Compliance Risk Management

Interview met Laurent Claassen

R.J.H Stappers CCP EMoC[1]

In 2005 heeft Laurent in het Tijdschrift voor Compliance nr. 6[2] **een artikel geschreven over Compliance Risk Management (CRM). Destijds was dit artikel een eerste handreiking over dit onderwerp en hoewel het artikel vooral gaat over de Compliance Risk Assessment (CRA) lijkt het nog altijd relevant. Reden genoeg om Laurent uit te nodigen om te reflecteren op dit artikel en in te gaan op de nodige ontwikkelingen in de tussenliggende periode van bijna vijftien jaar compliance-ervaring.**

"Het was erg leuk om dit artikel weer eens te lezen. Zoveel lijkt er ook weer niet veranderd in de loop van de jaren en de inhoud is nog steeds actueel" vindt Laurent.

Waarom heb je dit artikel destijds geschreven? Ik adviseerde destijds financiële instellingen over het onderwerp Operational Risk Management (ORM) en merkte dat er nog nauwelijks iets over CRM was geschreven. Veel partijen worstelden met het definiëren en het beheersen van compliancerisico's. Ik zag dat CRM wat betreft aanpak en methodiek niet zo heel ver weg stond van ORM. Veel maatregelen voor het mitigeren van operationele risico's dekten ook compliancerisico's af. Risicoterminologie specifiek voor CRM is pas later gekomen. Dat was er toen nog niet.

Het artikel was bedoeld als een eerste handreiking om de compliancerisico's te identificeren en te wegen met het CRA als uitgangspunt. Dit artikel heeft in 2005 behoorlijk wat werk opgeleverd, omdat ik bij veel instellingen werd uitgenodigd om de beschreven CRM-methodiek nader toe te lichten en te helpen de CRA voor te bereiden en uit te voeren.

1 Raimond Stappers is sinds 2016 senior compliance consultant, bij de Nederlands Compliance Instituut. Hij was daarvoor zelfstandige en heeft in die hoedanigheid verschillende projecten uitgevoerd bij diverse type ondernemingen. Laurent Claassen is zelfstandig adviseur op het gebied van Regulatory Compliance, Trade & Export Control Compliance en Financial (Economic) Crime.

2 L. Claassen, Compliance Risk Management, *Tijdschrift voor Compliance*, nr.6, 2005.

Hoe heeft CRM zich sinds de publicatie van jouw artikel ontwikkeld? Het vakgebied CRM heeft zich enorm ontwikkeld in de loop van de jaren. In het begin zag je vaak een juridische benadering, waarbij iedere wet en de daarbij behorende wettelijke vereisten zelfstandig werden geanalyseerd en de risico's van niet-naleving in detail in kaart werden gebracht. Hierbij werd voor iedere wet, ieder artikel uit de wet of lid daaruit een interne norm geformuleerd. Dit was een omslachtig en tijdrovend proces. Het is in de afgelopen jaren (gelukkig) geëvolueerd naar een holistische, thematische en op risico gebaseerde benadering. Hierbij komen normen uit verschillende wettelijke bronnen samen tot een thema, zoals bijvoorbeeld 'Ken Uw Klant' of 'Insider trading'. Door te kiezen voor de thematische benadering hoeft niet iedere keer het hele interne CRM-raamwerk op de schop als er iets wijzigt in wetgeving, maar is slechts aanpassing nodig op niveau van het specifiek thema dat geraakt wordt.

Voorheen, in 2005, waren er vereisten vanuit de Wet toezicht effectenverkeer (Wte) en de Wet toezicht op het kredietwezen (Wtk). Deze vereisten waren 'verstopt' in Nadere Regelingen of Handboeken (zoals de Regeling Organisatie & Beheersing). De financiële industrie had destijds echter geen goed idee hoe zij om moest gaan met compliance-risico's en het inschatten van de gevolgen van niet-naleving van regelgeving.

Om de risicoanalyse op een objectieve wijze uit te kunnen voeren en de risico's onderling te kunnen wegen tijdens een CRA, begonnen veel financiële instellingen met het definiëren van parameters voor impact en *likelihood*, bedoeld als uitgangspunt voor het inschatten van het compliancerisico. Een eenmalige risk assessment had weinig toegevoegde waarde zo bleek in de praktijk. Het gaat om de beweging van risico's in de tijd, het proces van beheersing van de geconstateerde risico's, en niet zo zeer om het plotten van risico's in een spreadsheet of op een *heat map* op enig moment. Toezichthouders zijn later gekomen met gestandaardiseerde methodieken om risicoanalyses uit te voeren. Het is goed dat dat er is gekomen, omdat de financiële instellingen parameters gebruikten die ver uit elkaar lagen. Onderling benchmarken was toen nog niet mogelijk.

Je ziet dat CRM een vlucht heeft genomen binnen financiële instellingen sinds 2005. Nog niet alle instellingen in de financiële sector zitten op hetzelfde niveau, maar als je dit vergelijkt met andere sectoren dan zie je zeker een hogere mate van volwassenheid.

In de afgelopen jaren heb ik rondgelopen in het bedrijfsleven en gezien hoe daar naar compliancerisico's gekeken wordt. Compliance wordt daar heel anders gepercipieerd. De functie compliance officer bestaat niet of wordt anders genoemd. Daarnaast zie je dat de taken of rollen die binnen de financiële industrie zijn ondergebracht bij de compliance officer vaak zijn verdeeld over verschillende functies en afdelingen. Dit maakt het moeilijk om een goed totaaloverzicht te krijgen van de interne beheersing van compliancerisico's. Het

Door te kiezen voor de thematische benadering hoeft niet iedere keer het hele interne CRM-raamwerk op de schop als er iets wijzigt in wetgeving.

is niet zo zwart-wit georganiseerd. Dit maakt dat compliance in het bedrijfsleven sterk incident- en topic-gedreven is, en veelal nog reactief in plaats van proactief.

In het bedrijfsleven wordt nog steeds weinig noodzaak gevoeld om de compliancefunctie sterker in te richten en de meest bedreigende compliancerisico's in kaart te brengen en proactief te managen. Veel bedrijven die met name internationaal opereren lopen daarom ongekende compliancerisico's. Voor familiebedrijven geldt dit nog meer, omdat zij in de praktijk voor de interne risicobeheersing ook nog eens volledig vertrouwen op de familieband en 'ogen en oren' in de organisatie. Men realiseert zich niet dat bijvoorbeeld bouten en moeren uit een vorkheftruck misschien ook gebruikt kunnen worden in een Russische straaljager, omdat zij bepaalde G-krachten kunnen weerstaan. Dergelijke producten kunnen dus voor andere doeleinden gebruikt worden dan waarvoor zij worden gemaakt en verkocht, zogenoemde 'dual-use' producten. De toezichthoudende autoriteiten, zeker de Amerikaanse, gaan er vanuit dat een verkoper hiervan op de hoogte is en de internationale regelgevende kaders kent. Dit is niet altijd het geval, terwijl de boetes van niet-naleving van dergelijke regelgeving gigantisch kunnen zijn.

Een andere belangrijke ontwikkeling is onder meer dat de compliancefunctie tegenwoordig veel meer samenwerkt met andere risicomanagementafdelingen dan in 2005 het geval was. In het verleden zag je dat instellingen achteraf separaat ontwikkelde CRM- en ORM-methodieken met elkaar moesten integreren, omdat verschillende risicomanagementafdelingen verschillende raamwerken hadden ontwikkeld en uitgerold in de organisatie. Wij moesten dan van de twee raamwerken een enkel functionerend raamwerk zien te maken. Je ziet nu vaker dat compliance tijdig aansluiting zoekt bij bijvoorbeeld Risk Management en Auditafdelingen en de onderlinge expertise wordt uitgewisseld. Risicoparameters binnen de risicofuncties moeten *aligned* worden. Hoewel

compliancerisico ook een niet-financieel risico is, is wel sprake van een andere dimensie omdat er specifieke wetgeving is die voorschrijft wat er gebeuren moet. Dit heb je niet bij operationele risico's.

Als je de minimumnormen uit de wetgeving niet in je compliancerisico's tot uitdrukking laat komen, dan loop je het risico op een boete en zelfs reputatieschade. Voor de melding van ongebruikelijke transacties bijvoorbeeld bestaan wettelijke grenzen die moeten worden bewaakt. Je kunt deze grenzen niet naar eigen inzicht of vanuit een risicobenadering gaan aanpassen.

In vergelijking met 2005 zie je steeds vaker dat er onderscheid gemaakt wordt tussen financiële risico's en niet-financiële risico's. Een onderscheid in verantwoordelijkheid voor deze risicogebieden op het niveau van CFO en CRO kan voor de integere bedrijfsvoering echt een verschil zijn. Compliancerapportage loopt steeds vaker via de CRO en niet via de CFO.

De definiëring van compliance risk appetite blijkt lastig in de praktijk. Hoe moet hiermee worden omgegaan? Bij de introductie van CRM wilden de bestuurders van financiële instellingen nog wel eens opleggen dat de organisatie geen enkel risico accepteerde als het gaat om compliance-onderwerpen, zogenoemd *zero tolerance*. Maar nul-risico is onmogelijk als risk appetite, omdat er dan zo veel beheersingsmaatregelen moeten worden geïmplementeerd dat je feitelijk als organisatie geen geld meer kan verdienen. Het is niet realistisch. Ondernemen is en blijft risico's nemen. Het opleggen van nul-risico is meer een respons op een risico dat zich heeft voorgedaan, dan een vooraf gedefinieerd risk appetite.

In het bedrijfsleven wordt nog steeds weinig noodzaak gevoeld om de compliance-functie sterker in te richten.

Dit neemt niet weg dat er altijd topics zijn waar zero tolerance wel tot keiharde normen leidt en de consequenties van niet-naleving van deze normen voor iedereen duidelijk moeten zijn. Als een insider van de instelling bijvoorbeeld handelt in aandelen met voorwetenschap – met kennis verkregen uit transacties van een klant – en deze insider op de hoogte is van de potentiële consequenties, dan is er sprake van zero tolerance en moet je afscheid nemen van de betreffende persoon. Je *license to operate* als instelling is dan in gevaar. Ik denk dat financiële instellingen dergelijke dossiers niet altijd even hard durven aan te pakken, afhankelijk van de positie en de functie van deze insiders binnen de organisatie.

Wat vind je van de good practice van DNB aangaande de Integrity Risk Appetite? Ik heb in de loop der jaren wel geleerd dat guidance van toezichthouders er niet voor niets komt. De industrie had zich ook kunnen organiseren om iets vergelijkbaars te ontwikkelen. Compliance zou geen competitief onderwerp moeten zijn, maar dient het belang en de betrouwbaarheid van de hele industrie. Als je het zelf niet goed doet, dan komen uiteindelijk de toezichthouders met aanvullende maatregelen of guidance. Zo werkt het spel gewoon.

Het is goed dat er guidance van DNB is gekomen. Sommige instellingen hebben dat gewoon nodig. Wat je ook inhoudelijk van de guidance vindt, hij is er en schept een stuk duidelijkheid. In de praktijk blijkt het overigens altijd weer lastig om dit naar de *day-to-day* processen door te vertalen en in de dagelijkse besluitvorming te verankeren.

Je spreekt in jouw artikel van 2005 over het ontbreken van een vastleggingstool. Je was destijds van mening dat hier geen specifieke software voor bestond. Is hier de afgelopen jaren iets in gewijzigd? In de tijd van dit artikel was er eigenlijk maar één partij die een vastleggingstool aanbood om processen en specifiek compliancerisico's in beeld te brengen, als ik het me goed herinner. Inmiddels zijn er genoeg tools. Dat kan geen argument meer zijn om processen niet volledig vast te leggen, inclusief het vastleggen van (compliance)risicobeheersingsmaatregelen en de effectiviteitmeting daarvan. Bedrijven die nog steeds met spreadsheets werken lopen achter. Tools helpen de organisatie bij het bewaken van inzicht in de risico's en geven overzicht van de uit te voeren activiteiten om deze risico's binnen de vooraf gedefinieerde grenzen te beheersen. Je raakt het overzicht met de gedefinieerde activiteiten als uitvloeisel van de CRA snel kwijt. Het belangrijkste is dat je volledigheid van de risicobeheersing borgt en de juiste prioritering aanbrengt. Dit kan door alle risicothema's en beheersmaatregelen goed te wegen en hierbij de taken en verantwoordelijkheden goed vast te leggen en te managen met behulp van de vastleggingstool. Dat is zelfs belangrijker dan de keuze voor de 'perfecte' tool. Het gaat erom dat duidelijk

wordt welke mensen verantwoordelijk zijn voor opvolging van de gedefinieerde activiteiten, zodat zij ook verantwoordelijkheid nemen in de dagelijkse uitvoering van hun werkzaamheden.

Het ontduiken van verantwoordelijkheden is niet meer mogelijk met tooling. Zo maak je als organisatie zichtbaar dat je ook echt met compliance bezig bent. Je kan het vertellen aan de toezichthouder, maar met juiste vastleggingstool ook daadwerkelijk laten zien volgens het concept *'show me-prove me'*. Met de invoering van tooling zijn meer mensen bewust betrokken bij de interne risicobeheersing. De betrokkenheid van meerdere medewerkers en afdelingen zorgt ook voor het verhogen van het risicobewustzijn. Dit is een mooie bijvangst.

Wat zijn de belangrijkste stappen om te doorlopen in het CRA-proces? Wat is een praktische benadering om deze effectief te doorlopen? Het artikel is wat betreft de beschreven stappen nog best wel actueel. Het heeft geen zin om deze stappen te herhalen. Ik vind een goede voorbereiding nog altijd erg belangrijk. Dit duurt vaak langer dan de assessment zelf en de uitwerking daarvan. Een goede voorbereiding kan weken of zelfs maanden duren. Het assessment zelf kan in een tot twee dagen worden uitgevoerd en de uitwerking duurt ook weer een paar weken, maar een goede voorbereiding bepaalt grotendeels de kwaliteit van de uitkomsten.

Tijdens de voorbereiding kijk je bijvoorbeeld naar:

- Wat is de scope van de CRA?
- Welke thema's moeten worden behandeld? Zijn alle thema's voldoende voorbereid en uitgewerkt voor een effectieve assessment?
- Is er voldoende kennis in huis om de wettelijke vereisten en de compliancerisico's die daaruit volgen goed in kaart te brengen ter voorbereiding op de risk assessment?
- Wie zitten er in de sessie? Hebben deze mensen voldoende kennis en een goed beeld van de dagelijkse processen? Zitten er te dominante mensen in de sessie, die te veel sturen richting een gewenste uitkomst?

Deze factoren zijn belangrijk voor het verdere proces van de CRA en verdienen daarom aandacht. De tijdsinvestering is het grootst bij een eerste sessie. Een tweede uitvoering van een CRA kan een stuk minder tijd in beslag nemen, omdat je niet meer vanaf nul hoeft te beginnen. Helemaal als je het kader en de uitkomsten van de CRA met een vastleggingstool kunt vastleggen en onderhouden.

Tools helpen de organisatie bij het bewaken van inzicht in de risico's en geven overzicht.

Zeker als je de CRA naar thema's brengt, kan dat helpen in efficiency van het gehele proces. De tool is een middel om het proces te ondersteunen. Periodiciteit is zeer belangrijk. Hoe maak je je risk assessments vergelijkbaar over de jaren heen? Is dat mogelijk zonder standaardisatie in werkwijze? Topics veranderen nauwelijks, onderliggende regelgeving wel natuurlijk. Als je CRA's periodiek en gestandaardiseerd uitvoert, dan kunnen ook trends geïdentificeerd worden.

In het artikel stip je de uitdaging aan van het bepalen van inherent risico. Is hier in de loop der jaren iets in gewijzigd? Probeer je eens een risico voor te stellen zonder rekening te houden met het feit dat er beheersingsmaatregelen zijn. Dit vinden mensen ook nu nog steeds lastig. Een voordeel van het schatten van het inherente risico is dat het beter mogelijk is om de effectiviteit van de beheersingsmaatregelen te beoordelen. Ik zag tijdens mijn opdrachten wel eens een hoog inherent risico, waar tot wel tien beheersingsmaatregelen aan waren gekoppeld, maar het restrisico bleef hoog. De beheersingsmaatregelen dekten in dat geval de lading niet. Je kunt direct in de CRA de conclusie trekken of je wel met de juiste dingen bezig bent. Ik ben er een voorstander van om dit te blijven doen en niet direct in de CRA te komen tot de inschatting van het restrisico, waarbij wel rekening wordt gehouden met de geformuleerde en geïmplementeerde beheersingsmaatregelen.

Je gaat je bij het schatten van het inherente risico ook afvragen: 'Speelt dit risico überhaupt bij ons?' Sommige compliance- en integriteitsrisico's spelen gewoon niet bij alle instellingen en kun je dus feitelijk direct afstrepen. Door het schatten van het inherente risico bij een risicoanalyse maak je inzichtelijk of een risico wel of niet relevant is. Als het eenmaal inzichtelijk is gemaakt, dan kan dit te allen tijde worden overlegd aan de toezichthouder bij een eventuele controle. De toezichthouder ziet dan dat het risico is overwogen en beoordeeld. Dit is een prima uitgangspunt voor een gesprek over het risico.

Hoe kan monitoring effectief worden ingericht? Het is 'best practice' als je monitoring direct is verbonden aan je risicoanalyse. Waar verdient monitoring prioriteit en in welke mate en met welke diepgang dient monitoring plaats te vinden? Dit wordt bepaald door de inschatting van de geconstateerde risico's tijdens de CRA. Maar het monitoren of uitvoeren van reguliere controles is echt wat anders dan bijvoorbeeld het werven van klanten of het behalen van omzettargets, en kunnen zelfs lijnrecht tegenover elkaar staan. Lijnmanagers zijn vaak commerciële mensen en die staan niet altijd bekend om hun liefde voor beheersing en het monitoren van risico's. Zij krijgen toch verantwoordelijkheid voor de interne beheersing van hun afdeling, inclusief risicobeheersing. Als je zo'n conflictsituatie ziet, dan moet je hier mensen inzetten die dit wel kunnen en willen. Als je als instelling afdelingen hebt met verstand van risicomanagement en (interne) controle dan kunnen die een goed monitoringsraamwerk opzetten, controles uitvoeren en monitoringsactiviteiten toepassen als onderdeel van de dagelijkse operationele werkzaamheden.

Het is 'best practice' als je monitoring direct is verbonden aan je risicoanalyse.

Er zijn instellingen waar het lastig is om monitoringsactiviteiten voldoende in te bedden in de dagelijkse operationele werkzaamheden. Kleine instellingen bijvoorbeeld, hebben mogelijk geen dedicated risk-management of (interne) controle-afdeling. In dergelijke situaties heb je wellicht liever een stuk vermenging in de dagelijkse operatie – in de eerste defensielijn – dan dat monitoring helemaal niet (op onafhankelijke wijze) geschiedt.

Je hebt de afgelopen jaren veel internationaal gewerkt. Hoe verhoudt de Nederlandse markt zich tot andere markten? Nederland heeft op het gebied van het vakgebied compliance een trekkende rol gehad, zeker in Europa. Heel veel regelgeving vanuit de EU over 'hoe compliance ingericht moet zijn' is een kopie van hoe Nederland het al geregeld had. Ik heb niet gezien dat als gevolg van nieuwe EU-richtlijnen over de inrichting van de functie compliance-instellingen in Nederland het roer volledig moesten omgooien.

De financiële crisis heeft ertoe bijgedragen dat alle systeembanken binnen de EU CRM wel degelijk in het oog hebben, maar voor partijen die geen systeembank zijn kan dat anders zijn. Wat betreft de kwaliteit en inrichting van de compliancefunctie en de verankering daarvan in de organisatie, kunnen de verschillen tussen de EU-landen behoorlijk groot zijn.

Welke valkuilen kan je met ons delen? Een van de grootste valkuilen die ik in de loop van de jaren heb gezien, is het 'inkopen' van compliancerisico. Wat we in de consolidatieslag die in de jaren na de financiële crisis heeft plaatsgehad hebben gezien, is dat financiële instellingen niet altijd of onvoldoende aandacht hebben gehad voor compliancerisico's, terwijl dit zo van wezenlijk belang is. Bij een fusie of een overname kun je grote risico's inkopen als je geen goede compliance due diligence[3] uitvoert. Met name banken die wilden groeien door het opkopen van klantenportefeuilles in Centraal-Europa hebben daar achteraf flinke boetes voor betaald en er lopen nog steeds onderzoeken in dit kader. Als zij toen een goede compliance due diligence hadden gedaan op de aanwezige klanten en de achterliggende geldstromen, dan hadden ze misschien een andere keuze gemaakt. Nu worden ze aangepakt door de toezichthouders.

Daarnaast kan met name bij bedrijven buiten de financiële sector het verankeren van compliance due diligence bij overnames of voorafgaand aan het doen van zaken nog veel beter. Bedrijven zijn zich niet altijd bewust van het risico dat zij lopen. Ik ken een partij die een overname wilde doen in Afrika. Tijdens de compliance due diligence bleek een voormalig leider van Hezbollah – die stond genoteerd op diverse internationale sanctielijsten – een van de aandeelhouders te zijn bij de over te nemen partij. Een groot risico waar ze

3 Over dit onderwerp schrijven ook Elmas, Rogozinski en Vis in dit Jaarboek.

op tijd achter kwamen. Hieruit blijkt maar weer eens hoe belangrijk het is om een goede compliance due diligence uit te voeren.

Zijn er nog specifieke ontwikkelingen die positief kunnen bijdragen aan CRM? Recent zie je dat een tweetal ontwikkelingen – overigens breder toe te passen dan alleen maar voor compliance – bijdragen aan het efficiënter uitvoeren van dagelijkse processen en het preventief analyseren van potentiele risico's.

Allereerst zie je dat processen waarin veel repetitieve werkzaamheden en standaard-controles zitten, steeds vaker volledig geautomatiseerd worden. Dit wordt ook wel 'Robotics' genoemd. Voordeel is dat je alleen uitzonderlijke cases of alleen de proces-handelingen met een verhoogd risico door mensen laat uitvoeren of (steekproefsgewijs) gaat toetsen. Een voorbeeld binnen compliance zou kunnen zijn het proces van pre-clearing van insider transacties. Dit zijn redelijk gestandaardiseerde processen, waarbij het normenkader en de te toetsen normen vooraf duidelijk gedefinieerd moeten zijn. Dit kun je met Robotics automatiseren. Indien het geautomatiseerde proces eventuele verzoeken van insiders als verhoogd risico ziet, dan kan het proces worden overgenomen door mensen. Er zal altijd nog door middel van een steekproef gekeken moeten worden naar transacties die volledig zijn afgewikkeld door het geautomatiseerde proces, om vast te stellen of dit tot de juiste besluitvorming heeft geleid. Ik heb zelf ook veel ervaring met pre-clearing van insider transacties en weet hoe moeilijk het is om alle normen en alle details waaraan getoetst moet worden uit je hoofd te kennen om een transactie goed te kunnen beoordelen en een goed afgewogen besluit te nemen. Mooie bijvangst van Robotics is dat je de controles in veel meer detail kunt laten uitvoeren, waardoor het risico van het foutief beoordelen van een insider-transactie veel kleiner is.

Een andere ontwikkeling is dat met behulp van *data analytics* potentiele compliance-risico's preventief en proactief kunnen worden afgevangen. Indien bijvoorbeeld een financiële instelling haar klantendossiers volledig heeft geautomatiseerd, dan kun je per type klant en risicoclassificatie de minimum dossiervereisten definiëren. Met behulp van data analytics kun je de volledigheid van de dossiers toetsen en tijdig signaleren dat dossiers niet volledig zijn en relevante (veelal ook wettelijk vereiste) dossierstukken ontbreken. In recente cases, in met name de bancaire industrie, zie je ook nu weer dat het goed bijhouden en steeds volledig hebben van klantendossiers een hekel punt is. Met behulp van data analytics kun je focussen op die dossiers die niet volledig zijn. Ook nu weer zal je steekproefsgewijs controles op de klantendossiers moeten laten uitvoeren door mensen. Een volledig dossier betekent nu niet direct een kwalitatief goed dossier dat aan de wettelijke vereisten voldoet.