Complianceprogramma's voor niet-financiële ondernemingen: overbodige luxe of bittere noodzaak?

mr. M.E.P.A.R. Jans CCP en L.P.J. van Kan-Janson*

Trefwoorden: compliance programma's, non-financials, beheerste en integere bedrijfsvoering

In de financiële sector worden complianceprogramma's gebruikt om de eisen van beheerste en integere bedrijfsvoering nader invulling te geven. Bij de non-financials zien wij de inzet van complianceprogramma's minder nadrukkelijk of uitgebreid terugkomen. Of er wordt wel met een complianceprogramma gewerkt, maar dat is dan beperkt tot voor de hand liggende onderwerpen en maatregelen, die niet of niet voldoende diepgaand worden uitgewerkt. In dit artikel bespreken we de kansen die een complianceprogramma biedt aan *non-financials*, de bedreiging die uitgaat van het ontbreken van een niet-adequaat of voldoende uitgewerkt complianceprogramma, en de elementen die de effectiviteit van een complianceprogramma voor *non-financials* beïnvloeden.

Ondernemen is risico nemen; risico's zijn onvermijdelijk

Ondernemen is risico nemen; risico's zijn onvermijdelijk. In iedere onderneming zijn omstandigheden of situaties aan te wijzen waaraan extra risico's zijn verbonden. Hoewel de beheersing van risico's van continu belang is, is het tijdig identificeren en controleren van risico's juist in die 'spannende' situaties cruciaal voor de continuïteit van de onderneming. Gaat het op een dergelijk moment mis, dan is een spreekwoordelijke explosie onvermijdelijk, en is men aangewezen op maatregelen om de schade te beperken: '*damage control*'. Hoe mooi zou het zijn als die schade kon worden voorkomen.

In de streng gereguleerde financiële sector staat in beginsel voorgeschreven op welke wijze de risico's worden geïdentificeerd, gewogen en waar mogelijk beheersbaar worden gemaakt

In de streng gereguleerde financiële sector staat in beginsel voorgeschreven op welke wijze de risico's worden geïdentificeerd, gewogen en waar mogelijk beheersbaar worden gemaakt. Daar wordt stevig op een proactieve aanpak gestuurd, en hierop wordt ook intensief toegezien door de externe toezichthouders. De wet vereist dat financiële instellingen een beheerste en integere bedrijfsvoering hanteren, en die beheersing dient ook te kunnen worden aangetoond.[1] Dit ligt echter anders voor ondernemingen buiten de financiële sector (die in dit artikel voor het gemak onder de noemer '*non-financials*' worden geschaard). Ook zij moeten als ieder ander voldoen aan de vigerende wet- en regelgeving, maar de manier waarop dat gebeurt, wordt meer vrij gelaten. Dit is tegelijkertijd een kans, maar ook een bedreiging.

Dit ligt echter anders voor ondernemingen buiten de financiële sector

1. De kans

'ABN Amro moet van DNB alle particuliere klanten doorlichten' en 'DNB geeft ABN Amro tik op vingers om falende witwascontrole', kopte het Financiële Dagblad op 7 augustus van dit jaar.[2] Financiële instellingen, waaronder banken, zijn verplicht te beschikken over gedragslijnen, procedures en maatregelen om risico's op, onder andere, witwassen en financieren van terrorisme te beperken en effectief te beheersen, krachtens art. 2 lid c sub 1 Wet ter voorkoming van witwassen en financieren van

* Marlène Jans en Loes van Kan-Janson zijn respectievelijk Director en Senior Consultant bij RSM Netherlands (GRC) Consultancy B.V. Dit artikel is op persoonlijke titel geschreven.

[1] Art. 3:10 en 3:17 Wft

[2] https://fd.nl/ondernemen/1311181/winst-abn-amro-stijgt-licht-ondanks-grote-investering-witwasonderzoek. en https://fd.nl/ondernemen/1311220/dnb-geeft-abn-amro-tik-op-vingers-om-falend-witwasbeleid.

terrorisme (Wwft). Om een betrouwbaar financieel stelsel te creëren en te behouden, ligt in de financiële sector de focus voor compliance sterk op het toezicht: het afwenden van integriteitsrisico's. Dit wordt ten uitvoering gebracht door een proactieve houding: toezicht, controle bij vergunningverlening en handhaving. Deze aandacht voor het onderwerp compliance leidt tot steeds grotere budgetten voor deze afdeling binnen financiële instellingen[3]: Zo maakte ABN Amro voor het doorlichten van zijn particuliere klanten 114 miljoen euro beschikbaar.[4]

Voor ondernemingen buiten de financiele sector, waarbij kan worden gedacht aan multinationals of ondernemingen in diverse sectoren wordt in verhouding veel minder proactief gehandhaafd. Ondernemingen worden daardoor pas met de gevolgen geconfronteerd als het kwaad al is geschied

Voor ondernemingen buiten de financiële sector, waarbij kan worden gedacht aan multinationals of ondernemingen in diverse sectoren zoals bijvoorbeeld transport & logistiek (geen kleine sector in ondernemend Nederland) , (dier-)voeding, IT of producenten van *hi-tech* apparatuur en goederen, wordt in verhouding veel minder proactief gehandhaafd. Ondernemingen worden daardoor pas met de gevolgen geconfronteerd als het kwaad al is geschied, en krijgen dan pas inzicht in de aard en omvang van de (financiele) gevolgen en reputatieschade. Een welbekend en al wat ouder voorbeeld van de gevolgen van een incompleet/falend complianceprogramma bij een non-financial, zijn de schendingen van de *International Emergency Economic Powers Act* (IEEPA) – de Amerikaanse handelsembargo's tegen Iran, Soedan en Birma – door onze eigen Fokker Services, tussen 2005 en 2010. Deze langslepende juridische affaire eindigde uiteindelijk in 2014 niet alleen in een schikking voor totaal $21 miljoen en de acceptatie van voorwaarden gesteld door de OFAC, USAO en BIS[5], maar ook in een stortvloed aan internationale publiciteit over de totaal 1150 vastgestelde overtredingen van de Amerikaanse wetgeving. Er zijn legio meer recente voorbeelden op te sommen, naar sommige voorbeelden wordt later in dit artikel verwezen.

Natuurlijk worden er ook voor *non-financials* tal van richtlijnen gegeven. Om risico's op overtredingen zoals zich die bij Fokker voordeden te ondervangen, neemt men de '*Framework for OFAC Compliance Commitments*'[6], voor de zorgsector zijn daar o.a. de 'compliance handvatten'[7] van de Nederlandse Zorgautoriteit en Berenschot, en voor de exporteur van strategische goederen en diensten publiceerde Nederland de 'Richtlijnen voor het opstellen van een Intern Compliance Programma'.[8] In sommige gevallen wordt de inhoud van zulke programma's wel degelijk beoordeeld door de autoriteiten[9], maar in de meeste gevallen dienen de richtlijnen puur om de betreffende sector te helpen hun complianceprogramma te verbeteren teneinde de risicobeheersing op het gewenste niveau te krijgen. Een stringent, contentieus extern toezicht op dit terrein bestaat niet.

Hoewel de gevolgen van non-compliance voor *financials* en *non-financials* over het algemeen identiek zijn, namelijk financiële en niet-financiële schade, hebben *non-financials* de kans om naar eigen inzicht te bepalen hoe de compliancefunctie wordt ingericht zonder daarvoor rechtstreeks onder toezicht te staan

Hoewel de gevolgen van non-compliance voor *financials* en *non-financials* over het algemeen identiek zijn, namelijk financiële en niet-financiële schade zoals bijvoorbeeld reputatieschade, hebben *non-financials* de kans om, zolang dit maar effectief gebeurt, naar eigen inzicht te bepalen hoe de compliancefunctie wordt ingericht zonder daarvoor rechtstreeks onder toezicht te staan. Zolang er geen overtredingen worden begaan, lijkt er nauwelijks sprake te zijn van financiële of bijvoorbeeld reputatieschade. Met andere woorden: de kans op zulke schade is voor *non-financials* een stuk kleiner dan voor *financials*. Dat denkt men althans.

---

[3] L.C.M. Bouchier-Morssink, 'Compliance anno 2017: kansen en bedreigingen', *Jaarboek Compliance 2018,* p.225.

[4] T. Borst, 'ABN Amro maakt op aandringen van toezichthouder 114 miljoen vrij om particuliere klanten door te lichten', *De Volkskrant,* 7 augustus 2019.

[5] Enforcement information for June 5, 2014, OFAC https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20140605_fokker.pdf.

[6] https://www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf.

[7] https://www.berenschot.nl/inspiratie/klantcases/klantcases/belangrijke-stappen-compliance/.

[8] https://www.rijksoverheid.nl/onderwerpen/exportcontrole-strategische-goederen/documenten/richtlijnen/2019/02/22/richtlijnen-opstellen-internal-compliance-programme.

[9] Zie https://www.rijksoverheid.nl/onderwerpen/exportcontrole-strategische-goederen/vraag-en-antwoord/wat-is-een-icp.

2. De bedreiging

Helaas heeft de vrijheid van aanpak voor *non-financials* ook een keerzijde. Dit begint met de interpretatie van de term compliance. Wij komen nog regelmatig ondernemingen tegen, waar compliance wordt uitgelegd als het strikt voldoen aan wet- en regelgeving. Deze interpretatie is de klassieke vertaling, die ook jarenlang in de financiële sector is gehanteerd. Totdat naar aanleiding van de financiële crisis – nu meer dan 10 jaar geleden – moest worden geconstateerd dat daarmee de risico's niet afdoende in kaart konden worden gebracht en worden beheerst. De Vereniging voor Compliance Officers (VCO) heeft in haar beroepscompetentieprofiel voor compliance officers compliance gedefinieerd als 'het versterken van de integriteit van de organisatie om daarmee bij te dragen aan duurzame waardecreatie door de organisatie'.[10] Daarmee wordt de focus verlegd van de letter van de wet naar de geest van de wet, het achterliggende doel waarom de wet ook alweer tot stand is gekomen.

Helaas heeft de vrijheid van aanpak voor *non-financials* ook een keerzijde

Er zijn talloze voorbeelden te noemen van ondernemingen die vanuit het meer traditionele gedachtengoed over compliance minder belang hechten aan een effectieve opzet en implementatie van compliance maatregelen dan bij financiële instellingen het geval is, en daardoor ook minder genegen zijn om hiervoor financiële middelen ter beschikking te stellen. Dit resulteert in minder personeel, met kans op minder intern aanwezige kennis en minder respect en rugdekking voor de compliancefunctie. Hierdoor heeft de compliancefunctie een minder sterke positie dan in de financiële sector en kan de non-*financial* slechts nog de overtredingen remediëren die zijn ontstaan; de realisatie van een proactieve aanpak om zo bij te dragen aan een beheerste en integere bedrijfsvoering en duurzame waardecreatie van de onderneming wordt daarmee een grote uitdaging.

Een voorbeeld hiervan is de identificatie van strategische goederen (i.e. militaire goederen, of goederen welke een commercieel doel hebben maar ook kunnen worden ingezet voor ontwikkeling van wapens). Exporteurs van zulke goederen zijn onderworpen aan een vergunningplicht bij o.a. export, maar het beoordelen van alle goederen in de inventaris van een bedrijf met als doel te bepalen of hier goederen tussen zitten die vergunning plichtig zijn, is geen exercitie waarop wordt gehandhaafd. De douane is vervolgens aangewezen op hun kennis van zaken, zoals bleek bij een veroordeling in 2017 waarbij de douane een doorvoerzending onderschepte van KLM welke bestemd waren voor *'Taura Air Force Base'*. De douanebeambte vond op de betreffende zending een label met o.a. de woorden 'Vliegtuig' en 'Cheetah', en wist uit ervaring dat met 'Cheetah' mogelijk een militair gevechtsvliegtuig bedoeld kon worden. Vanaf dat punt is onderzoek verricht en uiteindelijk vastgesteld dat een individuele doorvoervergunning benodigd was, die overigens ontbrak.[11]

Met een geringere aandacht voor het onderwerp compliance, benut de *non-financial* niet het voordeel wat ontstaat door de proactieve inrichting van het interne toezicht in de vorm van de compliancefunctie.

3. Extrinsieke motivatie

Daarnaast signaleren wij dat de stringente eisen die worden gesteld aan de banken en overige financiële instellingen, steeds vaker één op één worden doorvertaald in de eisen die financiële instellingen stellen aan hun cliënten. Indien de financiële instelling het complianceprogramma van de cliënt opvraagt en vervolgens constateert dat dit programma niet aan de gestelde eisen voldoet, kan dit leiden tot vervelende verrassingen voor de cliënt en zelfs tot mogelijke beëindiging van de relatie tussen de financiële instelling met die cliënt. De bank dient immers die risico's die zij loopt bij haar cliënten zo goed mogelijk in kaart te brengen en te beheersen. En zo kan ineens de huisbankier geen huisbankier meer willen zijn, met alle vervelende gevolgen van dien. Een belangrijke reden voor *non-financials* om de ontwikkelingen rond wet- en regelgeving in de financiële sector goed in de gaten houden en daar ook zoveel mogelijk op te anticiperen.

In de Verenigde Staten wordt gewerkt met een andere aanpak. Daar tracht men de *non-financial* te stimuleren om een effectief complianceprogramma in te richten door er voordelen tegenover te zetten. Het Amerikaanse *Department of Justice* publiceerde in april 2019 een nieuwe versie van het '*Guidance Document Evaluation of Corporate Compliance Programs*'.[12] Dit Amerikaanse departement, onderdeel van het kabinet onder de *U.S. Government Executive Branch*, is de instantie die het handhaven van de wetten en het verdedigen van de belangen van de Verenigde Staten als hoofdmissie heeft. In de vernieuwde publicatie wordt duidelijk gemaakt dat het complianceprogramma wordt gezien als een factor die voordelen kan opleveren voor het bedrijf, bijvoorbeeld bij het bepalen van de hoogte van een straf bij een overtreding. In hoofdstuk acht van de

[10] https://www.vco.nl/vereniging/over-de-vco/beroepscompetentieprofiel. Daaraan wordt toegevoegd dat 'een integere organisatie onder meer vereist een integer bestuur en medewerkers, transparante en verantwoorde producten, diensten en afzetkanalen, maar ook integere klanten en andere belanghebbenden zoals leveranciers. Daarnaast is de interne organisatie en de besturing daarvan (ook wel interne governance) zodanig ingericht dat openheid en tegenspraak worden gestimuleerd, de besluitvorming evenwichtig plaatsvindt en dat adequate '*checks and balances*' aanwezig zijn.'

[11] Rechtbank Noord-Holland, zaaknummer 15/994178-17.

[12] https://www.justice.gov/criminal-fraud/page/file/937501/download.

US Federal Sentencing Guidelines[13] wordt gesteld dat er bij overtredingen twee factoren zijn die de uiteindelijke straf van een organisatie kunnen verminderen, te weten de aanwezigheid van een effectief compliance- en ethiek programma, en de *self-reporting*, medewerking of acceptatie van verantwoordelijkheid voor de overtreding.
Zowel de Europese Unie als Nederland hebben er tot dusver niet voor gekozen om de *non-financial* dergelijke voordelen in het vooruitzicht te stellen. Sterker nog, de Autoriteit Commerciële Markten (ACM) heeft zelfs enige tijd geleden een boete aan KPN wegens een overtreding bij aanbestedingsprocedures verhoogd vanwege een niet-functionerend compliance-programma.[14] Er wordt dus niet alleen verwacht dat een compliance-programma wordt ingericht, maar ook dat dit goed functioneert. Is dit een mogelijke overweging om maar helemaal geen compliance-programma te voeren?

'Trust takes years to build, seconds to destroy and forever to repair'

4. Nut van het compliance-programma

'Trust takes years to build, seconds to destroy and forever to repair.'

Voor zowel financiële instellingen alsook voor *non-financials* is het van belang dat men zich realiseert dat drastische ontwikkelingen gaande zijn op verschillende terreinen met een wereldwijde impact, waaronder *cybercrime*, artificiële intelligentie, *block-chain* en geopolitieke ontwikkelingen. Een compliance-programma heeft niet tot doel om boetes te voorkomen, maar om structureel niet-financiële risico's te beheersen, en een bijdrage te leveren aan een beheerste en integere bedrijfsvoering, om daarmee een robuuste basis te bieden voor een duurzame ontwikkeling van de onderneming. Dit omvat ook het communiceren van de eigen normen en waarden richting de eigen organisatie, richting leveranciers, klanten en andere relevante ondernemingen. Een goede inrichting van de compliance binnen de organisatie, en een effectieve implementatie van en communicatie over het compliance-programma, zorgt voor vertrouwen bij derde partijen, en draagt zo bij aan een duurzame waardecreatie voor de onderneming.

Een compliance-programma kent voor veel *non-financials* geen strikt wettelijke noodzaak, en we kunnen daarmee ook concluderen dat ook aan de vorm inhoud van het compliance-programma geen vaste eisen worden gesteld. *Non-financials* doen er goed aan om deze kans te grijpen en juist die inhoud van het compliance-programma te kiezen die aansluit bij de risicobereidheid van de onderneming, bij de risicofactoren die van toepassing zijn op de industrie waarin de onderneming zich beweegt, en bij de inrichting

Een compliance-programma kent voor veel *non-financials* geen strikt wettelijke noodzaak, en we kunnen daarmee ook concluderen dat ook aan de vorm inhoud van het compliance-programma geen vaste eisen worden gesteld

van de organisatie. Op deze manier wordt de onderneming niet met een papieren tijger opgescheept.

Het belang van een effectieve implementatie van het compliance-programma staat vervolgens buiten kijf. Over de effectiviteit van compliance-programma's zijn veel artikelen verschenen in jaargang 19 van het *Tijdschrift voor Compliance*, daarom richten wij ons in dit artikel op de onderdelen van een compliance-programma die over het algemeen vaak wat minder goed over het voetlicht komen.

5. Onderdelen van het compliance-programma voor non-financials

In paragraaf 3 werd al gesproken over de voorzet van de *US Federal Sentencing Guidelines* om te komen tot een effectief compliance- en ethiekprogramma. Welke handvatten worden hiervoor gegeven?

[13] https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2018/GLMFull.pdf, blz. 517 e.v.
[14] Uitspraak 24-10-2013 zaaknummer AWB-12_03579.

Voor een effectief compliance en ethisch programma wordt verwacht dat:
- de nodige zorgvuldigheid aan de dag wordt gelegd om non-compliant ('crimineel') gedrag te voorkomen en op te sporen; en
- anderszins een organisatiecultuur wordt bevorderd die ethisch gedrag en een *commitment* tot naleving van de wet aanmoedigt.

Een dergelijk programma op het gebied van naleving en ethiek moet op een redelijke wijze worden ontworpen, uitgevoerd en gehandhaafd, zodat het programma over het algemeen effectief is in het voorkomen en opsporen van non-compliant gedrag.

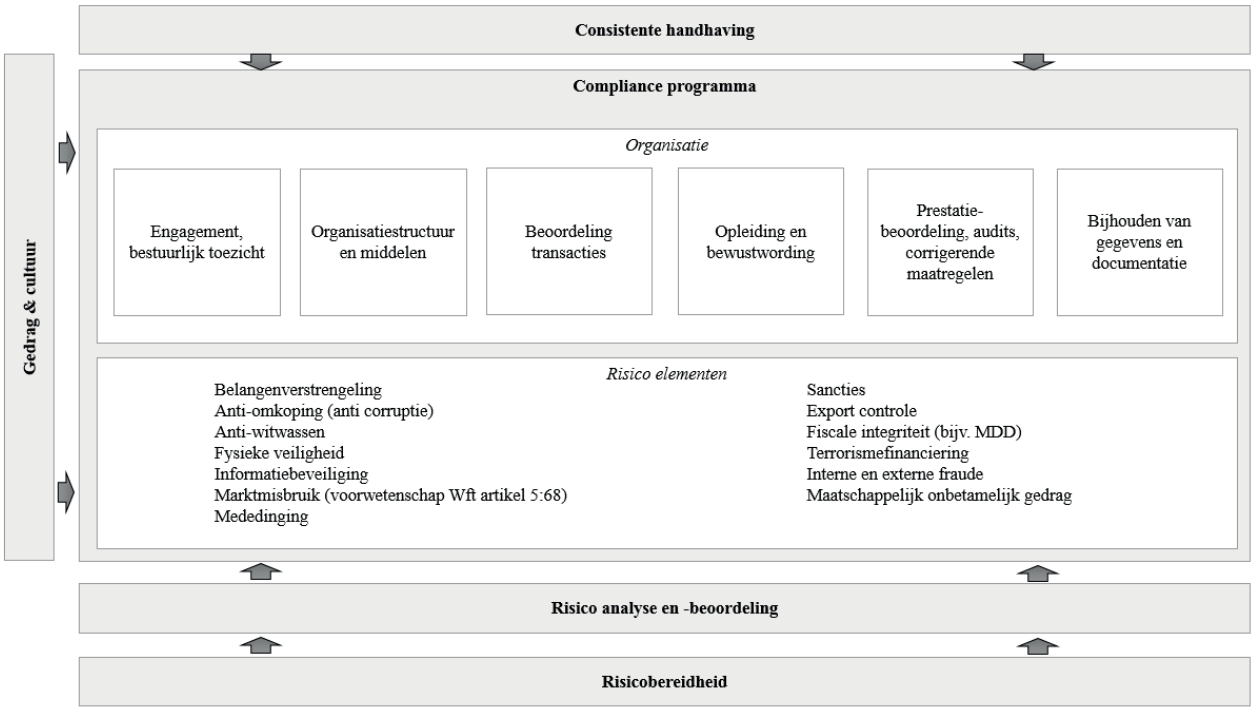
De nodige zorgvuldigheid en de bevordering van een organisatiecultuur die ethisch gedrag en een verbintenis tot naleving van de wet als hierboven vermeld vereisen minimaal het volgende:
1. De organisatie dient normen en procedures vast te stellen om crimineel gedrag te voorkomen en op te sporen.
2. Taken en verantwoordelijkheid van (senior) management:
   a. De directie van de organisatie moet goed op de hoogte zijn van de inhoud en de werking van het compliance- en ethiekprogram en moet een redelijk toezicht uitoefenen op de uitvoering en effectiviteit van het programma voor naleving en ethiek.
   b. Het senior management van de organisatie dient ervoor te zorgen dat de organisatie een effectief compliance- en ethiekprogramma heeft, zoals beschreven in deze richtlijn. Specifieke personen binnen het senior management moeten de algemene verantwoordelijkheid voor het compliance- en ethiekprogramma krijgen toegewezen.
   c. Aan een of meer specifieke personen binnen de organisatie wordt de dagelijkse operationele verantwoordelijkheid voor het programma op het gebied van compliance en ethiek gedelegeerd. De persoon of personen met operationele verantwoordelijkheid moeten periodiek verslag uitbrengen aan het senior management en, in voorkomend geval, aan de directie c.q. raad van bestuur, over de doeltreffendheid van het compliance- en ethiekprogramma. Om deze operationele verantwoordelijkheid uit te voeren, worden voldoende middelen en passende tools ter beschikking gesteld, en krijgen zij rechtstreeks toegang tot het directieniveau.
3. De organisatie dient redelijke inspanningen te leveren om binnen het senior management van de organisatie geen personeel op te nemen waarvan de organisatie weet of had moeten weten, dat zij zich schuldig hebben gemaakt aan illegale activiteiten of ander gedrag dat niet strookt met een effectief compliance- en ethiekprogramma.
4. Communicatie: De organisatie dient redelijke stappen te ondernemen om haar normen en procedures en andere aspecten van het compliance- en ethiekprogramma, op een praktische wijze te communiceren met de leden van de raad van bestuur, senior management en andere kaderleden, de werknemers van de organisatie en, in voorkomend geval, met de vertegenwoordigers van de organisatie. Dit gebeurt door het uitvoeren van doeltreffende opleidingsprogramma's en het op andere wijze verspreiden van informatie die geschikt is voor de respectievelijke taken en verantwoordelijkheden van deze personen.
5. De organisatie dient redelijke maatregelen te nemen:
   a. om ervoor te zorgen dat het compliance- en ethiekprogramma van de organisatie wordt gevolgd, met inbegrip van controle en audits om non-compliant gedrag op te sporen;
   b. om periodiek de effectiviteit van het compliance- en ethiekprogramma van de organisatie te evalueren; en
   c. door een klokkenluidersregeling op te stellen en implementeren, met de nodige waarborgen rond vertrouwelijkheid omgeven, die het mogelijk maakt om werknemers en agenten van de organisatie potentiële of werkelijke non-compliant gedragingen te laten melden, of om advies te vragen zonder angst voor represailles.
6. Het compliance- en ethiekprogramma dient in de gehele organisatie consequent te worden ondersteund en gehandhaafd door middel van 1) passende stimulerende maatregelen om te presteren in overeenstemming met het compliance- en ethiekprogramma; en 2) passende disciplinaire maatregelen voor het plegen van non-compliant gedrag en voor het niet nemen van redelijke maatregelen om non-compliant gedrag te voorkomen of op te sporen.
7. Nadat non-compliant gedrag is ontdekt, dient de organisatie redelijke maatregelen te nemen om adequaat te reageren op het gedrag en om verder soortgelijk crimineel gedrag te voorkomen, met inbegrip van het aanbrengen van de nodige wijzigingen in het compliance- en ethiekprogramma van de organisatie.

Tot slot wordt verwacht dat de organisatie periodiek het risico van non-compliant gedrag evalueert en dat zij passende maatregelen neemt om het programma aan te passen en te verbeteren op basis van de geconstateerde bevindingen. Ook wordt aandacht besteed aan de gewenste proportionaliteit van het programma: het programma dient in lijn te zijn met 1) gebruikelijke industrie- en overheidsstandaarden, 2) de omvang van de organisatie en 3) vergelijkbaar wangedrag.

Het is afhankelijk van de aard, omvang en het specifieke karakter van de *non-financial* welke risicogebieden in het complianceprogramma moeten worden behandeld, en hoe ver een complianceprogramma op die risicogebieden dient te worden gespecificeerd. Echter maakt een aantal onderdelen standaard deel uit van het programma. Ook is het uitgangspunt van het programma voor alle *non-financials* uiteindelijk hetzelfde; voorkomen dat men onbewust en onbedoeld in de problemen komt.

Het ontwerp wordt allereerst gebaseerd op de risicobereidheid van de onderneming, dit is allesbepalend voor de uiteindelijke samenstelling en inhoud van het compliance programma. Aangezien een effectief complianceprogramma in eerste instantie wordt gedragen door de directie, bepaalt en formuleert deze ook de risicobereidheid als onderdeel van het strategische beleid. Meer risico betekent over het algemeen meer (commerciële) kansen, maar ook een hogere mate van benodigde controlemaatregelen. Vergelijk dit bijvoorbeeld met een auto: als je harder wilt kunnen rijden, heb je ook betere remmen nodig. Op basis hiervan wordt een risicoanalyse gemaakt. Hierbij is het van belang om met een *helikopter view* naar de organisatie te kijken, risico's kunnen niet worden geïsoleerd tot één afdeling, er zijn altijd ook andere afdelingen of teams bij betrokken. Wanneer het duidelijk is met welk doel het complianceprogramma wordt opgezet en welke risico's dienen te worden afgedekt, worden de elementen uit de risico analyse bepalend voor het raamwerk van het complianceprogramma. Een effectief complianceprogramma is dus ook voor *non-financials* volledig maatwerk.

Hieronder een schematische weergave van een complianceprogramma.



6. Standaard: de organisatie

Deze elementen worden in een complianceprogramma standaard opgenomen:

a. Engagement (bestuurlijk toezicht, compliance vanuit het management[15]); onder wiens leiding komt dit programma tot stand;
b. Organisatiestructuur, verantwoordelijkheden en middelen: hoe is de structuur van *3 lines of defense* ingericht;
c. Screenen van transacties, risicobeoordeling;
d. Opleiding en bewustwording;
e. Prestatiebeoordeling, audits, verslaglegging en corrigerende maatregelen (inclusief anonieme rapportage); en
f. Bijhouden van gegevens en documentatie.

7. Ter overweging: een aantal risico-elementen uitgewerkt

De noodzaak tot maatwerk komt vooral tot uiting in de uitwerking van de risico-elementen. Een toelichting op alle elementen gaat verder dan hier in dit artikel gewenst is; bovendien is een aantal elementen redelijk tot goed bekend. Wij lichten een paar specifieke elementen uit en gaan daar wat dieper op in.

a. Belangenverstrengeling

Belangenverstrengeling dient te worden voorkomen door het zich terugtrekken uit discussies omtrent, stemmingen over, of deelnemen aan beslisprocessen

[15] https://www.transparency.nl/nieuws/2018/08/tien-onmisbare-elementen-effectief-compliance-programma/.

of -activiteiten waar een belangenverstrengeling kan ontstaan.[16] Wanneer belangenverstrengeling voor de organisatie een verhoogd risico vormt, bijvoorbeeld wanneer voormalige overheidsfunctionarissen in dienst zijn bij de organisatie waarbij de eerdere functie rechtstreeks verband hield met de huidige functie, wordt aangeraden om in het complianceprogramma op te nemen hoe men ermee om dient te gaan. De focus ligt hierbij niet direct op het voorkomen, maar op het stimuleren tot mitigeren van het risico dat het kan ontstaan, op het herkennen van een situatie van belangenverstrengeling en op het melden ervan. In ieder geval wordt een statement opgenomen in het complianceprogramma dat belangenverstrengeling in geen van de lagen van de organisatie wordt gedoogd.

Om een situatie van (mogelijke) belangenverstrengeling te kunnen herkennen of te zien ontstaan, is het allereerst van belang dat de betrokken personen goed in kaart zijn gebracht, met hun (zakelijke en persoonlijk) relaties, netwerken, sportclubs, etc. Dat geldt dus eventueel ook voor die van de partner van de medewerker. Het stimuleren van open gesprekken over de risico's rond belangenverstrengeling is een essentieel instrument hiervoor, zodat het algemene bewustzijnsniveau op een hoog niveau wordt gebracht.

b. Anti-omkoping (anti-corruptie)
Een element over anti-corruptie ondersteunt de vertaling van de waardes van de onderneming op dit gebied in praktijkgerichte maatregelen.[17] Zoals bij belangenverstrengeling wordt ook hier vanuit het management duidelijk gemaakt dat corruptie en omkoping niet wordt gedoogd. Corruptie hoeft niet direct in de eigen organisatie plaats te vinden, maar kan ook elders in de *supply chain* voorkomen; een relevante overweging om op te anticiperen in het eigen complianceprogramma. Omkoping is voor multinationals een onderwerp van constante zorg; het kan ook de besten overkomen, zoals we (redelijk) recent hebben gezien bij Philips, SHV en Damen Shipyards.[18]

c. Informatiebeveiliging
Voor het gemak wordt hier ook cybersecurity onder geschaard. Ook hier kan veel dieper op worden ingegaan. Een belangrijk element welke wij onder de aandacht willen brengen, is het risico van CEO-fraude en de steeds geavanceerdere wijze waarop dit plaatsvindt. Waar eerder nog medewerkers zogenaamd van hun CEO of CFO per mail de opdracht kregen om bedragen over te maken aan bepaalde externe partijen, wordt hiervoor inmiddels ook software ingezet die de stem van de betreffende leidinggevende kan nabootsen.[19]

d. Third party due diligence; screening van bijv. toeleveranciers
Als de toeleveranciers of andere partijen in het netwerk van een organisatie niet goed of diepgaand genoeg in kaart worden gebracht, is de potentiële schade soms niet goed te overzien. Allereerst is een inventarisatie nodig van de integriteit van de betreffende partij. Onderschat echter ook de risico's niet waar diegene mee te maken heeft. Dat kan variëren van risico's die worden gelopen door hun toeleveranciers, maar b.v. ook risico's die voortvloeien uit (mogelijk nog) onverwachte hoek, zoals risico's gerelateerd aan klimaatverandering, zoals de toename van verdroging, verandering van oogstopbrengsten en energielasten, toename van risico's uit stormen en natuurbranden, etc. Maar je kunt je ook afvragen of de toeleverancier alle elementen van de Algemene Verordening Gegevensbescherming (hierna: AVG) goed in kaart heeft gebracht, of mogelijk kwetsbaarheden kent m.b.t. de IT-systemen (cyberrisico's). Onze blik op risico's zal de komende periode ingrijpend moeten veranderen, willen wij goed zijn voorbereid. Een diepgaander onderzoek naar risico's lijkt daarmee onvermijdelijk.

e. Handelen in strijd met handelssancties
Het voldoen aan sanctieprogramma's is veel meer dan het vermijden van de '*usual suspects*' Noord-Korea, Soedan en Iran. Op ondernemingen in Nederland zijn de sanctieprogramma's van Nederland, de Europese Unie, de Verenigde Naties en in sommige gevallen ook die van de Verenigde Staten van toepassing. Naast transacties met klanten dienen ook leveranciers, partners en medewerkers te worden gescreend.
Er zijn gevallen waarin het voldoen aan een sanctiewetgeving in strijd is met andere wetgeving. Een voorbeeld hiervan is de Amerikaanse wetgeving die in sommige gevallen van de werkgever eist om niet alleen de huidige nationaliteit, maar ook vroegere nationaliteiten van werknemers vast te stellen. De AVG erkent de Amerikaanse wetgeving niet, waardoor het vastleggen van deze gegevens niet ter zake doet, en daarom niet is toegestaan. Het complianceprogramma dient in zo'n geval te omschrijven hoe de organisatie met dergelijke situaties omgaat.
Recente voorbeelden waar het mis ging op het gebied van sanctiewetgeving zijn bijvoorbeeld DAF Trucks en

---

[16] International Chamber of Commerce, *Guidelines on Conflicts of Interest in Enterprises*, oktober 2018, https://www.iccmex.mx/uploads/ICC%20Conflicts%20of%20Interest%20Guidelines%20Final%20July%202018.pdf.

[17] H. Nieuwlands, '*Auditing Anti Bribery Programs*', mei 2018, zie https://www.iia.nl/kenniscentrum/vaktechnische-publicaties/publicatie/auditing-anti-bribery-programs.

[18] Voorbeelden zijn Philips https://fd.nl/ondernemen/1301569/fbi-onderzoekt-volgens-reuters-rol-van-philips-in-braziliaanse-steekpenningen-affaire of https://fd.nl/ondernemen/1313350/philips-was-gewaarschuwd-over-fraude), SHV https://www.nrc.nl/nieuws/2017/02/24/begraven-onder-een-dikke-laag-zand-6975941-a1547650 of Damen Shipyards https://www.nrc.nl/nieuws/2018/10/20/corruptie-onderzoek-verkopers-van-scheepsbouwer-damen-doen-wereldwijd-verdachte-betalingen-a2687740.

[19] https://fd.nl/ondernemen/1315877/software-die-stem-van-de-baas-nabootst-gebruikt-voor-diefstal en https://www.washingtonpost.com/technology/2019/09/04/an-artificial-intelligence-first-voice-mimicking-software-reportedly-used-major-theft/?noredirect=on.

haar moederbedrijf Paccar[20], of een bedrijf dat onderdelen van gasturbines aan Iran leverde en niet had verwacht dat dit zou opvallen bij de autoriteiten.[21]

f. Exportcontrole

Naast goederen zijn ook software, diensten en kennis onderworpen aan de regelgeving omtrent exportcontrole. Alle exporteurs worden geacht te voldoen aan de wet strategische goederen, het besluit strategische diensten en daarmee verband houdende Europese en Nederlandse regelgeving. Vooral bedrijven die zich bezig houden met technisch hoogwaardige goederen, software en kennis, alsmede bedrijven in de telecommunicatie-, chemische-, luchtvaart-, defensie-, en veiligheidsindustrie zullen maatregelen moeten nemen om aan deze regelgeving te voldoen. De regelgeving is voornamelijk gericht op voorkoming van het omleidingsrisico: het risico dat strategisch belangrijke goederen en kennis beschikbaar worden gesteld aan personen of organisaties die deze inzetten voor doeleinden die niet in lijn zijn met het Nederlandse strategische belang, en de Nederlandse normen en waarden op het gebied van bijvoorbeeld de schending van mensenrechten. Verder dient zowel de exporteur als de importeur op te letten bij het gebruik van goederen of kennis met een Amerikaanse oorsprong. Vanwege de Amerikaanse '*long arm jurisdiction*' is het in die gevallen mogelijk dat de Amerikaanse export controles van toepassing zijn op een Nederlandse export.[22]

g. Fiscale integriteit (bijv. de Mandatory Disclosure Directive)

De Nederlandse banken hebben recent *guidance* ontvangen van De Nederlandsche Bank over de inventarisatie van belastingstructuren van hun klanten.[23] Achterliggende gedachte van de ontwikkeling van deze *good practices* is dat belastingontduiking, maar ook belastingontwijking, een signaal of voorbode kan zijn van structuren die worden gebruikt om gelden wit te wassen. Dit is wederom een voorbeeld waar de eisen gesteld in de financiële sector op het gebied van compliance doorgrijpen op de *non-financials,* en de basis kan vormen voor een lastig gesprek met de huisbankier.

Een andere ontwikkeling is de EU *Mandatory Disclosure Directive* (MDD) uit 2018, die advocaten, accountants en belastingadviseurs verplicht om agressieve belastingstructuren van hun cliënten te melden bij de Belastingdienst.[24] De combinatie van bovenstaande elementen maakt dat inmiddels op andere wijze naar belastingstructuren wordt gekeken dan nog zo'n tien jaar geleden het geval was, en de vraag ontstaat daarmee 1) of alle belastingstructuren afdoende in kaart zijn gebracht, 2) of die nog aansluiten bij de huidige wet- en regelgeving, en 3) of voldoende en snel genoeg wordt ingegrepen als dit niet zo blijkt te zijn. Anders ontstaat daarmee een mogelijk substantieel reputatierisico, plus andere gevolgen in de fiscale hoek die wij nu voor het gemak even buiten beschouwing laten.

h. Interne en externe fraude

Een aantal situaties van fraude is in de voorgaande paragrafen al kort besproken. Ook hier geldt dat het risico maar al te vaak wordt onderschat, of dat medewerkers zich niet bewust zijn dat ze meewerken aan fraude, bijvoorbeeld omdat zij bijvoorbeeld in een sterk hiërarchische structuur zijn opgeleid, waarbij het '*no go*' is om aan de uitspraken en opdrachten van een meerdere te twijfelen of daar vragen over te stellen.

Fraude kan ontstaan in de meest onverwachte uithoeken van een organisatie. Volledig *out of the box* denken kan helpen om fraude te voorkomen. Zo kan bijvoorbeeld fraude ook voorkomen in douane-gerelateerde onderwerpen: in sommige productcategorieën zijn de invoerrechten hoog en kunnen deze, indien verkeerd aangegeven, resulteren in een flinke verlaging van de kosten. Een goede focus van het complianceprogramma, waarbij ook de afdelingen in de eerste lijn worden betrokken om gezamenlijk te analyseren wat er allemaal fout kan gaan, kan helpen om deze risico's beter in kaart te brengen en te beheersen.

8. De ethische kant van de zaak

De elementen gedrag en cultuur zijn in de voorgaande onderdelen al meermaals kort aangestipt; een uitweiding over deze risico-elementen is niet de strekking van dit artikel.[25] De risico's voortkomend uit de bedrijfscultuur en het gedrag van medewerkers mogen ook voor *non-financials* niet in het rijtje van te beheersen risico's ontbreken. Recente incidenten zoals bij Boeing, waar niet-aanspreekbaarheid van het management door de experts die waarschuwden voor technische mankementen van de 737 Max uiteindelijk heeft geleid tot bijna 350 dodelijke slachtoffers van twee vliegtuigcrashes en zeer grote (financiële en reputatie)schade voor de gehele organisatie[26], drukken ons scherper dan ooit met de neus op de feiten. Dat

[20] https://www.nrc.nl/nieuws/2019/08/20/amerikaanse-sancties-zijn-ook-hier-lastig-te-ontlopen-a3970604.

[21] https://fd.nl/economie-politiek/1272589/om-eist-miljoenen-van-limburgs-bedrijf-voor-verboden-handel-met-iran.

[22] De Export Administration Regulations (EAR) zijn te raadplegen via de website van het United States Department of Commerce, Bureau of Industry and Security: www.bis.doc.gov/index.php/ regulations/ exportadministration-regulations-ear.

[23] https://www.toezicht.dnb.nl/en/binaries/51-237528.pdf.

[24] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0822&from=EN.

[25] Wij willen niet nalaten om aandacht te vragen voor de Toolbox Gedrag & Cultuur, die door de Kennistafel Gedrag & Cultuur van de Vereniging voor Compliance Officers (VCO) is ontwikkeld. De Toolbox bevat waardevolle instrumenten voor de uitwerking van ethische elementen van een complianceprogramma aan de hand van praktische handvatten en *tools*. Zie hiervoor https://www.vco.nl/kennistafels/gedrag-cultuur.

Voor *non-financials* wordt het belang van bereidheid tot zelfreflectie steeds groter

zo'n incident ook grote impact heeft op de *supply chain* en afnemers van Boeing, blijkt bijvoorbeeld uit de laatste winstberichten van TUI.[27] En daarmee wordt opnieuw het belang aangetoond van *third party* of *supplier due diligence* voor *non-financials*.
Teruggrijpend op het incident bij Pathé rond CEO-fraude, zien we dat daar ook de vraag ontstaat op welke wijze een organisatie in staat – en ook bereid – is om van gemaakte fouten te leren.[28] De impact van het gebrek hieraan is mogelijk nog groter dan de directe gevolgen van zo'n fraudezaak. Voor *non-financials* wordt het belang van bereidheid tot zelfreflectie steeds groter. Organisaties met een sterke hiërarchische cultuur en waar medewerkers elkaar niet goed kennen, lopen in dit kader een groter risico.

9. Conclusie

Het ontbreken van een zware wettelijke grondslag van een complianceprogramma voor *non-financials* maakt dat het belang van zo'n programma nog te vaak wordt onderschat. En als zo'n programma al wordt ingericht, is de kans aanwezig dat de scope en/of de diepgang te gering blijven, met alle gevolgen van dien. Daarnaast kan het ontbreken van een goede risicobewuste cultuur stevige gevolgen hebben voor onder meer de reputatie van de organisatie.

Complianceprogramma's voor *non-financials* zijn nog regelmatig niet afdoende ingericht of focussen zich te veel op separate onderdelen

Complianceprogramma's voor *non-financials* zijn nog regelmatig niet afdoende ingericht of focussen zich te veel op separate onderdelen, zonder voldoende aandacht voor de samenhang van de elementen en de gevolgen van bijvoorbeeld een schending van de ene regel op andere onderdelen van de algehele bedrijfsvoering, en daarmee gevolgen voor bijvoorbeeld de reputatie van de onderneming.

Daarnaast tekent zich een trend af – mede onder invloed van externe toezichthouders – waarbij banken de aan hen opgelegde eisen steeds meer voorvertalen naar hun klanten. Daarmee komen ook de eisen gesteld in de financiële sector terecht op het bordje van *non-financials*. Naast de selectie van die onderdelen die voor de onderneming van belang zijn om de cruciale risico's te kunnen beheersen, doen *non-financials* er daarom bij het ontwerpen van hun complianceprogramma verstandig aan om oog te houden op een integrale aanpak, ook van hun *supply chain*, daarbij tevens rekening houdend met eventuele eisen van hun *stakeholders* – zoals de bank.

Wij concluderen daarmee dat een adequaat complianceprogramma niet meer kan worden beschouwd als overbodige luxe. Het is een bittere noodzaak om te voorkomen dat een organisatie wordt geconfronteerd met gevolgen van risico's waarvan de aard en de impact eerder niet werden voorzien. ■

---

[26] https://nos.nl/artikel/2289354-topman-boeing-erkent-fouten-bij-737-max.html en https://hbr.org/2019/05/boeing-and-the-importance-of-encouraging-employees-to-speak-up.

[27] https://fd.nl/beurs/1312317/winst-tui-keldert-door-vliegverbod-boeing-737-max.

[28] https://fd.nl/ondernemen/1297031/nieuwe-topman-pathe-ceo-fraude-kost-ons-niet-de-hele-jaarwinst en https://fd.nl/ondernemen/1277850/hoe-de-top-van-pathe-voor-19-mln-om-de-tuin-werd-geleid. De AFM heeft een mooie tool ontwikkeling voor het leren van fouten binnen organisaties, zie https://www.afm.nl/nl-nl/nieuws/2017/okt/onderzoek-open-foutencultuur. Deze aanpak is zeker ook geschikt voor non-financials.