De LAT-relatie tussen Compli

Wellicht is er nog steeds een missing link tussen Compliance en Internal Audit: beide afdelingen laten namelijk een belangrijke kans liggen om door onderlinge afstemming en zo het totale gevoel van 'in control zijn' te vergroten.

Inleiding

De Compliance officer (CO) is medeverantwoordelijk voor het signaleren van relevante wijzigingen in wet- en regelgeving, ontwikkelen van voorstellen om die wijzigingen in de interne beheersingsmaatregelen verankerd te krijgen en het zorgdragen dat de organisatie binnen deze wet- en regelgeving blijft. Compliance is meestal verbijzonderd in een stafafdeling: zij heeft daarbij zelden de formele macht en mankracht de naleving van de regelgeving te controleren, laat staan dit binnen de organisatie af te dwingen. Zij beperkt zich veelal tot het vooraf beoordelen van proceswijzigingen en het meekijken bij het ontwikkelen (en accorderen) van nieuwe producten en diensten. Daarnaast gaat veel tijd zitten in het afhandelen van de geconstateerde uitglijders binnen de organisatie. Kan de CO zijn verantwoordelijkheid voor de naleving dan eigenlijk wel dragen als hij afhankelijk is van de goede wil van anderen in de organisatie? De algemene opinie is dat de CO dit uitsluitend kan realiseren door intensieve samenwerking met de andere lijn- en stafafdelingen.

Een andere afdeling die een sleutelrol speelt in het verschaffen van 'assurance' aan het verantwoordelijk lijnmanagement is de internal audit-afdeling. Door het regelmatig uitvoeren van (operational en financial) audits geeft men het topmanagement signalen over de mate waarin de kwaliteit van beheersing zich verhoudt met de uitgangspunten van de sturingsbeginselen, de inrichtingsmodaliteiten, de voorwaarden voor de processen en afdelingen in de organisatie. Dit moet het management in staat stellen haar aandacht te richten op die vraagstukken of objecten waar mogelijk controlproblemen spelen en zo waar nodig in te grijpen.

Tijdens een van de cursussen die opleiden tot certified Compliance officer (CCO) van NIBE-SVV is geconcludeerd dat veel CO's weinig contact hebben met hun collega's van Internal Audit. Ook werd bij het uitvoeren van audits weinig aandacht besteed aan eisen die voortkomen uit specifieke wet- en regelgeving. En als er aandacht aan werd besteed, dan bleek dat de opvatting over hoe en

ance en Audit

door wie Compliance moet worden getoetst niet altijd besproken, laat staan afgestemd te zijn. Het management maakt daar dan om haar moverende redenen handig gebruik van.
De conclusie was dan ook dat er wellicht nog steeds een missing link is tussen Compliance en audit: beide afdelingen laten namelijk een belangrijke kans liggen om door onderlinge afstemming en zo het totale gevoel van 'in control zijn' te vergroten.

Dit was de aanleiding voor NIBE-SVV om hierover met een aantal Compliance officers en auditors een 'ronde tafel gesprek' te organiseren. De centrale vraag tijdens dit gesprek was: moet de relatie tussen de Compliance-functie en de internal audit-functie verbeterd en versterkt worden?

Compliance: van effecten checken naar beleidsvorming

Op een, voor het seizoen, veel te warme dag in een broeierig zaaltje in restaurant Slangevegt in Breukelen zijn ze aangeschoven: Bianca Lambooij, Carlina Poelstra, Bob Seemann, Louwrens Abercrombie, Joop Winterink, Arie Molenkamp en Ron van Loon. En het lijkt wel onvermijdelijk bij een discussie over dit onderwerp; de eerste vraag die beantwoord moet worden is wat Compliance exact inhoudt. Compliance is nu eenmaal een nog relatief jong vakgebied en de Compliance-functie is nog steeds fors in ontwikkeling. Alle reden tot duiding van het begrip 'Compliance'.
Bianca Lambooij: "Compliance is de laatste 3 jaar totaal veranderd. Tot voor kort was de Compliance-functie uitsluitend gericht op de controle op effectentransacties. Pas de laatste jaren is er een Compliance-policy geformuleerd en is de functie grotendeels beleidsvoorbereidend geworden. We zijn niet alleen politieagent meer."

Als je Compliance letterlijk vertaalt is het simpelweg voldoen aan wet- en regelgeving.
Zo zijn de doelstellingen van het eerste COSO-rapport :

- effectiveness and efficiency of operations;
- reliability of financial reporting;
- Compliance with applicable laws and regulations;
- safeguarding of assets.

De centrale vragen:

1. Compliance en Internal Audit. Een logische noodzaak tot nadere samenwerking?
2. Waar ligt de verantwoordelijkheid voor het toetsen op naleving van wet- en regelgeving: Compliance of Internal Audit?
3. Hoort "Compliance with laws and regulation" in een interne / operational audit te worden meegenomen?
4. Bestaat er voldoende communicatie en samenwerking tussen de CO en de auditor? Zijn er best practices?
5. Bestaat er een kenniskloof tussen Compliance en Internal Audit-afdeling? Wat zou men over elkaars vakgebied moeten weten?

Hierbij wordt niet expliciet afgebakend welke wet- en regelgeving hiertoe behoren. Bij een dergelijke uitleg lijkt het werkterrein van Compliance vrijwel gelijk aan dat van een afdeling Juridische Zaken (JZ), een uitleg die niet veel organisaties hebben overgenomen.
Als de Compliance officer zich niet verantwoordelijk voelt voor alle wet- en regelgeving wordt het nog meer van belang wat het werkterrein van JZ is en wat de 'body of knowledge' van de Compliance-functie zou moeten zijn. Ook bij de deelnemers blijkt hier niet een 100% overeenstemming over te zijn.
Arie Molenkamp: "In sommige organisaties is bijvoorbeeld duurzaam ondernemen ('Sustainability') ook bij Compliance ondergebracht, hoewel dit lang niet altijd zaken betreft die door wetten worden afgedwongen." Het lijkt erop dat een deel van de keuzes, wat tot het vakgebied van Compliance wordt gerekend en wat niet, door persoonlijke voorkeuren binnen organisaties wordt bepaald. >

Participanten ronde tafel gesprek

- Arie Molenkamp RO is onderzoekscoördinator en kerndocent bij de Executive Master of Internal Auditing Opleiding van de Amsterdam Business School aan de Universiteit van Amsterdam
- Drs. Bob Seemann RA is Algemeen Directeur van NIVE-SVV bv
- Mevr. mr. Bianca Lambooij is Compliance Officer bij Corporate Compliance van ING en freelance docent
- Joop Winterink RA RE is vanaf 1 september 2007 Directeur Interne Accountantsdienst UVIT, daarvoor Hoofd Internal Audit en Compliance Officer bij PGGM
- Louwrens Abercrombie is Compliance Officer bij Delta Lloyd Bank Nederland
- Mevr. mr. Carlina Poelstra is Themamanager Compliance bij NIBE-SVV bv
- Drs. Ron van Loon RA is zelfstandig consultant en docent bij de Universiteit van Amsterdam

De scope van Compliance: voorbeelden van recente wet- en regelgeving

- NRTE 1999
- NRG 2002
- ROB
- WID / CDD
- Mifid
- Basel 2
- WTK
- WTT
- WBP
- Solvency 2
- WFD
- WFT
- MOT

Bianca Lambooij: "Het is eigenlijk ook niet zo belangrijk, als je binnen één organisatie maar een duidelijke en werkbare taakverdeling hebt. Wij spreken vaak van de risico-straat waarin functies als Compliance, Juridische Zaken en Operational Risk Management allemaal een specifieke functie vervullen. Afstemming tussen met name die 3 partijen is essentieel."

Een werkbare definitie

Een algemene noemer om het gebied van Compliance te definiëren en zodoende af te bakenen van dat van andere stafafdelingen is wellicht de volgende: tot het kerngebied van de Compliance-functie wordt (vrijwel) altijd gerekend die wetgeving, die gericht is op *financiële integriteit*. Deze financiële integriteit is gericht op 3 hoofdgebieden:

1 integriteit van medewerkers (onder andere algemene integriteit, bij effectentransacties, geheimhouding);
2 integriteit van klanten (onder andere CDD, Wet MOT, zorgplicht);
3 het productontwerp en de productadministratie (onder andere voorwaarden, transparantie, risico-beoordeling).

Dit wordt als een, in het algemeen, werkbare omschrijving gezien waarbij het nog steeds belangrijk is vast te stellen of de grenzen van het aandachtsgebied goed zijn afgebakend met de andere stafafdelingen.

Bob Seemann: "De CO adviseert over de inpassing van de wet- en regelgeving in de bedrijfsprocessen en het 'productontwerp', de auditor stelt vast of deze vertaling houtsnijdt en controleert op de naleving van de daarbij gemaakte afspraken in de praktijk"

De ontwikkeling van de Compliance-functie

De belangrijkste ontwikkeling van de Compliance-functie in de laatste 10 jaar is de verandering van 'effectenchecker' naar mede-beleidsvormer. Eind vorige eeuw was het prototype van de CO de medewerker die nauwgezet privé-beleggingstransacties van medewerkers beoordeelde, voor- of achteraf, en op basis hiervan de integriteit van medewerkers en het naleven van wettelijke vereisten op dit gebied bevorderde. In zeer korte tijd is zowel het werkterrein als de organisatorische positie van de Compliance-functie sterk veranderd: de hoeveelheid relevante wetgeving is geëxplodeerd. De CO rapporteert als hoofd van een, in omvang fors toegenomen afdeling, direct aan de Raad van Bestuur.

De participanten zijn het er over eens dat Compliance op het punt staat een tweede belangrijke veranderingsgolf door te maken.
Joop Winterink: "In sommige organisaties is de verantwoordelijkheid voor Compliance al volledig in de lijn gelegd. Dit is in een concept van integraal management eigenlijk redelijk logisch." De CO wordt dan vergelijkbaar met andere staf-specialisten, zoals HR en Finance: zij bieden specifieke kennis, maar de lijn is verantwoordelijk voor een goede implementatie en naleving van elementen.
Louwrens Abercrombie: "Basel II geeft richting aan de volgende stappen van Compliance. Ook de ontwikkelingen die je nu al in Engeland ziet, zullen de komende jaren herkenbaar worden in de Nederlandse situatie. Daar is het nu al gemeengoed dat de CO aansprakelijk gesteld kan worden door de toezichthouder bij een Compliance-probleem."
Bob Seemann: "De belangrijkste ontwikkeling op dit gebied speelt misschien wel buiten de bankensector. Tot voor kort vond men vrijwel uitsluitend verbijzonderde CO binnen banken. Dit heeft zich al uitgebreid tot verzekeraars, pensioenfondsen en overige financiële instellingen. Industriële en handelsbedrijven starten nu ook al met een gespecialiseerde functie op dit gebied. Je ziet dat daar onze geschiedenis zich aan het herhalen is. Een geschiedenis waarin met vallen en opstaan wordt

ontdekt welke aanpak het beste past bij het bedrijf of bij de bedrijfstak".

Samenwerking met stafafdelingen en de lijn

De CO zal, om succesvol te zijn, intensief moeten samenwerken met andere afdelingen. De CO participeert in een fors aantal overlegvormen en projecten, om het hoofddoel (zorgen dat de organisatie compliant is met de gedefinieerde wet- en regelgeving) te bereiken. Dit kan zich vertalen in overleg met de IT-afdeling om te zorgen dat eisen met betrekking tot bijvoorbeeld vertrouwelijkheid in systemen worden gerealiseerd. Een ander voorbeeld is overleg met de HR-functie om vast te stellen dat wetgeving die gericht is op het waarborgen van integriteit van medewerkers voldoende in procedures is opgenomen.
Een belangrijke samenwerkingsrelatie zou moeten bestaan met de afdeling die verantwoordelijk is voor het vormgeven van processen, procedures en hulpmiddelen zoals formulieren. De Compliance-functie zal deze afdeling moeten 'voeden' met informatie over wettelijke eisen, zodanig dat deze eisen in procesbeschrijvingen in instructies worden vastgelegd. En uiteindelijk is de CO afhankelijk van 'de lijn', die moet zorgen dat zaken die op papier staan ook daadwerkelijk worden uitgevoerd.

Een belangrijke activiteit van de CO moet zijn permanente voorlichting en communicatie naar de lijn toe, om vooral de bewustwording op het gebied van wet- en regelgeving te realiseren. Eenmaal gerealiseerd moet er een permanent 'circus' plaatsvinden om die bewustwording ook te houden.
Bianca Lambooij: "Alle nieuwe medewerkers wonen een of meer bijeenkomsten bij waar Compliance-aspecten worden benadrukt. Dit gebeurt deels in E-learning modules waarin medewerkers zowel kennis overgedragen krijgen, moeten nadenken over dilemma's die in de vorm van cases worden gepresenteerd en deels in intensievere opleidingen op het gebied van Compliance."
Louwrens Abercrombie: "Een initiatief, zoals ING heeft genomen om een persoonlijk boekje met interne regelgeving te produceren en aan alle medewerkers ter beschikking te stellen, zien we bij steeds meer organisaties uitgevoerd worden."
Kort gezegd is waarschijnlijk 50% van het werk van de CO het intern doorvertellen van de eisen die externe partijen aan ons stellen.

Afstemming met auditor?

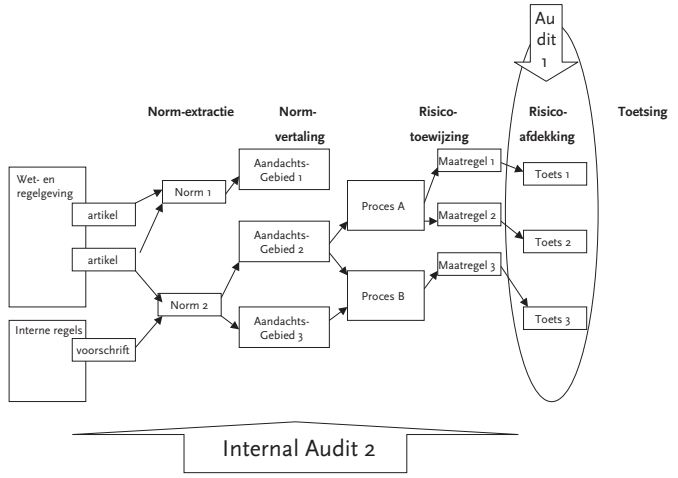
De samenwerking met de internal auditor blijkt in

Bianca Lambooij: "De CO is niet alleen meer een soort politie-agent."

organisaties nogal verschillend geregeld te zijn.
Joop Winterink: "Het hoofd Internal Audit is in sommige organisaties ook de CO, maar nooit eindverantwoordelijk voor Compliance. Dit blijft altijd het lijnmangement."
In sommige organisaties is ondertussen wel een regulier overleg opgezet tussen de Compliance-functie en Internal Audit. Naar een concrete taakafbakening en wijze van samenwerking moet soms nog worden gezocht.
Arie Molenkamp: "Door externe ontwikkelingen, zoals de wet Sarbanes Oxley zijn sommige organisaties de laatste jaren erg doorgeschoten in de nadruk die er op controls en verantwoording wordt gelegd. Hierdoor komt de natuurlijke taak van de internal auditor, het toetsen van en adviseren over beheersing, soms onder druk te staan."
De vraag of de Auditor een rol moet spelen bij het controleren op naleving van wet- en regelgeving kan vrij snel met 'ja' worden beantwoord.
Centraal in de discussie staat de relatie tussen Compliance en audit (zie figuur 1). De verantwoordelijkheid van CO kan vertaald worden van de >

Arie Molenkamp: "Externe wetgeving heeft audit soms met veel verplichte nummers opgezadeld zoals SOX."

Figuur 1 **De Compliance-functie en Internal Audit**



externe monitorfunctie (speuren naar wijzigingen in relevante wetgeving) tot en met het doorvertalen van gewijzigde wet en regelgeving in concrete procedures, instructies en hulpmiddelen. Na deze implementatie blijft echter nog behoefte aan de toetsing, of de vastgestelde instructies ook wel worden nageleefd. Dat wordt weergegeven in figuur 1, waarbij gecontroleerd wordt of in de dagelijkse werkzaamheden conform richtlijnen en instructies gewerkt wordt. De interne auditor moet in zijn normale audits dus meenemen of opzet en bestaan van de Administratieve Organisatie (AO) compliant is met de eisen die interne en externe regelgevers hebben geformuleerd. Met andere woorden of de interne procedure-afspraken worden nageleefd.

Joop Winterink merkt op dat dit slechts een deel van de waarheid is: "De internal auditor moet niet alleen kijken of 'de lijn' handelt conform instructies, ze moet ook kijken of de wetgeving adequaat en volledig is vertaald. Als ze dit doet voert ze in feite een audit uit op de Compliance-functie zelf!"

Louwrens Abercrombie: "Engelse ontwikkelingen, zoals aansprakelijkheid van de CO, zullen ook hier gemeengoed worden".

In sommige organisaties is het aspect Compliance nog geen expliciet onderdeel van het controleprogramma van de Internal Audit-functie. Soms voert Compliance zelf, ad hoc, enkele controles uit om vast te stellen of de organisatie de regelgeving naleeft. Dit is, behalve in zeer kleine organisaties waar men praktisch met het beperkt aantal personen moet omgaan, niet gewenst. Bob Seemann: "Auditing is het vergelijken van de aangetroffen werkelijkheid (de werkwijze en procedures) met de norm (de voorgeschreven werkwijze en procedures). Deze norm wordt idealiter ontwikkeld door de business samen met de Compliance Officer als 'advocaat van de duivel' en 'trusted advisor'. De Auditor controleert dan alleen of de wet- en regelgeving toereikend is vertaald naar deze voorgeschreven werkwijze en procedures en spreekt de Compliance officer aan indien hij afwijkingen constateert. Vervolgens stelt hij binnen zijn normale controleprogramma de naleving van de voorgeschreven werkwijze en procedures vast en confronteert de business met de bevindingen als dat nodig is. Ieder zijn vak met bijpassende verantwoordelijkheid en ook geen kans op functievermenging waarbij Compliance zijn eigen werkzaamheden zou controleren! Momenteel wordt een auditor nog wel eens gebruikt om de regeldrift van de CO aan de kaak te stellen. De auditor interpreteert dan zelfstandig de Compliance-eisen en stelt vast of de praktijk aan deze eisen voldoet. Wat daarbij wordt vergeten is dat bij het vertalen van de regels naar de praktijk weloverwogen keuzes worden gemaakt die daardoor opnieuw ter discussie kunnen worden gesteld. Dubbel werk dus en een bron van een zeer onvruchtbare relatie tussen auditor en CO."

Het lijkt logisch dat, net als voor andere aspecten van de bedrijfsvoering, er een duidelijke scheiding wordt aangebracht tussen de inrichtende taken (waar Compliance er een van is) en de toetsende taken (het verantwoordelijkheidsgebied van de auditor).

Compliance-kennis bij audit, audit-kennis bij Compliance

De vraag die opkomt is: kan de auditor simpelweg wel voldoende aandacht besteden aan Compliance. Herkent hij een 'Compliance-probleem' als hij erover 'struikelt'? Dit is zeker niet vanzelfsprekend,

daarom hebben sommige organisaties gewerkt aan het opbouwen van specifieke Compliance-kennis binnen de auditafdeling.
Louwrens Abercrombie: “Binnen onze afdeling Internal Audit zijn zes auditors aangewezen die een specifieke verantwoordelijkheid hebben om Compliance-aspecten in audits mee te nemen. Zij hebben hier gespecialiseerde kennis voor opgebouwd.”
Een ander model is de situatie waarbij de auditor een samenwerkingsovereenkomst met de CO aangaat en per audit, waar nodig, relevante kennis inleent. De CO stelt dan bijvoorbeeld een aantal uren van medewerkers per jaar ter beschikking waar de auditor, op basis van haar jaarplanning, een beroep op kan doen.

De vraag kan ook worden omgedraaid: weet de CO wat hij wel en niet van een auditor kan verwachten? Is hij op de hoogte van de doelstellingen van een operational audit, en het feit dat Compliance een van de vier hoofddoelstellingen van COSO-Internal Control Framework is? Is hij in staat om vragen die hij heeft zodanig te formuleren dat een auditor deze begrijpt en deze in een standaard-werkprogramma voor audits kan vertalen? Ook hier kan gesteld worden dat er een flink verschil bestaat per organisatie, waarbij sommigen al een ‘volwassen’ vorm van reguliere samenwerking hebben ontwikkeld, maar waarbij anderen nog aan het begin staan om een dergelijke wijze van werken te introduceren.

Conclusies

Na een lange en interessante discussie is de hoofdconclusie dat er geen algemene aanpak te geven is voor de inrichting van de Compliance-functie: daarvoor verschillen de organisaties van de deelnemers teveel van elkaar wat betreft omvang en de wijze waarop ze omgaan met Compliance-issues. Wel kan het volgende worden geconcludeerd:

1. Compliance heeft de laatste jaren een stormachtige ontwikkeling doorgemaakt. We staan echter niet aan het einde van een periode van verandering, maar misschien wel aan het begin van een nieuwe golf van ontwikkelingen rond het begrip Compliance. Om te zien wat ons te wachten staat is het misschien voldoende om even over de grenzen te kijken. Trends die op ons afkomen zijn onder meer de verdere versterking en professionalisering van de Compliance-functie en het introduceren van de Compliance-functie binnen andere organisaties dan banken, zoals verzekeraars en in de industrie.
2. Compliance is een (belangrijk) onderdeel van het ’in control zijn’ van de organisatie, en zou daarom in ieder geval in een toets op het gebied van beheersing moeten worden meegenomen. Dit gebeurt nu soms door de CO zelf en soms door de auditor. In een organisatie van redelijke omvang is het voor de afdeling Compliance zowel qua kennis als qua capaciteit in feite niet mogelijk om de toetsende rol te vervullen.
   Nu is er in het Internal Audit-vak altijd al gesproken over de wenselijkheid van het scheiden van de inrichtende en de toetsende taken binnen de organisatie: ook in dit kader is het veel logischer en wenselijker, dat het toetsen of de organisatie compliant is, door de auditor wordt verricht.
3. In een aantal organisaties realiseren de CO’s en auditors zich nauwelijks wat het werkterrein van hun collega-afdeling inhoudt. Communicatie is daarom soms zeer beperkt laat staan samenwerking.
   Het zou wenselijk zijn als beide functies meer van elkaar zouden weten en elkaar op het gebied assurance en Compliance kunnen vinden.

De doelstellingen van COSO (1992):

Internal control =
“a process, effected by an entity’s board of directors, management and other personnel, designed tot provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations;
- Reliability of financial reporting;
- Compliance with applicable laws and regulations;
- Safeguarding of assets

Joop Winterink: “de auditor moet ook de CO zelf auditen.

Ronde tafel gesprek

Benadrukt wordt dat samenwerken geen doel op zich is, het is een middel om de effectiviteit en daarmee de toegevoegde waarde voor het businessmanagement te vergroten. Welke invloed de samenwerking tussen organisatieonderdelen als compliance, auditing maar ook riskmanagement hebben op de business, wordt in het volgende artikel beschreven.

Drs. R.W.J. van Loon RA

De auteur is zelfstandig consultant en docent bij de Universiteit van Amsterdam

Mevr. mr. C.Y. Poelstra

De auteur is werkzaam bij

NIBE-SVV, afdeling Solutions