Compliancerisico's in control

Een nieuwe aanpak om evidence based en state-of-the-art aan opdrachtgevers te rapporteren over compliance en integriteit

Mr. dr. E.M.G. Creusen en drs. N. Westen[1]

Inleiding

Pensioenfondsen die hun werkzaamheden hebben uitbesteed aan uitvoeringsorganisaties leggen de lat voor wat betreft de kwaliteit van de uitvoering steeds hoger. Dat geldt ook voor de uitvoering van werkzaamheden op het gebied van compliance en integriteit. Als oorzaken kunnen worden genoemd de druk op het pensioensysteem, waardoor de pensioenconsument kritischer wordt, de steeds ingewikkelder wordende wet- en regelgeving waardoor de kans op fouten toeneemt, en niet in de laatste plaats de hogere eisen die binnenlandse en buitenlandse toezichthouders stellen.

De eisen worden niet alleen inhoudelijk opgeschroefd, maar ook de wijze waarop daarover verantwoording moet worden afgelegd is aan verandering onderhevig. Werd in de reeks 'trust me, show me, prove me' in het (recente) verleden nog genoegen genomen met 'trust me' en 'show me', tegenwoordig volstaat meestal nog slechts een met degelijk bewijsmateriaal onderbouwde rapportage ('prove me').

Gegeven de in het voorgaande geschetste nieuwe eisen, moeten pensioenfondsen en opdrachtnemers van die instellingen de bakens flink verzetten. Teneinde te kunnen voldoen aan de nieuwe inzichten moet een beter en meer systematisch ingericht compliance framework worden ontwikkeld. Een framework dat in staat stelt om op een trefzekere,

1 Mr. dr. E. (Ed) M.G.Creusen is Directeur Legal, Tax & Compliance en Chief Compliance Officer bij een pensioenuitvoeringsorganisatie. Drs. N. (Natascha) Westen is Manager Compliance, Risk & Bedrijfsvoering bij een pensioenuitvoeringsorganisatie. Dit artikel is op persoonlijke titel geschreven en bevat de opvattingen van de auteurs.

transparante en open manier de relevante compliance issues boven water te krijgen. Daarin zijn de 'harde' kant (naleving van wet- en regelgeving) en de 'zachte' kant (verbetering van gedrag en integriteit) ondergebracht in één bouwwerk dat zowel ruimte biedt aan de *uitvoering* van compliance activiteiten in een organisatie, alsook aan de *rapportage* over die activiteiten (en vooral de mate van assurance die de rapportage biedt). Met behulp van zo'n compliance framework kan een organisatie evidence based en state-of-the-art rapporteren.

Hoewel het in dit artikel beschreven compliance framework is opgezet vanuit een pensioenfondsoptiek, is het in beginsel geschikt voor alle organisaties die over compliance en integriteit moeten rapporteren aan opdrachtgevers en andere stakeholders. Op onderdelen zullen dan andere accenten moeten worden gelegd, maar dat doet niet af aan de opzet van het framework.

Organisaties hebben vaak moeite om externe wet- en regelgeving te vertalen naar heldere interne normen en regels. Dit wordt nog moeilijker als interne normen moeten worden gesteld die betrekking hebben op menselijk gedrag. Met betrekking tot dat laatste wordt dan verwezen naar een gedragscode (Code of Conduct). De rapportage komt dan meestal niet verder dan: er zijn dit kwartaal geen overtredingen van de gedragscode geconstateerd. Of, als het betreft naleving van wet- en regelgeving: er is dit kwartaal niet in strijd gehandeld met de relevante wet- en regelgeving. Maar hoe weten we dat het allemaal goed is gegaan? Blind vertrouwen op het rapporterende management (trust me)? En hoe is vastgesteld dat alle relevante regels in beeld zijn? Waar blijkt dat uit?
Het grote probleem is dus dat compliance en integriteit niet goed uit de verf komen als gevolg van te vage, globale interne normstellingen, en het veelal ontbreken van werkinstructies in de operationele sfeer. Daardoor is het bijna niet mogelijk om verantwoording af te leggen over de uitvoering van de compliance werkzaamheden. Compliance en integriteit dreigen dan rituele dansen te worden, met de daaraan inherente kans op het niet voldoen aan de vereiste hoge standaarden en het ontstaan van financiële of reputatieschade.

De grote uitdaging is dan ook om de bovenbeschreven situatie van haar 'vrijblijvendheid' te ontdoen en te vervangen door een organisatie en interne beheersing die op het gebied van compliance aantoonbaar in control zijn.

In dit artikel wordt in de vorm van een samenhangend geheel van processen een model beschreven dat naar het oordeel van de auteurs in hoge mate voldoet aan de eisen die heden ten dage worden gesteld aan een volwassen compliance bouwwerk en aan de rapportage over de producten die dat bouwwerk voortbrengt. Door de ontwikkeling van deze evidence based methoden, protocollen, monitors, toetsingsinstrumenten, implementatietools kan effectief en resultaatgericht compliance in de organisatie worden gevolgd en bijgestuurd waar nodig.

Maatschappelijke ontwikkelingen

Compliance heeft in de laatste decennia van de vorige eeuw en het eerste decennium van deze eeuw ingrijpende ontwikkelingen doorgemaakt. Dat heeft veel te maken met de omstandigheid dat de maatschappelijke normen over wat wel aanvaardbaar is en wat niet, zich in dit vlak in hoog tempo hebben ontwikkeld. Een voorbeeld ter illustratie. Nog niet zo heel erg lang geleden was het handelen in effecten met voorwetenschap niet ongebruikelijk. Sterker nog: het werd soms positief gewaardeerd als iemand gebruik maakte van zijn kennisvoorsprong. Slechts enkele decennia later is eenzelfde handelwijze strafbaar vanuit de – terechte – gedachte dat ook hier een level playing field dient te gelden.

Ook de excessen die zich hebben voorgedaan in het (internationale) bedrijfsleven hebben compliance hoger op de agenda geplaatst. Dit heeft geleid tot aanscherping van de boekhoudregels met soms verstrekkende gevolgen (denk aan de Sarbanes Oxley wetgeving in de Verenigde Staten). Falend in- en extern toezicht, alsmede een verkeerde cultuur in de bestuurskamers van bedoelde ondernemingen hebben dit veroorzaakt.

Tegen de achtergrond van bovengeschetste ontwikkelingen is ook de attitude jegens de inbedding van compliance en integriteitmaatregelen in de loop der tijd in positieve zin gewijzigd. Ten tijde van het ontstaan van de eerste complianceregels werden die beschouwd als een ongewenste last. Daarna werd het beschikken over een goede inrichting van de compliance-organisatie gezien als een 'unique selling point' bij het werven van nieuwe klanten (deze vraag wordt al gesteld in het offertetraject), tegenwoordig heeft een organisatie een achterstand als zij haar compliance framework niet op orde heeft. Je merkt dat de druk van de toezichthouders toeneemt. Klanten willen inzicht in de wijze waarop compliance is ingericht en wordt beheerst. Dit leidt tot meer verantwoording.

Rule based versus principle based

Zoals hierboven aangegeven hebben uiteenlopende gebeurtenissen tot gevolg gehad dat de wetgeving op verschillende beleidsterreinen aanzienlijk is verscherpt, waarbij detailvoorschriften niet werden geschuwd. En nog steeds, tot op de dag van vandaag, zien we de stroom financiële en verslaggevingwetgeving toenemen.

In een *rule based* benadering wordt gedetailleerd voorgeschreven hoe moet worden gehandeld. Er is in beginsel weinig of geen ruimte voor eigen interpretatie; daardoor wordt een hoge mate van rechtszekerheid geboden alsmede rechtsgelijkheid: iedereen past de regel immers op dezelfde manier toe. Er kunnen evenwel kanttekeningen worden geplaatst bij een dergelijke benadering. De eerste is dat een zekere starheid kan optreden. Als maatschappelijke trends veranderen kan de regelgeving gaan achterlopen. Deze moet namelijk steeds formeel worden gewijzigd door de wetgevende instanties. Een tweede kanttekening betreft het risico dat de regelgeving niet alle praktijksituaties dekt. Het is

van groot belang dat de rule based benadering zo is ingericht dat deze bestuurbaar is. Anders is er van rechtsgelijkheid geen sprake meer.

Een *principle based* benadering heeft eveneens positieve en negatieve kanten. Eigenlijk zijn dit in hoofdzaak de tegenhangers van de negatieve en positieve aspecten van een rule based insteek. Inherent aan een principle based systeem is de hoge mate van flexibiliteit. Doordat wordt gewerkt met zogenaamde open, abstracte normen kan een dergelijk systeem op flexibele wijze maatschappelijke opvattingen en trends volgen. Tegelijkertijd is ook nauwelijks denkbaar dat er praktijksituaties tussen wal en schip vallen, omdat elke situatie wel onder een norm zal zijn te brengen.
Aan de andere kant bergt een principle based aanpak ook risico's in zich. Het grootste risico is dat regels op een zeer uiteenlopende wijze worden toegepast vanwege de grote interpretatieruimte. Daarmee bestaat ook het gevaar dat die ruimte leidt tot een toepassing die te zeer afwijkt van doel en strekking van een bepaling. Je kunt je dan ook afvragen in hoeverre organisaties die uitsluitend volgens dit principe werken in control zijn.

Het onderscheid tussen rule based en principle based speelt een grote rol bij vraagstukken inzake compliance en integriteit. Juist daar kunnen opvattingen wat goed is en wat niet, sterk uiteenlopen, met alle gevolgen van dien. De in het voorgaande gememoreerde excessen in het bedrijfsleven spreken in dat verband voor zich. Omdat beide modellen voor- en nadelen hebben is in de loop van de tijd dan ook een slingerbeweging waar te nemen. Een grote mate van vrijheid (principle based) heeft in het verleden aan de basis gestaan van de genoemde 'ongelukken'. De maatschappelijke reactie was heftig: de slinger bewoog zich met grote snelheid in de richting van een rule based systeem. Vervolgens gingen er toch weer stemmen op om het gevoel een grotere rol te laten spelen bij de besluitvorming over belangrijke (bestuurlijke) vraagstukken.

De praktijk worstelt duidelijk met de vraag welk model het meest tegemoet komt aan de maatschappelijke wens om als organisatie zo compliant en integer als mogelijk te handelen. We zien dan ook dat compliance in organisaties niet volgens een vast stramien is ingericht.
Dat heeft overigens niet alleen te maken met de hiervoor beschreven zoektocht naar het optimale model, maar ook met het nagestreefde ambitie niveau (welke mate van assurance wil ik afgeven). Zoals in de Inleiding beschreven ligt het ambitieniveau voor de pensioenuitvoeringsorganisaties tegenwoordig heel hoog. Het model dat hierna wordt beschreven voldoet aan dit ambitieniveau. Zoals zal blijken kan dit slechts worden bereikt door het accent te leggen op een rule based aanpak, zonder dat dit ten koste gaat van de noodzakelijke flexibiliteit.

Een nieuw compliance framework

In veel organisaties brengt het compliance framework (als het al bestaat) het niet verder dan de inrichting (opzet en bestaan), en is het met het functioneren ervan zeer matig gesteld (werking). In het navolgende wordt een samenhangend instrumentarium beschreven dat een organisatie tevens in staat stelt de werking van het compliance framework aan te tonen.

Een state-of-the-art compliance framework bestaat uit een degelijk bouwwerk dat goed gefundeerd is, ook overigens een stevige structuur heeft, en effectief en efficiënt kan worden gebruikt. In compliance framework termen bestaat het fundament uit een duidelijk opgezette structuur, waarin zijn opgenomen alle producten van de betreffende organisatie, alsmede welke wet- en regelgeving daarop van toepassing is. Producten en wetgeving zijn geclusterd in zogenaamde thema's (zie voor een definitie hierna onder De Compliance Rapportage). De overige componenten van de basisstructuur zijn het Compliance Charter, het Compliance Program en de Code of Conduct. Deze basisstructuur zorgt er in combinatie met de overige instrumenten voor dat alles adequaat functioneert. De overige instrumenten zijn de zogenaamde Wet- en regelgevingmonitor (om de correcte naleving van wet- en regelgeving te waarborgen) en de Compliance Rapportage.

Het fundament en de overige structuur vormen als het ware opzet en bestaan van het bouwwerk, de overige instrumenten zorgen voor de werking van het geheel.

Alle genoemde instrumenten worden in het navolgende behandeld, waarbij uiteraard ook hun onderlinge samenhang aan de orde komt.

Het Compliance Framework
Het Compliance Framework is een matrix waarin de samenhang tussen wetgeving en producten/diensten is vastgelegd met behulp van thema's.

Het Compliance Charter
Het Compliance Charter bevat vier onderwerpen, te weten de *algemene uitgangspunten van compliance* binnen een organisatie, de *inrichting van compliance*, het *compliance risico management*, en tenslotte de *compliance documenten*. Gelet op het belang van het Compliance Charter dient het te worden vastgesteld door het hoogste orgaan, zijnde de Raad van Bestuur of Directie.

Onder de *algemene uitgangspunten* worden in elk geval de volgende kwesties geadresseerd:
- De definitie van compliance.
- De missie van compliance.
- De doelstellingen van compliance.
- Beantwoording van de vraag wie verantwoordelijk is voor compliance en integriteit.
- De scope van compliance (welke wetgeving valt er onder, welke niet).

Het belang van een *juiste inrichting van compliance* is nauwelijks te onderschatten. In het Compliance Charter worden in deze paragraaf de volgende onderwerpen beschreven:
- De positionering: waar in de organisatie kunnen we compliance vinden? Dat kan één plaats zijn, maar in een grote organisatie ook meerdere plaatsen. Uitgangspunt is in elk geval dat het lijnmanagement verantwoordelijk is voor compliance, en niet de compliance functie.
- Onafhankelijkheid: de compliance officer moet op een onafhankelijke wijze aan de hoogste leiding van een bedrijfsonderdeel dan wel aan de centrale leiding kunnen rapporteren. Dit kan deze functionaris overigens in een lastige positie brengen: loyaal aan de eigen directe leiding, of – als dat aan de orde is – loyaal aan de hoogste leiding van bedrijfsonderdeel of organisatie?
  Een belangrijk punt van aandacht is dat ingeval sprake is van een 'gelaagde' structuur van de compliance organisatie (een centrale chief compliance officer en decentrale compliance (afdelings) officers), de decentrale *managers* rapporteren aan de chief compliance officer, die vervolgens rapporteert aan de hoogste leiding van de organisatie. Een andere governance (de decentrale compliance officers rapporteren aan de chief compliance officer) zou er toe kunnen leiden dat de decentrale managers hun verantwoordelijkheid ontlopen.
- Taken, verantwoordelijkheden en bevoegdheden van de compliance officers (eventueel op verschillende niveau's) worden gedetailleerd beschreven in het Compliance Charter. Dit is essentieel omdat de functie scherp moet worden afgebakend ten opzichte van bijvoorbeeld risk controllers en interne accountants. In die beschrijving dient ook de onafhankelijke positie ondubbelzinnig tot uitdrukking te komen.

Het *compliance risico management* is eigenlijk de beschrijving van het hart van de werking van het compliance framework. In deze paragraaf wordt kort en krachtig uiteengezet hoe het compliance risico- en monitoring framework eruit dient te zien. Tevens wordt gedefinieerd wanneer mag worden geconstateerd dat de organisatie compliant is, deels compliant, of niet compliant. Het sluitstuk is de monitoring en rapportage. Daarop wordt later uitvoerig teruggekomen, omdat deze activiteiten de kern vormen van het aantonen van de werking van het bouwwerk.

In de paragraaf *compliancedocumenten* tenslotte worden de verschillende documenten beschreven die samen het compliancebouwwerk vormen.

Het Compliance Program
Het Compliance Program is een document dat jaarlijks door de compliance officer wordt opgesteld en door de hoogste leiding van de organisatie (of een organisatie onderdeel) wordt vastgesteld. Het bevat het gedetailleerde werkplan van de compliance afdeling in een (kalender)jaar. Naast de vaste programma-onderdelen zoals de periodieke rapportages, kunnen hierin bepaalde speerpunten worden opgenomen, onderwerpen die in dat jaar extra aandacht krijgen. Uiteraard wordt over de resultaten en bevindingen van de uitvoering van het programma gerapporteerd in de rapportages.

De Code of Conduct
De Code of Conduct (gedragscode) is een belangrijk document in dienst van het bevorderen van integriteit van de medewerkers in een organisatie. Onderwerpen die in een pensioenfondsomgeving daarin een plaats behoren te hebben zijn in elk geval het effectentypisch gedragstoezicht, het aanvaarden en geven van uitnodigingen en geschenken, en het aanvaarden van nevenfuncties. In een andere omgeving zou bijvoorbeeld kunnen worden gedacht aan een integere behandeling van klanten, of aan een zuivere rol bij het inschrijven op een aanbesteding.

Evenals de andere compliance instrumenten dient de Code of Conduct een gedetailleerde beschrijving te geven van het gewenste dan wel ongewenste gedrag. Een code die slechts principes bevat biedt te weinig guidance en komt vaak niet verder dan de bekende 'open deuren' ('Gij zult niet stelen'). Uiteraard is het belangrijk dat de code aangeeft welke sancties staan op overtreding.

Tenslotte is het in het kader van de awareness nuttig om bij elke min of meer ingrijpende wijziging van de Code of Conduct de medewerkers opnieuw te laten verklaren dat ze bekend zijn met de inhoud van de code en deze te zullen naleven.

De Wet- en regelgevingmonitor
Veel organisaties hebben grote moeite om te waarborgen dat de voor hen geldende – vaak complexe – nationale en internationale wet- en regelgeving tijdig, juist en volledig wordt nageleefd. Dit geldt vooral voor organisaties die meerdere bedrijfsonderdelen hebben, die verschillende activiteiten verrichten waarop soms verschillende, soms dezelfde wetgeving van toepassing is. De kunst is dan om alle relevante wetgeving tijdig bij de juiste afdeling te krijgen. Tijdig wil niet zeggen de mededeling dat een wet in het Staatsblad is geplaatst. In de meeste gevallen zal er behoefte aan zijn om in een (zeer) vroegtijdig stadium te weten welke voorstellen er in voorbereiding zijn. Dat kan nodig zijn omdat er misschien een lobby-activiteit moet worden opgestart, maar zeker ook omdat nieuwe wet- en regelgeving vaak (ingrijpende) impact heeft op bedrijfsprocessen.

Voor een goede werking van het geheel dient aan ten minste twee randvoorwaarden te worden voldaan. In de eerste plaats moet een breed scala van informatiebronnen voorhanden zijn opdat nieuwe ontwikkelingen kunnen worden opgemerkt. Dat zullen veelal digitale bronnen zijn, maar het kan ook op andere wijze. In de tweede plaats zal er in de organisatie voldoende deskundigheid aanwezig moeten zijn om de opgeleverde informatie te beoordelen op impact voor de organisatie.

De werking van de Wet- en regelgevingmonitor:

1. Door middel van het vooraf gedefinieerde compliance framework wordt vastgesteld welke wet- en regelgeving systematisch moet worden gevolgd.

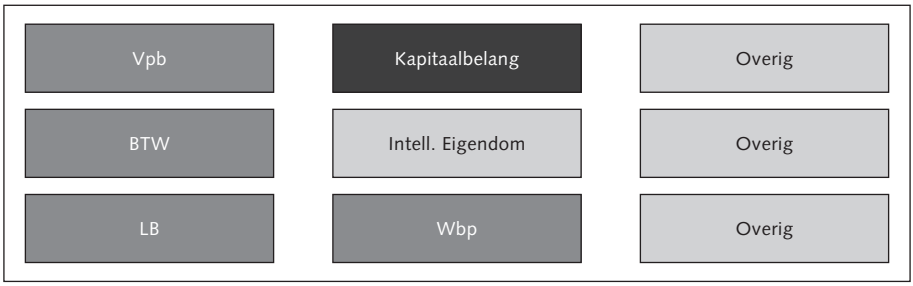
2. Vervolgens wordt bepaald wie wordt belast met het volgen van welke wet- en regelgeving. Hoewel de betreffende wetgeving wordt toegewezen aan een medewerker die of bedrijfsonderdeel dat daarmee het meest te maken heeft, kan het voorkomen dat de betreffende wetgeving ook voor andere personen of onderdelen van de organisatie van belang is. Daarom moeten in beginsel alle wijzigingen, ook die welke niet onmiddellijk van belang zijn voor de medewerker of het bedrijfsonderdeel dat is belast met de monitoring, worden gemeld (zie punt 3).

3. Maandelijks melden alle monitorende medewerkers/bedrijfsonderdelen de status van de wijzigingen aan de centrale compliance afdeling[2]. Onder status wordt hier verstaan de fase waarin het wijzigingsproces zich bevindt (bijvoorbeeld een eerste opvatting van een bewindspersoon, behandeling in de Tweede Kamer, plaatsing in het Staatsblad, etc.).

4. De centrale compliance-afdeling beheert de Wet- en regelgevingmonitor. Dit is een digitaal overzicht waarin per gevolgde wet of regeling is aangegeven welke wijzigingen op stapel staan en in welke fase deze zich bevinden. En in hoeverre de afdelingen die hier mee te maken krijgen op schema liggen met betrekking tot de voorbereiding van de implementatie van de aankomende wijzigingen. Zo wordt gevolgd of de betreffende wijzigingen tijdig en juist in de processen worden doorgevoerd.

2 Hier wordt gesproken over de centrale compliance-afdeling. In kleinere organisaties zal er meestal slechts één compliance-afdeling/compliance officer zijn. Hetzelfde geldt voor voor de plaatsen waar in het navolgende wordt gesproken over Chief Compliance Officer; in kleinere organisaties zal er slechts sprake zijn van één compliance officer. Dit doet niet af aan de werking van het model.

Op basis van de input van de medewerkers/bedrijfsonderdelen wordt de Wet- en regelgevingmonitor maandelijks van een update voorzien en gepubliceerd op de website van de centrale compliance afdeling. Per wet geeft de Wet-en regelgeving-monitor tevens aan voor welke medewerkers/bedrijfsonderdelen die wet relevant is.



Figuur 1. Bezoekers van de Wet- en regelgevingmonitor komen via een knop op de start-pagina rechtstreeks terecht bij de betreffende wet- of regelgeving.

5. Uit het in de Wet-en regelgevingmonitor opgenomen statusoverzicht per wet of regeling kan door de centrale compliance afdeling worden afgeleid of tijdige, juiste en volledige implementatie ook daadwerkelijk plaatsvindt. Daarmee vervult de Wet-en regelgevingmonitor tevens een rol als sturingsinstrument.

Met dit instrument wordt bereikt dat in beginsel geen relevante wetswijzigingen worden gemist, dat er steeds een up-to-date overzicht van de stand van zaken is, en dat de medewerkers/bedrijfsonderdelen die wat met de op handen zijnde wijzigingen moeten doen daarvan op de hoogte zijn. Daarnaast wordt gecontroleerd of de implementatie daadwerkelijk is doorgevoerd.

De Compliance Rapportage

De periodieke Compliance Rapportage (CR) is het centrale document waaruit blijkt hoe het is gesteld met de compliance en integriteit in een organisatie. In deze rapportage wordt over alle onderwerpen die te maken hebben met compliance en integriteit uitvoerig en gedetailleerd gerapporteerd.

In de Compliance Rapportage worden de voor een organisatie gedefinieerde *Compliance thema's* verbonden met de zogenaamde *Compliance producten* en de *wet- en regelgeving* die via de Wet- en regelgevingmonitor wordt gevolgd. In het navolgende worden de Compliance thema's en Compliance producten toegelicht. Daarnaast hebben alle

overige onderwerpen die te maken hebben met compliance en integriteit een plaats in de rapportage. Om goed inzicht te krijgen in dit belangrijke document wordt het in het navolgende uitvoerig behandeld.

Definities
Een *Compliancethema* ('thema') is een aandachtsgebied van een organisatie waarbinnen compliance een belangrijke rol speelt; niet-naleving van wet- en regelgeving kan betekenen dat producten (zie hierna) binnen een thema niet compliant zijn, en daarmee het thema niet. Thema's zijn bijvoorbeeld: het ontwikkelen en beheren van producten, interne waarden en gedrag, fiscaliteit, privacy.

Een *Compliance product* ('product') is een product dat kan leiden tot non-compliance indien niet tijdig, juist en/of volledig aan de op dat product betrekking hebbende wet- en regelgeving wordt voldaan. Bij de voorbeeldthema's behorende producten zijn bijvoorbeeld: een pensioenreglement, een gedragscode, een fiscale aangifte of een intern voorschrift van de Functionaris voor de Gegevensbescherming (FG).

Samenhang producten en wet- en regelgeving
De producten moeten voldoen aan de daarop betrekking hebbende wetgeving, en moeten worden aangepast als wijziging van die wetgeving daar aanleiding toe geeft. Weer de voorbeelden volgend: wijziging van de Pensioenwet kan leiden tot aanpassing van het pensioenreglement, wijziging van de wetgeving inzake beheerste en integere bedrijfsvoering kan leiden tot aanpassing van de gedragscode, wijziging van de Wet op de vennootschapsbelasting kan van invloed zijn op de aangifte vennootschapsbelasting, een wijziging van de Wet bescherming persoonsgegevens kan aanpassing van het interne voorschrift van de FG noodzakelijk maken.

Samenhang producten en thema's
De thema's behoren het totale compliancegebied van een organisatie te dekken. Indien derhalve goed is nagedacht over de vraag of alle producten onder een thema zijn benoemd, dan kan er theoretisch gezien niets tussen wal en schip vallen. Het kan zijn dat er in de loop der tijd iets wijzigt op het gebied van wet- en regelgeving; hier sluit de Wet- en regelgevingmonitor dan onmiddellijk op aan. Tijdens de monitoring wordt er gekeken welke producten eventueel aangepast dienen te worden. Het kan ook zijn dat hieruit een nieuw product voortkomt; dit wordt dan verwerkt in het framework waardoor de organisatie weer in control is.

Beoordeling status compliance
In elke CR dient op basis van een toetsing een statusoverzicht te worden opgenomen inzake zowel de mate waarin de aan de thema's gekoppelde producten (en daarmee de thema's) worden beheerst (hebben we alle producten in beeld?), als de mate waarin de

aan de wet- en regelgeving gekoppelde producten worden beheerst (voldoet elk product aan de relevante wet- en regelgeving?). Deze dubbele invalshoek geeft extra comfort dat er niets wordt vergeten. Middels kleurstelling (groen, geel of rood, elke kleur duidelijk gedefinieerd) kan in één oogopslag de status worden gekend.

Opzet CR
Teneinde de leesbaarheid van de omvangrijke CR te bevorderen is deze onderverdeeld in een 'hoofdtekst' en een aantal bijlagen, ruwweg in de verhouding 1:3. De hoofdtekst is zelfdragend en geeft op hoofdlijnen een beeld, de bijlagen bevatten gedetailleerde informatie. De hoofdtekst informeert het (top)management adequaat over de stand van compliance en integriteit in de organisatie; de hoofdtekst begint met een Management-samenvatting die de 'highlights' bevat voor de hoogste leiding.

Hoewel de hoofdtekst zelfstandig kan worden gelezen, bevatten de bijlagen belangrijke *sturingsinformatie*. Gesteld zou kunnen worden dat de hoofdtekst aangeeft op welke gebieden de organisatie compliant is en op welke niet of onvoldoende, en dat uit de bijlagen blijkt wat er moet gebeuren om een hoger niveau van compliancy te bereiken.

Inhoud hoofdtekst
Om een meer concreet beeld te geven van de inhoud van de hoofdtekst van de CR worden onderstaand de onderwerpen weergegeven die achtereenvolgens aan de orde komen.

- Managementsamenvatting (de 'highlights').
- Inleiding (kernpunten van de CR – 'oneliners' – ingedeeld naar thema's).
- Overzicht compliancethema's (per thema biedt de kleurstelling onmiddellijk inzicht in de status).
- Materieel toezicht (per wet- en regelgeving biedt de kleurstelling onmiddellijk inzicht in de status).
- Incidenten (overzicht compliance incidenten in de verslagperiode: lopend aantal ultimo vorige periode, aantal nieuw gemeld, aantal afgehandeld, lopend aantal ultimo huidige periode, aantal gemeld aan toezichthouder).
- Organisatorische ontwikkelingen van belang voor compliance (deze ontwikkelingen kunnen van invloed zijn op de compliance structuur).
- Monitoring gedragscode (hier wordt een overzicht gegeven van aantallen geschenken, uitnodigingen en nevenfuncties).
- Betrouwbaarheidstoetsing (de compliance officer begeleidt toetsingen door de toezichthouder van nieuwe (mede)beleidsbepalers).
- Integriteitbeleid (de gedefinieerde integriteitrisico's worden middels kleurstelling gescoord).

De hoofdtekst van de CR geeft dus vooral aan waar het in de organisatie al dan niet fout zit met compliance en integriteit. De uitwerking is te vinden in de bijlagen (zie hierna).

Inhoud bijlagen
De CR bevat vier bijlagen.

Bijlage 1 bevat de status van de activiteiten binnen de Compliancethema's. In deze bijlage worden per thema de onderwerpen behandeld die in de betreffende verslagperiode vermeldenswaard zijn. Bij elk onderwerp wordt een toelichting gegeven, worden een of meer aandachtspunten benoemd, en wordt de status beschreven. Met name aandachtspunten en status bieden sturingsinformatie voor het management.

Bijlage 2 bevat een toelichting op nieuwe en gewijzigde wet- en regelgeving. De input voor deze bijlage wordt geleverd door de Wet- en regelgevingmonitor. Naar analogie van de systematiek bij de onderwerpen in Bijlage 1 wordt ook hier elke nieuwe of gewijzigde wet of regeling voorzien van een toelichting en status.

Bijlage 3 geeft een overzicht van de bevindingen ten aanzien van de toetsing van privé-effectentransacties die door insiders zijn verricht.

> Geplande privé-effectentransacties van medewerkers en anderen die als zogenaamde 'insider' zijn aangemerkt worden geadministreerd in een geautomatiseerd systeem. Dit systeem controleert of het betreffende instrument (aandeel, obligatie, etc.) verhandeld mag worden. Het verzoek daartoe wordt geregistreerd (pre-clearance) en de aanvrager krijgt een e-mail met toestemming of weigering om de transactie uit te voeren. De daadwerkelijk uitgevoerde transactie wordt opgevoerd in het systeem met daarbij een upload van de effectennota als bewijs dat de transactie is uitgevoerd.

Bijlage 4 tenslotte bevat een overzicht van de contacten die in de verslagperiode hebben plaatsgevonden met toezichthouders. Het gaat dan om De Nederlandsche Bank (DNB), de Autoriteit Financiële Markten (AFM), het College bescherming persoonsgegevens (CBP), alsmede buitenlandse toezichthouders.

Flankerende maatregel
Om het beschreven framework goed te laten werken en te bereiken dat de CR elk kwartaal verder wordt verbeterd, vindt maandelijks intensief overleg plaats met de werknemers in de organisatie die zich bezighouden met de dagelijkse compliancepraktijk en input leveren voor de CR. Dit overleg wordt volgens een vast stramien gevoerd en het behandelt de belangrijkste onderwerpen van de CR. Hiermee worden twee doelen

gediend. In de eerste plaats blijft de centrale compliancefunctie goed op de hoogte van de ontwikkelingen in de organisatie, en in de tweede plaats kunnen tussentijds medewerkers van nadere informatie en – indien gewenst – ondersteuning worden voorzien. Daardoor kan in het volgende kwartaal een betere rapportage worden opgeleverd. Er is dus als het ware sprake van een leercirkel.

De Praktijk

De structuur bevat een aantal instrumenten te weten het Compliance framework, het Compliance Charter, het Compliance Program, de Code of Conduct, de Wet- en regelgevingmonitor en de Compliance Rapportage. Om deze structuur te laten werken is het noodzakelijk dat ook de 'zachte' elementen goed zijn ontwikkeld. Toepassing van de structuur is mensenwerk. De instrumenten worden immers bediend door mensen. Om die mensen te helpen dat goed te doen is – zoals uit het voorgaande moge blijken – dat instrumentarium heel concreet gemaakt: er wordt nauwkeurig aangegeven wat wordt verwacht van de input; daarbij wordt weinig ruimte geboden. In die zin ligt er dus een zwaar accent op een rule-based benadering. Zelfs waar het betreft de monitoring van een zacht element als integriteit, is getracht dat zo concreet mogelijk te maken door elke afdeling te laten rapporteren over voor die afdeling vooraf vastgestelde integriteitrisico's. Hoewel de instrumenten rule-based zijn ingericht zijn ze in hun werking dynamisch; daardoor is de structuur in staat om de komende wijzigingen te volgen en direct door te voeren. Naast de wijze van opzet van de structuur, wordt – zoals in het voorgaande aangegeven – in de perioden tussen de rapportages stelselmatig gecommuniceerd met de medewerkers belast met compliance. Tenslotte worden ontwikkeling en awareness met betrekking tot de zachte elementen gestimuleerd door periodieke integriteittrainingen voor alle managementlagen.

Het ontwikkelde bouwwerk lijkt nogal 'zwaar'; toch valt dat in de praktijk erg mee. De rapportage is weliswaar uitgebreid, maar een afdeling hoeft slechts in te vullen wat voor haar van belang is. Samengesteld ontstaat dan een volledig beeld van alle aspecten over de gehele organisatie heen. De kracht van het samenhangende instrumentarium is met name dat het aantonen van de werking van het compliance framework er zeer goed door wordt ondersteund. Door deze evidence based methoden kan effectief en resultaat gericht compliance in de organisatie worden gevolgd en zo nodig worden bijgestuurd.

Aanbevelingen

- Stel het compliance- en integriteitbeleid in een organisatie centraal vast.
- Geef de implementatie van het compliance en integriteitbeleid vorm door middel van een samenspel van instrumenten waarvan de inhoud zo concreet mogelijk is.
- Het aldus ontstane framework heeft meer kenmerken van een rule based dan van een principle based benadering.
- Geef ook de zachte elementen zoals integriteit een plaats in het bouwwerk en probeer de monitoring en rapportage daarover zo analytisch mogelijk te doen plaatsvinden.
- Zorg ervoor dat de model compliance rapportage een concrete leidraad is voor degenen die hem moeten invullen. Het format mag geen ruimte bieden voor vage statements; het moet dwingen tot concrete rapportage.
- Houd centraal te allen tijde de vinger aan de pols, corrigeer, creëer een leercirkel!