C. Bleker-van Eyk

Intern Toezicht in relatie tot de 1e lijn

De definitie van compliance die in de postdoctorale opleiding Compliance en Integriteit Management wordt gehanteerd luidt: "het in de meest algemene zin bevorderen en handhaven van de wet- en regelgeving en van de integriteit van de organisatie evenals de integriteit van haar bestuurders en medewerkers met als doel risico's te beheersen en de daaruit voortvloeiende schade te voorkomen."

Compliance is een vorm van gedrag

Compliance gaat om het bevorderen van een bepaald gedrag, waarmee de integriteit van de organisatie beschermd wordt en de mogelijke risico's die ongewenst gedrag met zich meebrengt beheerst worden. Compliance ziet toe op gedrag en streeft naar een bepaalde cultuur binnen de organisatie waarin het gewenste gedrag de leidraad is. Subculturen zijn mogelijk, zolang zij zich maar in de kern positief verhouden tot de fundamentele basiscultuur, welke compliant is met deelafspraken die zijn gemaakt. Kortom *'compliance'* refereert rechtstreeks naar een gewenste, integere *'cultuur'*. Bij deze interpretatie is het begrijpelijk dat we vanuit de opleiding vaak stellen dat compliance een 'gedragswetenschap' is en is het niet verbazend dat de opleiding bijzondere aandacht geeft aan onderwerpen zoals integriteit, change management en behavioral finance. Compliance vereist gedrag en gedrag wordt weer beïnvloed door de cultuur van de organisatie.

Compliance in de 1e lijn

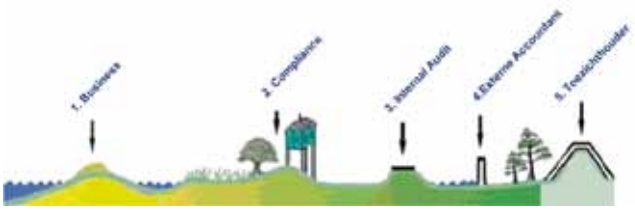
Als het bovenstaande het uitgangspunt is, klinkt het bijna ongelofelijk dat compliance in beginsel altijd een onderwerp vanuit de 2e of 3e lijn is geweest. Bij de opkomst van compliance werd het vooral opgepakt vanuit de 3e lijn, meestal internal audit. De 3e lijn is de interne toezichtlijn die eind jaren 80 en in de jaren 90 compliance taken op zich nam. Het ging toen vooral bij financiële instellingen om wetgeving inzake voorwetenschap en ook bij beursgenoteerde fondsen namen legal (2e lijn) of internal audit (3e lijn) deze taken op zich. Op zich toch niet zo onbegrijpelijk, omdat de definitie van compliance in die tijd meestal een zeer beperkte scope omvatte, immers controle op handel met voorkennis. Dit betreft de bestuurders en medewerkers door de hele organisatie heen en dus werkzaam in alle verdedigingslinies. Naarmate de scope van compliance werd uitgebreid veranderde de positie van compliance. De toename van de complexiteit van de wet- en regelgeving – met name bij financiële instellingen – leidde tot behoefte aan gespecialiseerde medewerkers die de wet- en regelgeving niet alleen bijhielden, maar ook vertaalden naar de specifieke vereisten voor de onderneming. Daarnaast moest compliance de 1e lijn overtuigen van het belang van de regels en de naleving ervan monitoren. Al vlug ontstond bij de 1e lijn de perceptie dat compliance er alleen was om spaken in de wielen van de business te steken en omzet te verlagen. Ze lieten compliance over aan de 2e lijn en die moesten de valkuilen dan maar zoeken en de problemen oplossen. Compliance kreeg de verantwoordelijkheid van de 1e lijn in de schoenen geschoven en zwoegde verder. Immers, op het niveau van de Raad van Bestuur en Raad van Commissarissen was vaak weinig affiniteit met het onderwerp compliance. Alleen als er een flink incident plaatsvond zag men gedurende de periode van herstel tijdelijke bewustwording van de effecten van compliance op bestuurlijk niveau. Deze tekst is geschreven in de verleden tijd, maar helaas zijn er nog te veel bedrijven waar deze tekst ook in de tegenwoordige tijd nog opgeld doet.

Toezicht in de 1e lijn

In de eerste paragraaf zagen we dat compliance onlosmakelijk verbonden is aan een integere cultuur. Compliance vereist een bepaald gedrag van de medewerkers. De wet- en regelgeving worden niet ontworpen voor het functioneren van de 2e of 3e lijn (op enkele specifieke wet- en regelgeving na), maar om zeker te stellen dat de werkzaamheden ('productie') die een bedrijf uitoefent ook gebeuren in overeenstemming met de waarden en normen die in de maatschappij worden gesteld en dat de randvoorwaarden waaronder de business functioneert ook overeenkomstig deze waarden en normen zijn uitgevoerd. De meeste financiële regelgeving betreft de wijze waarop financiële instellingen hun primaire activiteiten vervullen. De waarden en normen worden omgezet in regels die de werkzaamheden reguleren opdat de productie veilig en ordentelijk plaatsvindt, of je nu hypotheken verkoopt, bruggen bouwt of auto's produceert. De productie wordt gekoppeld aan gewenst gedrag, waarbij de wetgever de kaders aangeeft waarbinnen de productie dient plaats te vinden.

"In de 1e lijn moet het toezicht worden opgetuigd"

Compliance is gedrag en voor het grootste gedeelte rechtstreeks gekoppeld aan de activiteiten van de 1e lijn. Compliance is dus de verantwoordelijkheid van de 1e lijn. Het gaat om het gedrag van de medewerkers. Om het gewenste gedrag te verkrijgen moet een integere cultuur gecreëerd worden. Hierbij moet de Raad van Bestuur doordrongen zijn van de plaats die compliance heeft bij de inkadering van de gewenste cultuur en compliance voldoende en krachtig mandaat geven om samen met alle interne stakeholders alles op alles te zetten om de organisatie te voeden met de ingrediënten voor de gewenste cultuur. Het verkrijgen van de gewenste cultuur behoeft top-down mandaat en openlijke, duidelijke en vooral constante ondersteuning. Voorbeeldfunctie alleen is onvoldoende. De boodschap moet herhaald worden en bevestigd worden. Het is een kwestie van educatie en daarbij ligt de kracht wel degelijk in de herhaling. Echter, ook bottom-up moet aan de cultuur gewerkt worden. Cultuur is niet iets wat je aantrekt als een soort van verplichte bedrijfskleding.



Five Lines of Defense

De wet- en regelgeving alsmede de interne waarden en normen geven het kader van de cultuur aan. Het dient in het DNA te zitten. Eenvoudiger gezegd dan gedaan. De vraag moet dus zijn: heb ik de juiste mensen in dienst die de vereisten in ieder geval in hun genen hebben en hoe krijg ik die eigenschappen boven tafel? Zeg dus niet: "dit is de jas en nu trek je hem aan, want zo houden wij ons bedrijf warm"! Vraag bottom-up aan je medewerkers: "dit is de temperatuur waaronder wij het beste kunnen werken, wat kunnen wij doen om jou op die temperatuur goed te laten functioneren?" Vergeet niet om dan ook de vraag te stellen of iemand wel op die temperatuur wenst te werken.

In de 1e lijn moet het toezicht worden opgetuigd. De leidinggevenden moeten beseffen dat compliance een essentieel onderdeel is van 'veilig' werken. Iedere leidinggevende is binnen zijn/haar span of control verantwoordelijk voor het bereiken van het doel van compliance: de integriteit, financiële positie en reputatie van het bedrijf te beschermen door alle toepasselijke wet- en regelgeving en ethische normen na te komen. Om dat doel te realiseren, ontwikkelt het bedrijf een compliance-programma met minimum normen waaraan alle medewerkers zich bij het verrichten van hun taken en verantwoordelijkheden dienen te houden. Aan de leidinggevenden om te sturen en toezicht te houden op de realisatie van de productie, maar zeker ook op de verwezenlijking van de compliance-doelstelling. <<

Raf Houben

(Her)oriëntatie op de kerntaken van de compliancefunctie: een noodzakelijk gegeven

In de laatste twee decennia is er in Nederland veel moeite en tijd is gestoken in het inrichten en verder uitbouwen van de compliancefunctie zowel binnen de financiële sector als daarbuiten. Hierbij is de compliance functie in de meeste gevallen geëvolueerd tot een risicomanagementfunctie. De compliancefunctie wordt hierbij neergezet als een functie in de zogenaamde 'tweede verdedigingslinie' binnen het 'Enterprise Risk Management' model van de onderneming[1]. Daarnaast kenmerkte de financiële sector zich de laatste vijf jaren door de economische crisis en diverse schandalen. Het imago van de Nederlandse financiële sector is hierdoor sterk geërodeerd met als gevolg (nog meer) overheidsingrijpen alsmede het verworden tot een speelbal van de politiek en de publieke moraal.

De vraag rijst of de compliancefunctie er voldoende in is geslaagd zich aan te passen aan dit nieuwe tijdsbeeld en een niveau heeft bereikt dat recht doet aan haar kernverantwoordelijkheid. Immers, naast het managen van compliancerisico's en zodoende bijdragen aan een beheerste en integere bedrijfsvoering, wordt er door de buitenwereld steeds meer nadruk gelegd op de 'juiste' cultuur binnen de financiële sector en verantwoord gedrag van daarin werkzame personen.

(Her)oriëntatie op de kerntaken van de compliancefunctie noodzakelijk

In het verleden is (uitputtend) gekeken naar de compliancefunctie, haar positionering, taken en verantwoordelijkheden. Een probleem hierbij is echter dat deze (her)oriëntatie in meerdere gevallen heeft plaatsgevonden naar aanleiding van incidenten of op aandringen van toezichthouders. Heroriëntatie op de kerntaak van de compliancefunctie binnen de onderneming is als gevolg hiervan achtergebleven.

Hoewel er in de praktijk initiatieven zijn genomen door compliancefuncties, ontbreekt het aan duidelijke (inter)nationale richtlijnen, concrete regelgeving, een duidelijke sturing door toezichthouders en aan visie bij ondernemingen zelf. Zo komt in de visie van het kabinet over de toekomst van de financiële sector de compliancefunctie niet terug en blijft deze steken in hoogdravende teksten die erop neerkomen dat financiële instellingen 'hun verantwoordelijkheid beter moeten nemen'[2].

De praktijk leert dat de positie van de compliancefunctie in diverse gevallen niet duidelijk is bepaald en een operationeel risicokarakter heeft, dat wil zeggen (te) sterk is betrokken bij diverse operationele processen (bijvoorbeeld bij de beoordeling van marketinguitingen). Een uitvloeisel hiervan is dat de compliancefunctie rapportages oplevert die sterk doen denken aan financiële of operationele risicomanagementrapportages (inclusief 'dashboards en stoplichten'). De compliancefunctie wordt soms onder druk van de omstandigheden en/of in reactie op vastgestelde tekortkomingen in de organisatie, zelfs belast met een lijnverantwoordelijkheid. In essentie tast dit de eigen verantwoordelijkheid van het lijnmanagement aan en 'vervagen' de verantwoordelijkheden van de compliancefunctie. Bovendien staat dit haaks op het idee van een compliancefunctie die – naast beheersing van compliancerisico's - de regie voert over en toezicht houdt op de integriteit binnen de onderneming[3].

Drie scenario's

Het bovenstaande geeft aanleiding te heroriënteren op de kernverantwoordelijkheden van de compliancefunctie. Hierbij zijn drie scenario's denkbaar:

Bestendiging van de traditionele rol van de compliance functie

Er zou aan gedacht kunnen worden de compliancefunctie te laten zoals deze nu is (geworden). Het voordeel hiervan is dat er geen (extra) effort gestoken hoeft te worden in een nieuwe oriëntatie. Daarnaast heeft de compliancefunctie bewezen voldoende meerwaarde te hebben binnen ondernemingen. Het nadeel is echter dat de externe omgeving is veranderd. (Financiële) ondernemingen zijn (al of niet gedwongen) op zoek naar nieuwe verdienmodellen en een 'nieuwe cultuur'. De compliancefunctie dient in dit verband mee te evolueren anders dreigt zij ingehaald te worden door de ontwikkelingen en de 'grip' te verliezen op haar eigen ontwikkeling en voortbestaan.

> "Compliance moet niet leiden tot morele luiheid elders"

Heroriëntatie binnen de 'tweede verdedigingslinie'

Hierbij kan gedacht worden aan twee varianten. De eerste variant betreft de vraag of de compliance functie nog wel thuishoort in de 'tweede verdedigingslinie'. Naleving van regelgeving is immers een randvoorwaarde binnen een onderneming en heeft minder te maken met risicomanagement. Een wetenschappelijke onderbouwing van compliance risicomanagement is er niet en in de praktijk wordt zoveel mogelijk aansluiting gezocht bij operationeel risicomanagement[4]. Een nadeel van deze benadering is echter dat het eerder genoemde 'Enterprise Risk Model' heeft bewezen een meerwaarde te hebben bij het 'in control' krijgen of managen van risico's binnen een onderneming. De compliancefunctie heeft in dit model een duidelijke en effectieve plaats en rol binnen de onderneming.

De tweede variant betreft de vraag of de compliancefunctie efficiënter en effectiever zou kunnen opereren binnen de 'tweede verdedigingslinie' door kennis en ervaring te bundelen met andere staf- en risicomanagementfuncties (zoals de (operationele) risicomanagementfunctie, veiligheidszaken, interne controle, juridische zaken, en de HR functie). Kortom het vormen van een 'pool van 'professionals' binnen een onderneming die het bedrijf ondersteunen elk vanuit de eigen rol (zoeken naar 'synergie'). Een groot voordeel hiervan is dat moeizame discussies over de positionering van een functie en welke taken en verantwoordelijkheden deze precies heeft, alsmede de hiermee onvermijdelijke verband houdende competentiestrijd, worden vermeden. Een nadeel van deze benadering dat mogelijk de compliancefunctie haar (door regelgeving afgedwongen) onafhankelijke positie moet opgeven.

Investeren in een (gedeeltelijk) nieuwe rol

Een derde benadering is dat de compliancefunctie naast haar traditionele kerntaken of in plaats daarvan de rol aanneemt van interne cultuurbewaker of gedragstoezichthouder. Het begrip 'counsel' of adviseur zou in dit verband overigens dan beter op zijn plaats zijn dan compliance officer. De compliancefunctie zou dan een 'spiegelende' of toetsende rol kunnen spelen. Een nadeel hiervan is dat door de onderneming een investering zal moeten worden gedaan in het opbouwen van kennis en ervaring t.a.v. van gedrag- en cultuurveranderingtrajecten. Bovendien zullen op de een of andere manier de traditionele kerntaken van de compliancefunctie wel uitgeoefend moeten blijven worden.

Het is overigens ook denkbaar dat andere personen binnen de onderneming die dichter bij de commercie staan, een rol spelen in dergelijke trajecten omdat deze de 'business' beter kennen. De compliancefunctie zou in een dergelijk geval vanuit haar traditionele rol kunnen toezien op naleving van gemaakte afspraken. Overigens moet het belang van de traditionele compliancefunctie niet overschat worden anders leidt dit tot een ongebalanceerde verhouding van verantwoordelijkheden en 'morele luiheid'. Het is van groot belang dat een cultuuromslag vanuit de onderneming zelf komt.

Afsluiting

De tijd is rijp voor een (her)oriëntatie op de kerntaken van de compliance functie. In een tijd waarin er veel (nieuwe) wet- en regelgeving afkomt op ondernemingen, cultuur- en gedragsaspecten in de financiële sector een steeds grotere rol gaan spelen, en toezichthouders hun inspanningen vergroten, is een 'nieuwe' compliancefunctie noodzakelijk.

Hierbij is het eerste scenario geen optie meer. Naar mijn mening zou nagedacht moeten worden over een combinatie van de twee overige geschetste scenario's waarbij de compliancefunctie meer 'losgekoppeld' wordt - dan wel een meer zelfstandige rol krijgt als gedragstoezichthouder - van andere functies zonder de synergie uit het oog te verliezen. Dit heeft als voordeel dat alle goede elementen samengevoegd kunnen worden om zodoende de compliancefunctie het meest efficiënt en effectief neer te zetten. Dit doet recht aan haar rol en de huidige tijdsgeest. <<

Mr. R.A.M. (Raf) Houben is als kerndocent verbonden aan de Postgraduate opleiding Compliance & Integriteit Management en werkzaam bij ASR Nederland. Dit artikel is op persoonlijke titel geschreven

1 Het COSO II (Enterprise Risk Management) model.
2 R.W.A. Bakkers en A.J.C.C.M. Loonen, 'De kabinetsvisie toekomst financiële sector; teveel gericht op structuur, te weinig op cultuur', TvCo 2009, nr. 5, p. 158-160.
3 'Bijdragen aan verandering; een nieuwe visie op compliance', 2009, Compliance Position Paper van Groep Olivier.
4 Vergelijk de risicomodellen voor 'non financials risks' voortvloeiend uit Basel II/III en Solvency II.
5 R.A.M. Houben, 'Overschatting van de compliance functie leidt tot morele luiheid', TvCo 2012, nr. 4, p. 259-261

Vincent Wanders

De interne accountant: van controleur naar regisseur

Na de omkering van de positieve macro economische ontwikkelingen naar een negatieve, is een zoektocht naar herijking van zekerheden gaande. Als de grootste financiële instellingen maar ook klassieke industrieën als de auto industrie wereldwijd alleen met staatssteun in stand blijven en nog maar veertien landen een triple A rating hebben, waar is dan nog de zekerheid te verkrijgen dat landen en ondernemingen in control zijn en toekomst hebben? Wie heeft welke rol bij de creatie van zekerheid in de huidige economie?

In onderstaand artikel wordt ingegaan op de rol die de interne accountant speelt en die hij (of zij natuurlijk) kan gaan spelen. Het is niet vanzelf sprekend om hierover te spreken, want tot op heden is de interne accountant behoorlijk in de schaduw gebleven. Maar de wereld is in beweging en de maatschappelijke structuren dus ook. Een deel van de oplossing kan dan ook uit onverwachte hoek komen.

Rol van de interne accountant

Historisch gezien houdt de interne accountant zich bezig met het verschaffen van zekerheid bij de financiële verantwoording, derhalve de financial audit rol. Daarbij wordt met name gesteund op de administratieve organisatie en de interne beheersing binnen de te controleren organisatie. De interne accountant heeft dan ook intensieve organisatiekennis opgebouwd. Tevens was een heldere afgebakende verantwoordelijkheid met de externe accountant vastgelegd. Onderdelen van de inhoud van onderstaande toekomstvisie gelden wellicht ook voor de nieuwe toegevoegde waarde die van de externe accountant wordt verwacht.

Deze financiële audit taakopvatting is soms nog herkenbaar. Bij het kennismakingsgesprek van een aantal jaren geleden als interne accountant bij een multinational zei de CEO tegen mij: “je telt alles toch wel goed na hé? “. Ik keek hem nog aan om te zien of dit zijn gevoel voor humor was, maar ik ben bang dat dit niet zo was.
Afhankelijk van de aard van de activiteiten van de organisatie kwam vervolgens focus op IT audit. De onderzoeken richten zich met name op de betrouwbare en continue geautomatiseerde gegevenswerking binnen een organisatie. Met name bij financiële instellingen werd kennis opgebouwd over de opzet en werking van de geautomatiseerde systemen en de interne accountant was in bepaalde gevallen het wandelend geheugen van de IT legacy geworden. Een verdieping van de rol derhalve.
De volgende stap was de operational audit: het uitvoeren van een onderzoek naar het functioneren van het management beheerssysteem van een organisatie. Hierbij worden risico analyses betrokken, en vond het Enterprise Risk Management (ERM) zoals dat in COSO rapporten is beschreven, zijn plek. Bij het COSO ERM framework wordt vanuit een proces de beheersing van de strategische, compliance, financiële en operationele aspecten doorlopen. Hier wordt compliance dus explicitiet binnen ERM als aandachtsgebied neergezet.

De risico analyse vindt plaats langs verschillende niveaus in een organisatie: van dochteronderneming tot totaal concern.

Neveneffect van deze insteek is dat tevens meer inzicht in het business model bij de interne accountant gaat ontstaan. Met name het aspect inzicht in het business model heeft na de Enron en Xerox affaire meer belang gekregen. De centrale vraag hierbij is op welke manier de inkomstenstromen feitelijk tot stand komen.
Tevens is inzicht in de efficiency en effectiviteit van het intern control systeem (ICS) ontwikkeld. Control moet hierbij niet gezien worden als controle, maar als beheersing. Aan deze aspecten is tevens het Corporate Performance management gerelateerd.
Door de introductie van operational audit wordt op het gebied van de interne organisatie en cultuur inzicht in de governance van een organisatie verkregen. De kennis in breedte en diepte van de organisatie bij de interne accountant nam dus toe.
Tegelijkertijd werd de financiële audit functie geoutsourced aan de grotere accountants kantoren, waarschijnlijk omdat door de bredere taken de kosten voor een interne

accountantsafdeling (IAD) fors toenamen. De outsourcing heeft echter geleid tot kennisverlies bij de IAD rond het cijfermatige inzicht in de organisatie, hoe aannemelijk het kostenargumenten overigens ook is

Actuele ontwikkelingen

Binnen ons raamwerk zijn wij binnen de opleiding van het onderscheiden van three Lines of defense naar Five Lines of Defense gegaan. De derde lijn is daarbij ingeruimd voor de interne accountant. In organisaties zien we daarnaast in de tweede lijn een toename van risk, control en compliance functies. Een toenemende complexiteit van de structuur en van de inhoud is het gevolg.
Naast de hierboven genoemde aspecten is de interne accountant tevens toezicht houder op de GRC geworden: de combinatie van Governance, Risk en Compliance.
Deze trend werd al eerder gesignaleerd in het rapport "de Internal auditor als spin in het GRC net" uit 2010. Het rapport is door het toenmalige Nivra en de IIA (Instituut Internal Auditors) opgesteld. Hierin wordt het volgende gesteld:

> *Bij de invulling, uitvoering maar vooral ook de beheersing van de diverse GRC-activiteiten binnen een organisatie moet Internal Audit haar verantwoordelijkheid nemen. Daarnaast heeft Internal Audit veel belang bij een evenwichtig, efficiënt en effectief samenspel tussen de verschillende risk- en controlfuncties binnen de organisatie*

De ondertitel van het rapport is *samenwerking met behoud van onafhankelijkheid*. Deze ondertitel geeft gelijk het spanningsveld weer met de randvoorwaarde waarbinnen een IAD moet opereren: absolute onafhankelijkheid.

De volgende stap

Bovenstaande ontwikkelingen leiden tot de vraag hoe een IAD toekomstbestendig toegevoegde waarde aan een organisatie kan leveren. Hierbij zijn twee aspecten belangrijk:

- Wat wordt het profiel van de interne accountant qua opleiding, ontwikkeling en als persoon
- hoe gaat de 'community' (of samenwerking) met andere gerelateerde functies eruit zien?

Profiel en rol

Recent onderzoek van het NBA ("op de toekomst voorbereid") naar de toekomstige opleidingseisen van de accountant geven aan dat psychologie, communicatieve vaardigheden en maatschappelijk inzicht relevante kennisgebieden worden voor alle accountants, dit naast de reeds bekende functionele kennisgebieden. Bij deze laatste gebieden zijn risk management en compliance steeds meer overheersend. Deze punten sluiten aan op de hierboven eerder beschreven ontwikkeling.

Op het gebied van ontwikkeling is overigens nog toe te voegen dat meerjarige ervaring in diverse rollen en functies evenzeer relevant is, waardoor het inlevingsvermogen toeneemt.
De kosten van een IAD zullen echter toenemen als op bovengenoemde wijze invulling wordt gegeven aan de functie. Daartoe zal de interne accountant samenwerking vorm moeten geven. Om aan deze samenwerking vorm te geven is de GRCA community op te richten. Inderdaad, GRC met de voor de hand liggende term 'audit' daarbij.

Community

Naar mijn idee zal de IAD regisseur zijn, en procesmatig audits uitvoeren met gebruik van andere onafhankelijke interne deskundigen. Voorwaarde is wel dat de interne accountant voldoende inhoudelijke basis kennis heeft van de gebieden. Een andere voorwaarde is dat de onafhankelijkheid van de interne accountant geborgd is. Uitwerking van de GRCA zal overigens nog concreet moeten plaatsvinden. informeel heb ik deze community structuur een enkele keer gezien als een snelle en efficiënte oplossing voor de onderneming nodig was.

Tenslotte

Het werken aan versterken van zekerheid van instituties en het herwinnen van vertrouwen in instituties en functies bij het maatschappelijk verkeer is een lange weg. Er zijn goede wegen ingeslagen, en laat de interne accountant een duidelijke nieuwe rol hierin krijgen. <<

Vincent Wanders is als kerndocent verbonden aan de Postgraduate opleiding Compliance & Integriteit Management en partner bij Compliant & More.

Richard Bakkers

Extern toezicht op interne beheersing

Deze bijdrage gaat over de rol van de externe toezichthouder, ook wel de 'vijfde defensielinie' genoemd, bij het (toezicht op) interne beheersing. Interne beheersing definieer ik hiertoe als het verkrijgen van een redelijke mate van zekerheid omtrent het bereiken van doelstellingen op het gebied van:

- De effectiviteit en efficiency van de bedrijfsprocessen;
- De betrouwbaarheid van de financiële informatieverzorging;
- De naleving van relevante wet- en regelgeving, beleidsrichtlijnen en procedures;
- Het bewaken van activa of waarden.

Het inbedden van compliance vereisten en integriteitnormen in het raamwerk van interne beheersing maakt hier dus nadrukkelijk onderdeel van uit.
Hoewel ik geloof in de kracht van een model om de werkelijkheid beter zichtbaar en bespreekbaar maakt, vind ik persoonlijk het 'defensielinies-model' teveel een consultantterm die als ultieme waarheid is aangenomen. Wetgeving, zoals de Wet op het financieel toezicht (Wft), kent deze term ook niet. Wetgeving gaat uit van de business (ook wel de 'eerste defensielinie' genoemd) die primair eindverantwoordelijk is voor interne beheersing, inclusief het voldoen aan compliance vereisten en integriteitnormen. Dat bepaalde functies – zoals compliance, risk management en internal audit – de business daarbij *ondersteunen* is evident. In de Wft worden aan deze functies zelfs specifieke taken toegekend, maar een rangschikking naar een plaats in de (defensie)linies wordt daarin mijns inziens noch genoemd noch gesuggereerd. In wetgeving buiten de financiële sector heb ik dit ook nooit gelezen. Wat mij opvalt, is dat in de COSO ERM brondocumenten ook niet wordt gesproken over 'lines of defense[1]'. In de welbekende COSO ERM kubus zien we de doelstellingen (strategisch, operationeel, compliance en rapportage) gebroederlijk naast elkaar bestaan en is klip en klaar aangegeven dat management hiervoor primair eindverantwoordelijk is.
In mijn ogen is er maar één defensielinie en dat is de onderneming als geheel, vertegenwoordigd door de business. Als de business een wetsovertreding begaat, bijvoorbeeld het niet-leven van sanctiebepalingen of zorgplichtvereisten, dan is het niet zo dat compliance (ook wel de 'tweede defensielinie' genoemd) dit kan oplossen, het kwaad is immers al geschied. Wel heeft compliance een belangrijke rol in het managen van dit issue richting externe toezichthouder(s) en andere belanghebbenden. En een belangrijke rol in het opzetten en laten inbedden in de business van verbetermaatregelen. Dit kan enkel leiden tot boetematiging of een sterkere positie voor een schikking, zo leren ons bijvoorbeeld de 'sentencing guidelines'. De discussie zou mijns inziens dan ook niet moeten gaan over de 'volgorde' in linies maar over de gewenste rol die elke functie binnen het bedrijf zou moeten innemen. De gewenste rol voor compliance is dan in mijn ogen het borgen van de 'license to operate' van de onderneming. Deze 'license to operate' staat ook centraal in de competenties van onze opleiding[2]:

Wat voor mij scherper zou mogen is dat de externe toezichthouder rechtstreeks de business uitdaagt en bevraagt. Niet zelden communiceert de externe toezichthouder met de onderneming via de compliance of interne audit afdeling. Terwijl nu juist de business moet aantonen dat de interne beheersing op orde is en dat die business zelf moet kunnen uitleggen hoe het aspect 'inbedden van compliance vereisten en integriteitnormen' hierin is meegenomen. De business zal dan (nog) meer doordrongen zijn dat zij primair verantwoordelijk is voor interne beheersing incl. compliance vereisten en integriteitnormen. Als een onderneming de compliance afdeling informatieverzoeken laat beantwoorden of als in face-to-face gesprekken hierop de compliance officer structureel het antwoord geeft, dan moeten wat mij betreft de rode lichten bij de externe toezichthouder gaan branden: de business weet het dus niet. Mijn boodschap aan externe toezichthouders: schrijf liefst geen brieven "t.a.v. de directie" maar maak ze persoonlijk en richt ze bij voorkeur direct aan de verantwoordelijke voor het betreffende bedrijfsonderdeel waarop het informatieverzoek betrekking heeft. Verwacht ook het antwoord van die verantwoordelijke. En vraag nadrukkelijk business mensen als 'voorzitter' bij face-to-face gesprekken. En aan compliance officers: laat je in gesprekken met externe toezichthouders waarin woorden als 'regels' of 'compliance' vallen niet automatisch verleiden tot het geven van de antwoorden. De business moet dat zelfstandig kunnen. Compliance moet de business dermate (blijvend) voeden met informatie zodat de business dit ook kan waarmaken.
Pleit ik dan voor een uitgeklede compliance functie? Integendeel. Maar wel, in lijn met het betoog van Raf Houben elders in dit magazine, voor een (her)oriëntatie van de kerntaken van de compliance functie. Externe toezichthouders moeten vervolgens in lijn daarmee de compliance functie niet louter beoordelen (afvinken) op de taken die zij al dan niet via sectorspecifieke wetgeving toebedeeld hebben gekregen. Maar op veel fundamentelere aspecten als: Wat is niveau en kennis van de compliance functie? Is zij voldoende onafhankelijk? Hoe proactief informeert zij de business? Stelt zij de juiste vragen? Zit compliance hier op regeltjes-niveau of richt zij zich (ook) op grotere problemen? Pakt zij door op issues die zij signaleert? Houdt compliance de integriteitspiegel (voldoende) voor aan de business? Betrekt zij gedrag & cultuur in haar analyses en adviezen? Etc.

"In mijn ogen is er maar één defensielinie en dat is de onderneming als geheel..."

In dit kader is ook van belang de (toenemende) rol van interne beheersing in relatie tot de aard van de verhouding met en de werkzaamheden van de externe toezichthouder. Toezichtstrategieën zoals Toezicht op Maat (AFM), FOCUS! (DNB) en Horizontaal Toezicht (Belastingdienst) betrekken nadrukkelijk de kwaliteit van interne beheersing van de onderneming. Dit heeft bijvoorbeeld zijn weerslag op de toezichtintensiteit op een onderneming en de mate waarin een externe toezichthouder kan en willen leunen op de werkzaamheden van de onderneming zelf. In het kader van Horizontaal Toezicht is een aantoonbaar adequate interne beheersing (het zogenaamde 'tax control – of tax compliance – framework') zelfs een basisvoorwaarde voor het afsluiten van een convenant met de Belastingdienst. Ook bijvoorbeeld de Inspectie Leefomgeving en Transport zit op die lijn[3]. Een toezichtrelatie onder een convenant leidt tot een wezenlijk andere verhouding – veel meer op vertrouwen en transparantie, maar ook veel meer op beheersing dan op controle – met de externe toezichthouder dan zonder convenant. <<

Richard Bakkers is partner bij FPLC en is als opleidingscoördinator / kerndocent verbonden aan de Postgraduate opleiding Compliance & Integriteit Management

1 In COSO ERM implementatiehandboeken zien we dan wel weer de 'defensielinies' terugkomen, maar deze managementboeken zijn dan in de regel geschreven door consultants/adviseurs.
2 Hierbij geïnspireerd door het 'Why, How, What' model van Simon Sinek, zie http://www.startwithwhy.com/
3 Zie hiervoor de bijdrage van Han Pret in het vorige magazine (2012-2).

Symposium

‘Intern toezicht en compliance programma’s’

Op maandag 27 mei 2013 organiseren de Postgraduate Opleiding Compliance & Integriteit Management, De Nederlandsche Bank en Deloitte wederom hun jaarlijkse symposium.

Dit jaar gaat het symposium in op het thema‘Intern toezicht en compliance programma’s’. Gedurende de afgelopen jaren is de aandacht voor dit jaarlijks congres sterk toegenomen. Ook dit jaar hopen wij een boeiend programma te hebben samengesteld, waar wij u graag voor uitnodigen.
In het symposium van 2013 brengen wij business en compliance managers bij elkaar om met hen te discussiëren over de relatie tussen intern toezicht en compliance.
Intern toezicht wordt daarbij onderverdeeld in governance, besluitvormingsprocessen en gedragselementen. Het achterliggende vraagstuk is op welke wijze compliance kan bijdragen aan het borgen van de continuïteit van de organisatie, rekening houdend met de eisen die de moderne samenleving aan organisaties stelt.
Enkele toonaangevende sprekers zoals Erik van de Merwe (Achmea), Theo Bruijninckx (Ballast Nedam) en Olaf Sleijpen (DNB) zullen dit thema vanuit hun specifieke invalshoek uiteenzetten.
Vervolgens gaan we de opgedane inzichten in workshops verdiepen. <<

Aan deelname zijn geen kosten verbonden en is mogelijk vanaf half april via de site.

Alumnus aan het woord...

Arthur de Hart "Vertrouwen komt te voet en gaat te paard"

Postgraduate opleiding Compliance & Integriteit Management
Leergang 2

Het is voor mij al weer jaren geleden dat ik ben afgestudeerd. De opleiding was destijds een zeer financieel gerichte studie waar ik als eerste *"non-financial"* voor inschreef. Daarom heb ik ook met Jean Frijns gesproken over hetgeen de studie mij zou kunnen bieden.
Als intern toezichthouder bij Tata Steel ben ik met name geïnteresseerd in monitoring van gedrag, ethische vraagstukken en de mogelijkheid om mensen te helpen in het doen van de juiste dingen. Dit kan door opleiding, training, overtuigen en, met name, voorbeeldgedrag. In dat laatste geloof ik heel sterk. En dan bedoel ik niet alleen de directieleden, maar ook staffunctionarissen en het goede voorbeeld van je chef.
Ik profiteer nog altijd in mijn werk van de beslissing de opleiding te volgen.
Een groot deel van mijn werkzaamheden bestaat uit het onderhouden van het "Business Control Framework" in IJmuiden dat de COSO-aanpak volgt. Het framework is met name van de grond gekomen door de komst van Sarbanes – Oxley (SOX 302 / 404) en later ook de Nederlandse code Tabaksblat. Tabaksblat schrijft voor dat een Nederlandse onderneming een intern risicobeheersingssysteem moet hebben en dat het bestuur daar verantwoording over aflegt.
Deze "in-control statements" worden onderbouwd met intern toezicht. Daarbij worden afgesproken beheersingsmaatregelen binnen de onderneming periodiek getest.
Na de komst van het systeemgericht toezicht bij de grote accountantskantoren, rekenen zij op een gedegen risicobeheersing bij de ondernemingen. Aantoonbaar, transparant, onafhankelijk en professioneel.
Als Manager Compliance ben ik de zogenaamde "second line of defence" en help ik het locale management met deze maatregelen. Met name in het kader van de jaarrekening. Denk aan risico's bij inkoop, verkoop, voorraadwaardering, salarisadministratie en betaalsystemen. Een breed gamma.
Met de komst van Horizontaal Toezicht, rekenen Belastingdienst en de Douane ook op risicobeheersing op hun gebied. Het "Business Control Framework" heeft daarmee een nieuwe *boost* gekregen en een verdiepingsslag ondergaan. En net als bij de jaarrekening, stemmen we de risico's af in overleg met de toezichthouder en bespreken we de haalbaarheid van de maatregelen. Toezichthouders richten zich daarna alleen nog op restrisico's. Deze vorm van samenwerking is gebaseerd op vertrouwen en zal in de toekomst een grote vlucht nemen.
Hoe ik dat doe? In principe werk ik alleen, maar alle proceseigenaren (locale manager en controllers) zijn verantwoordelijk voor hun risico's en de afgesproken beheersingsmaatregelen. Het interne toezicht wordt door henzelf gedaan. Maar dan wel de een bij de ander. Bijvoorbeeld de financiële man of vrouw van Inkoop houdt toezicht bij HR en test daar de beheersingsmaatregelen. En dan ook andersom. Dat noemen we "Peer Review" en zo zie je hoe de beheersing *"bij de buren"* wordt uitgevoerd. Iedereen leert ervan en stimuleert elkaar.
Ikzelf houd het kwaliteitsniveau en de objectiviteit van het interne toezicht in de gaten. Hoe zijn de steekproeven, hoe is de testdocumentatie en wordt er kritisch doorgevraagd?
Toezichthouders maar ook de directie rekenen op het nakomen van gemaakte afspraken. En dan geldt het aloude adagium: "Vertrouwen komt te voet en gaat te paard". De samenwerking met toezichthouders is op basis van vertrouwen en te kostbaar om te verliezen!

Drs. Arthur de Hart RC EMoC
is Manager Compliance & Risk Management Tata Steel IJmuiden

Agenda

Leergang 2011
Blok IV: januari t/m juni 2013
Het laatste blok van de opleiding wordt helemaal besteed aan eigen onderzoek en het schrijven van een scriptie.

Leergang 2012
Blok II: 14 januari 2013 t/m 24 juni 2013
“Managen van Compliance en Integriteit”
In dit blok wordt gestart met het onderwerp ‘Compliance & Integriteit Cultuur’. Colleges over Compliance Leadership, Organisatiecultuur en Veranderstrategieën vormen de bouwstenen hiervoor. Vervolgens gaan de colleges dieper in op een aantal specifieke Compliance & Integriteit risico’s, die zowel voor financiële als voor niet-financiële ondernemingen relevant zijn, zoals: belangenverstrengeling, fraude, mededinging en privacy.
Aan het einde van dit blok ontvangen de studenten hun eerste scriptiecollege. In het tweede studiejaar wordt hiermee verder gegaan. Het definitief uitwerken van het onderzoek en het schrijven van de scriptie gebeurt in blok IV in het tweede studiejaar.

Najaar 2013
‘Compliance voor Financials en non-Financials’
Blok III is deels gesplitst in een traject financials en non-financials.

Het traject ‘Financials’, vast onderdeel van de opleiding, staat tevens open voor externe studenten die deze 8 colleges als losse module kunnen volgen. Inschrijving is mogelijk via de website van de opleiding.

Het traject ‘Non-financials’ gaat dieper in op compliance- en integriteitaspecten die specifiek zijn voor niet-financiële ondernemingen, zoals Zorgplicht voor non-financials’, ‘Traditionele Compliance en de weg naar nieuwe Compliancegebieden: van pharma tot zorg’ en ‘Inbedding van Compliance en Integriteit binnen een non-financial”.

Leergang 2013
Startdatum maandag 2 september: Agorazaal 5 Hoofdgebouw VU.
Inschrijving voor de opleiding via de website. Meer studie-informatie is te vinden op: www.feweb.vu.nl / opleidingen / postgraduate opleidingen / Compliance & Integriteit Management en op Blackboard voor de huidige studenten.

Symposium
“Intern Toezicht en compliance risico’s”

Op welke wijze kan compliance bijdragen aan het borgen van de continuïteit van de organisatie, rekening houdend met de eisen die de moderne samenleving aan organisaties stelt?
Maandag 27 mei van 13.00 – 19.00, toegang gratis.
Inschrijven mogelijk vanaf half april via de site.

Colofon

Compliance & Integriteit is een uitgave van De Vrije Universiteit, Postgraduate Opleiding Compliance & Integriteit Management
De Boelelaan 1105, 1081 HV Amsterdam
Compliance & Integriteit verschijnt 3x per jaar, oplage 400.

Redactie: Richard Bakkers, Sylvie Bleker en Eugénie Megens
Eindredactie: Eugénie Megens
Fotografie: Rinie Bleeker, Rotterdam / Peter-Paul Schouten, Hilversum / Shutterstock
Ontwerp & opmaak: Room for ID’s, Nieuwegein
Drukwerk: Damen, Werkendam