

WET IS BESCHERMING, GEEN BEDREIGING

Op naar een Effective Compliance Function

Financiële instellingen kunnen de compliancefunctie meer toegevoegde waarde laten leveren. Daarvoor zullen ze echter een antwoord moeten vinden op de groeiende druk die wet- en regelgeving opleggen. Het is daartoe belangrijk dat ze niet alleen voldoen aan alle relevante regels, maar ook een 'effective compliance function' (ECF) inrichten die integraal onderdeel vormt van hun risicomanagementmodel.

Door *Henny Rekelhof*

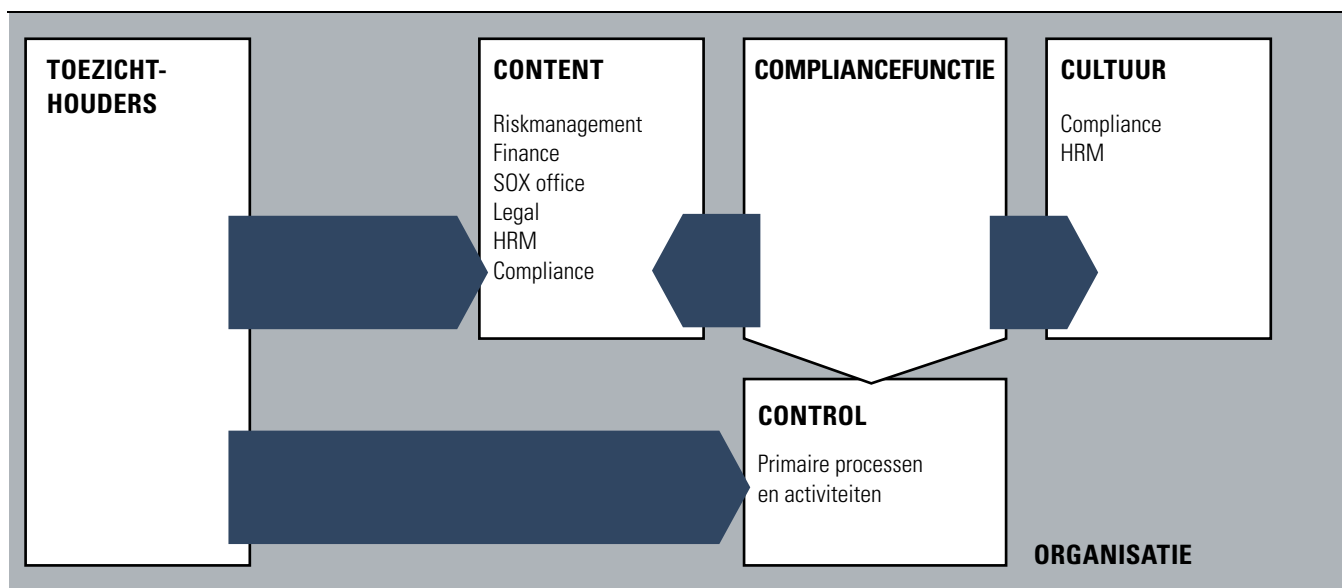
In de afgelopen tien jaar is er in hoog tempo een veelheid aan regelgeving voor financiële instellingen opgekomen en complexer geworden. Denk aan MiFID, WFT, Solvency II, SOX en SEPA en andere wetten en regels die de aandacht opeisen van afdelingen als compliance, finance en riskmanagement. Aan hen de taak om de opkomende ontwikkelingen in de regelgeving op het radarscherm te krijgen en een inventarisatie te maken van die regelgeving die geen invloed heeft op de huidige organisatie, maar dat in de toekomst mogelijk wel zal kunnen krijgen. Binnen bedrijven wordt de stortvloed aan regels vaak gezien als een bedreiging van het ondernemerschap. In werkelijkheid kan compliance het ondernemerschap ook ondersteunen. Het lijkt de gedelegeerde taak van de compliancefunctie om hier iets mee te doen. De toegevoegde waarde van de compliancefunctie ligt in het oproepen van verstand in plaats van weerstand. Het ondersteunen van de organisatie om met creatieve oplossingen te komen voor het voldoen of het bewerkstellingen van nieuwe business vanuit compliance. Voorwaarde is dat de financiële instellingen niet alleen voldoen aan alle relevante regels, maar ook een 'effective compliance function' (ECF) inrichten die integraal onderdeel vormt van hun risicomanagementmodel. In de hiernavolgende paragrafen schetsen we een aantal stappen die moeten worden gezet om tot een dergelijke ECF te komen. Allereerst zullen we ons richten op de definitie van de term compliance. Vervolgens willen we de inhoud van de compliancefunctie binnen een modern bedrijf bespreken. Daarna presenteren we een groeimodel waarin de mogelijke ontwikkelingen van de compliancefunctie

aan bod komen. Dit model geeft dan ook een goede gelegenheid om voor de totale functie of per regelgeving een Compliance Impact Assessment of 'health check' te verrichten. Ten slotte bespreken we in de conclusie kort de genoemde aandachtspunten om tot verdere verbetering van de compliancefunctie te komen.

De compliancefunctie kan grafisch worden weergegeven (zie onderstaande figuur). Daarbij wordt al snel duidelijk dat de complianceafdeling zeker niet de enige afdeling is die verantwoordelijk kan worden gesteld voor het 'compliant zijn' van een onderneming. De drie categorieën geven weer welke hoofdtaken er zijn voor de compliance-

deze basis kan de onderneming optimaal gebruikmaken van kennis en kunde die al in de onderneming aanwezig zijn. Specifiek nieuwe regelgeving kan aan de contentverantwoordelijke ter analyse worden voorgelegd. Een overzicht van de huidige organisatie en de gewenste organisatie (op basis van de aanvullende eisen en de analyse van welke zaken wel

Het huidige speelveld : Veel verschillende afdelingen, zonder coördinatie, maken het moeilijk te managen



ONZICHTBAAR Compliance kan worden gedefinieerd als het naleven door een organisatie van alle externe wet- en regelgeving waaraan ze, uit hoofde van de door haar verrichte activiteiten, zal moeten voldoen om haar doelstellingen te behalen. In deze definitie vangen wij dan ook het hele spectrum van regels die op ondernemingen kunnen afkomen (dus ook bijvoorbeeld Arbo- of milieuwetgeving). Over de inrichting en structuur van de compliancefunctie is daarmee nog niets gezegd.

functie. Content verschaft guidance voor de gehele onderneming die kan worden vastgelegd in interne richtlijnen (liefst zo weinig mogelijk). Culture: zorgt door middel van het geven van cursussen en communicatie binnen de onderneming dat kennis en houding doordringen in de onderneming. En als laatste Control: voor het werkelijk vaststellen of er wordt voldaan aan de intern gestelde richtlijnen, alsmede het rapporteren en analyseren van de uitkomsten in samenwerking met het management. Op

moeten veranderen en welke niet) levert een plaatje op van de stappen die moeten worden genomen. Belangrijk daarbij is dat hoe meer tijd men heeft, hoe rustiger de organisatie leeft. Binnen een tijdsbestek van twee jaar kleine, bijna onzichtbare veranderingen tot stand brengen is een ander proces dan een organisatie binnen zes maanden kantelen. Het is dan ook belangrijk om vast te stellen wat wel en wat niet al kan worden doorgevoerd. Een voorbeeld. Bij de overgang naar IFRS was bij de toenmalige IASB de IFRS

4-richtlijn in de maak omtrent de manier waarop volgens de IASB naar verzekeringscontracten werd gekeken. Belangrijke basislijnen in de richtlijn waren al snel bekend (halverwege 2003) en konden door de verzekeringsmaatschappijen al worden beoordeeld en doorgevoerd in de rapportagefunctie. Verzekeraars die deze stap namen, hadden zichtbaar minder problemen om uiteindelijk de 2004-deadline te halen dan de verzekeraars die pas bij het definitief worden van de richtlijn (voorjaar 2004) actie ondernamen.

KOSTBAAR Voldoen is leuk, blijven voldoen een must. Het huis op orde houden is van groot belang. Maar hoe komt men van 'niet voldoen' naar 'bijna automatisch voldoen'? Hiervoor is een groeimodel opgesteld dat de verschillende fasen probeert te onderscheiden.

In het model is, naast de verschillende stadia van compliance, ook weergegeven hoe de organisatie zelf wordt gekenmerkt. In eerste instantie zal de organisatie voornamelijk klagen over alweer extra regels waaraan men moet voldoen. De volgende fase is gericht op het voldoen aan de regels. De hoogste stadia kenmerken zich door het ontwikkelen van competitieve voordelen uit de complianceverplichtingen. Per stadium zullen de vier componenten Proces, Management en Governance, IT en Cultuur evenredig gereed moeten zijn om naar de volgende fase te kunnen gaan.

Wanneer er nieuwe wet- en regelgeving verschijnt en de onderneming daarop steeds reageert, zal er sprake zijn van ad-hoc-compliance. De organisatie zal in dat geval reactief, in redelijke mate voldoen aan de gestelde eisen. De ervaring leert

dat dit een zeer intensief en dikwijls tijdrovend en kostbaar traject is, vaak ook met behulp van (te?) veel externe krachten tot stand gebracht, waarbij de focus ligt op de contentcomponent. Zoals al eerder gezegd, heeft ook daarin het SOX-traject een goede voorbeeldfunctie. Terwijl de wet er in de zomer van 2002 door de regering Bush in sneltreinvaart doorheen werd gedrukt, startten de meeste trajecten pas halverwege 2004 (terwijl toen nog de 2005-deadline gold). Op dat moment (midden 2004) werd

moeten mogelijke extra veranderingen in de organisatie worden doorgevoerd. Waar in de eerste fase nog gebruik kon worden gemaakt van short cuts, zullen die in deze vervolgfase zo veel mogelijk teniet moeten worden gedaan. De controlcomponent wordt in dit stadium belangrijker. De complianceafdeling zal informatie moeten krijgen over de zaken die aanpassing behoeven om het 'voldoen' te verbeteren. De risico's op niet voldoen worden tijdens deze fase steeds verder verminderd.

Guidance wordt vaak moeilijk verkregen

pas begonnen met de risicoanalyse van de SOX-wetgeving, terwijl bijvoorbeeld Bazel II al veel langer werd besproken binnen de bancaire bedrijven en deze start al midden 2002 had kunnen worden gemaakt. In dit 'ad-hoc'-stadium zal de compliancefunctie zich nog voornamelijk richten op de vraag 'hoe te voldoen'. Moeilijkheid daarbij is dat guidance vaak moeilijk wordt verkregen (externe accountants doen vaak lang over het formuleren van een norm, aangezien zij wel toetsen, maar niet creëren). Bij Europese of afgeleide Nederlandse regelgeving beperken de toezichthouders zich vaak tot de passieve houding die bij principle-based regelgeving hoort.

SHORT CUTS Nadat men compliant is geworden, zal dat een tweede keer (repeatable compliance) aanzienlijk gemakkelijker zijn. De regels van het spel zijn bekend, het wordt alleen wat onwennig gespeeld. In deze fase is de nieuwe structuur van de organisatie bekend en

In de tussentijd heeft de functie wederom een groei doorgemaakt, externe resources zijn zo goed als verdwenen, de onderneming heeft haar complianceframework bevestigd en richtlijnen vormen een stevige basis om de onderneming conform de eisen te laten presteren. De nadruk komt steeds meer op de cultuur te liggen. Op dit volgende niveau is er sprake van manageable compliance. In deze fase verlegt de blik zich van extern naar intern. Het is belangrijk te bedenken dat de externe focus (welke regels komen er op ons af en welke invloed heeft dat) zeker niet mag worden onderschat, aangezien van de compliancefunctie wel wordt verwacht dat het radarscherm met daarop de naderende regelgeving op permanente basis beoordeeld wordt. De interne focus zal zich voornamelijk richten op de vraag: Hoe kunnen we onze processen verder aanpassen zonder compliance in de weg te staan? Daarnaast worden de issues die spelen tijdens gebruikelijke toetsingsmomenten (zowel van compliance als

andere attestatieonderdelen als audit en ORM) strak gemanaged en wordt er gericht gewerkt aan het oplossen van die issues. De rapportages aan toezichthouders worden verbeterd en de organisatie gaat bij verdere ontwikkelingen proactief met de toezichthouder in gesprek.

VRUCHTEN De verdere verbeteringen en vooral het trainen van het personeel (combinatie van HR en compliance) beginnen hun vruchten af te werpen. Al snel kunnen we spreken van sustainable compliance, waarbij de medewerkers van de onderneming zich steeds vaker vanuit zichzelf actief met de term compliance in het achterhoofd gaan mengen in discussies over de inrichting van processen. Dit begint met de manier waarop senior management en middenkader handelen in het geval van non-compliance. Wordt compliance alleen met de mond beleden of wordt er ook door het management integer en juist gehandeld?

Van daaruit worden steeds vaker ook business opportuniteiten gevonden die juist onder het complianceregime een voordeel voor de onderneming kunnen betekenen. Wanneer deze situatie is bereikt, is er sprake van 'beyond compliance'. Dan kan men er ook over denken om compliance mee te nemen in enterprise-riskmanagementmodellen als COSO II, waarin compliance een van de risico's is die de onderneming loopt, naast allerlei andere, vaak interne businessrisico's die kunnen ontstaan.

Concluderend kunnen we stellen dat de compliancefunctie wel degelijk iets zou kunnen doen aan de huidige weerstand tegen alle regelgeving. Het is niet gemak-

kelijk, maar zeker niet onmogelijk om de compliancefunctie zo in te richten dat er sprake kan zijn van manageable compliance (als minimaal vereist niveau).

Belangrijkste aspecten daarbij zijn de volgende.

- Allereerst zal het management zich ervan bewust moeten zijn dat compliance niet alleen een finance- of complianceaangelegenheid is, maar een veel bredere basis binnen de onderneming moet kennen. De complianceafdeling zal resources, maar vooral ook toegewezen verantwoordelijkheden en middelen moeten krijgen om als coördinerende afdeling te kunnen werken.
- De toezichthouder is je vriend, niet je vijand. Vaak kan de toezichthouder de onderneming vertellen hoe opkomende regelgeving geïnterpreteerd moet worden en moet hij evengoed zijn gedachten nog vormen om tot een zinvolle risicoanalyse te komen. (De AFM uit steeds vaker de behoefte om samen met organisaties te zorgen voor compliance in de markt.)
- Compliancefuncties zijn er niet als agent, maar veel meer als assistent van de onderneming, die de boot als een loods veilig door de compliancierivier naar de haven kan leiden.
- Men moet zich realiseren dat compliance niet het volgen van regels is, maar het volgen van ontwikkelingen en trends in de regelgeving. Op deze manier kunnen in een zeer vroeg-tijdig stadium risicoanalyses worden gemaakt en heeft de onderneming voldoende tijd om zich aan te passen aan de gevolgen van de invoering, nog voordat die een feit is.
- Compliance en daarmee het vertrou-

wen in de onderneming kan zich wel degelijk uitbetalen in beurswaarde. Aangezien de beurswaarde vaak gestoeld is op vertrouwen, kan dit in concrete gevallen zelfs worden gekwantificeerd.

- Uiteindelijk zou compliance op bestuursniveau moeten worden geïntegreerd in bestaande ERM-modellen, waarbij de risico's die compliance doelstellingen bedreigen, volledig worden meegenomen in de riskmanagementmodellen.
- Cultuur is een zacht begrip dat niet alleen tot stand komt door training, maar vooral door het handelen en voorbeeldhandelen van het management.

Een effectieve compliancefunctie is goed mogelijk. Daarvoor zal het management van de organisatie deze ECF met gerichte stappen vorm moeten geven. Waarbij het ondersteunen van een gezonde organisatie effectiever en efficiënter is dan het reactief beter maken van de patiënt. <<

Henny Rekelhof is Senior Business Consultant bij Atos Consulting