Reactie op Consultatie DNB Wwft Q&As and Good Practices

Inleiding

Met belangstelling heb ik kennisgenomen van de "Consultatieversie DNB 'Q&A's' en 'Good Practices' Wwft" van 18 oktober 2023. Ik maak graag gebruik van de mogelijkheid om hierop te reageren. Ik beperk mij daarbij tot de onderdelen van de eerste consultatievraag:

1.1. *Zijn er elementen in de beleidsuiting die een risicogebaseerde invulling in de weg staan, zonder dat dit wettelijk gezien noodzakelijk is?*

1.2. *Biedt de beleidsuiting voldoende aanknopingspunten om instellingen waar de wet dat toestaat risicogebaseerd te werken?*

1.3. *Zijn er elementen in de beleidsuiting die tot niet-risicogebaseerde belasting van klanten leiden, zonder dat hiertoe een wettelijke noodzaak is?*

Mijn reactie is geschreven vanuit het perspectief van de corporate governance van een bank en de dilemma's die daarbij aan de orde komen bij het streven naar compliance met de Wwft.

Open en gesloten normen

De Wwft bestaat uit zowel gesloten als open normen. Bij het naleven van de *gesloten* normen is sprake van een *resultaats*verplichting voor de betreffende instelling. Het al of niet voldoen aan een wetsartikel met een gesloten norm, en daarmee de vereiste compliance, kan objectief door de instelling zelf, de toezichthouder en/of andere daartoe bevoegde instanties worden vastgesteld en gehandhaafd. Het door DNB vervangen van de "Leidraden", met hun juridisch onduidelijke status, door de nu ter consultatie voorgestelde "Q&A's" is voor het naleven en waar nodig afbakenen van deze gesloten normen een verbetering voor de onder toezicht staande instellingen.

Bij de *open* normen van de Wwft is daarentegen sprake van een *inspannings*verplichting. De instelling moet aantonen dat hij of zij zich voldoende heeft ingespannen om aan de open norm van de wettelijke verplichting te voldoen.

In het geval van het naleven van de open normen van de Wwft is de mate van compliance van de instelling uiteindelijk afhankelijk van het al of niet (kunnen) voldoen aan de *verwachtingen* van de toezichthouder (DNB) met betrekking tot de vereiste inspanningen die de instelling zich volgens haar (had) moet(en) getroosten om te voldoen aan de invulling van deze open normen, en het resultaat daarvan.

Implicaties voor de corporate governance van een instelling

Om deze redenen bestaat er voor de corporate governance van de onder toezicht staande instellingen een belangrijk verschil tussen het zeker stellen van compliance met gesloten normen en compliance met open normen.

Bij *gesloten* normen is er geen discussie: het systeem van interne controle moet zorgdragen voor naleving van deze gesloten normen. Bij de *open* normen is dit anders: hier zal sprake moeten zijn van een belangenafweging van enerzijds de aangewende middelen voor de vereiste en gewenste beheersing van compliance- en reputatierisico's en anderzijds de positieve en/of negatieve invloed hiervan op de belangen van stakeholders zoals klanten en aandeelhouders.

Voor bestuurders en commissarissen van banken vloeit de noodzaak van deze belangenafweging ook voort uit de bankiers-eed. Deze vereist immers dat hij of zij *"(…) een zorgvuldige afweging zal maken tussen alle belangen die bij de onderneming betrokken zijn, te weten die van de klanten, de aandeelhouders/leden, de werknemers en de samenleving waarin de onderneming opereert"*.

Een objectieve en rechtszekere afbakening en invulling van de in deze eed cq. belofte bedoelde belangen is een essentiële voorwaarde voor het op een zorgvuldige wijze kunnen maken van deze afweging. Dit geldt ook voor de belangen cq. de kosten en opbrengsten van compliance met de Wwft.

Voor de naleving van de open normen in de Wwft is deze objectieve en rechtszekere afbakening, ook met deze nieuwe Q&A's, echter (nog steeds) niet mogelijk. Dit geldt met name voor het antwoord op de vraag wanneer er volgens DNB sprake is van een acceptabele risico-tolerantie voor de betreffende instelling.

Kernprobleem: Onzekerheid over afbakening van risico-tolerantie bij open normen

Om aan de vereisten van de Wwft te kunnen voldoen moeten instellingen de bandbreedte en de inhoud van de bij de naleving van de *open* normen te hanteren *risico-tolerantie* bepalen. Deze risico-tolerantie moet daarbij in lijn zijn met de verwachtingen die DNB *achteraf* bij haar toezicht zal gaan hanteren.

De beleidsuitingen cq. Q&A's in dit consultatiedocument die hierop betrekking hebben (zie bijlage bij deze reactie) leggen de bal hiervoor echter nog steeds volledig bij de onder toezicht staande instelling. Zij geven geen enkele juridisch verbindende guidance waar een instelling zich bij het vaststellen van deze voor compliance acceptabele risico-tolerantie voor open normen op zou kunnen baseren.

De *"Good practices"* kunnen deze rol ook niet vervullen. Zij bevatten in dit verband interessante suggesties, maar zoals de Leeswijzer beleidsuitingen DNB al stelt: *"Anders dan een beleidsregel en een Q&A wordt een good practice niet als uitgangspunt gehanteerd in de toezichtpraktijk van DNB, omdat deze een suggestie of aanbeveling is voor instellingen en DNB uitdrukkelijk de mogelijkheid open wil laten dat op een andere manier invulling wordt gegeven aan de wet- en regelgeving."*

Het is natuurlijk positief dat DNB de mogelijkheid open houdt dat *"…op een andere manier invulling wordt gegeven aan de wet- en regelgeving",* maar dit neemt niet de genoemde onzekerheden weg over wat voor DNB daarbij acceptabel zou kunnen zijn.

Het is niet zo dat DNB de grenzen van deze risico-tolerantie voor een bepaalde instelling niet zou kennen of niet vooraf zou kunnen aangeven. Zij doet dit immers achteraf alsnog, wanneer zij moet beoordelen of een instelling de bepalingen van de Wwft wel of niet (voldoende) heeft nageleefd.

Het niet vooraf met de instelling communiceren over deze grenzen van de risico-tolerantie leidt tot (onnodige) rechtsonzekerheid voor de betreffende instellingen.

Consultatievraag: Zijn er elementen in de beleidsuiting die een risicogebaseerde invulling in de weg staan, zonder dat dit wettelijk gezien noodzakelijk is?

Deze consultatievraag moet mijns inziens, op basis van het hiervoor gestelde, helaas bevestigend worden beantwoord.

Het risico van het niet naleven van de Wwft heeft binnen de risicobereidheid van een bank een hoge mate van negatief verwacht resultaat (ie. kans vermenigvuldigd met impact). De mogelijke negatieve impact op reputatie, mogelijke boetes en de *license to operate* is immers omvangrijk.

De onbekendheid van bankbestuurders met de toetsingscriteria van de toezichthouders (inclusief het OM) met betrekking tot de risico-tolerantie bij de naleving van open normen verhogen voor de bank het risico van deze mogelijke non-compliance. Om het hierdoor ontstane bruto risico van non-compliance te mitigeren is het om deze reden voor banken (mogelijk) niet voldoende om voor de naleving van de Wwft slechts risico-gebaseerd middelen toe te wijzen. Het systeem is immers ook met deze Q&A's in belangrijke mate nog steeds *rule-based* en in veel mindere mate *risk-based.*[1]

Dit kan voor deze banken vervolgens een reden zijn om *open-ended* c.q. *'whatever it takes'* middelen toe te (blijven) wijzen aan de naleving van de Wwft, ondanks de verduidelijkingen op een aantal belangrijke punten in het Q&A document van DNB. Dit gaat mogelijk ten koste van de belangen van andere stakeholders, zoals klanten en aandeelhouders.

FATF: "Framework that spells out the degree of discretion"

Deze *open-ended* c.q. *'whatever it takes'* benadering kan echter niet de bedoeling zijn geweest van de wetgever, gezien de bepalingen in de Wwft die vereisen dat de *maatregelen, om risico's op witwassen en financieren van terrorisme vast te stellen en te beoordelen, in verhouding staan tot de aard en de omvang van de instelling (artikel 2b.1) en gedragslijnen, procedures en maatregelen daaraan evenredig zijn (artikel 2c.2).*

De *"Risk-Based Approach guidance for the banking sector"* van de FATF uit 2014 stelt in lijn daarmee:[2]

"The effectiveness of a Risk Based Approach (RBA) depends on a common understanding by competent authorities and banks of what the RBA entails, how it should be applied and how Money Laundering/Terrorism Financing risks should be addressed. In addition to a legal and regulatory framework that spells out the degree of discretion, banks have to deal with the risks they identify, and it is important that competent authorities and supervisors in particular issue guidance to banks on how they expect them to meet their legal and regulatory AML/CFT obligations in a risksensitive way. Supporting ongoing and effective communication between competent authorities and banks is an essential prerequisite for the successful implementation of a RBA."

Het voorliggende Q&A consultatiedocument is zeker een stap in deze goede richting. Waar het de (in de bijlage hieronder aangegeven) open normen betreft kan het mijns inziens echter (nog) niet gekwalificeerd worden als een volledig en voldoende *framework that spells out the degree of discretion*. DNB laat daarvoor wat betreft deze open normen nog te veel onduidelijkheid mbt. *how they expect them* (de banken) *to meet their legal and regulatory AML/CFT obligations in a risksensitive way*.

"Common understanding by competent authorities and banks"

Diverse Q&A's in dit consultatiedocument (zie tweede deel van de bijlage bij deze reactie) benadrukken terecht het *individuele* karakter van de Wwft problematiek bij de verschillende instellingen.

[1] Zie ook: Stichting Maatschappij en Veiligheid, *Poortwachters tegen witwassen: Naar een poortwachtersfunctie van banken die beter bijdraagt aan voorkoming en bestrijding van witwassen,* 2022.

[2] Onderstreping JSTT.

Het is daarom belangrijk dat individuele banken en DNB in constructief overleg treden om tot een wederzijds verplichtende overeenstemming *vooraf* te komen met betrekking tot de operationele invulling van de risico-gebaseerde benadering van de open normen in de Wwft, en dan met name de voor de betreffende instelling te hanteren materialiteits- en risicocriteria. Dit kan de basis zijn voor de door de FATF aanbevolen *"common understanding".*

Dit zou de vorm kunnen krijgen van een wederzijds vooraf overeengekomen en wederzijds verplichtend 'toezichtsconvenant', waarbij de SIRA van de betreffende instelling, en de daarin gespecificeerde risico-tolerantie, *formeel* als uitgangspunt voor de naleving van de Wwft wordt geaccepteerd door DNB.[3] Indien (onverhoopt) geen overeenstemming bereikt kan worden over de verschillende werkwijzen, normen en standaarden hierin kunnen partijen hun verschil van mening vervolgens voorleggen aan de bestuursrechter.

In dit toezichtsconvenant kunnen zowel de voor goede corporate governance vereiste belangenweging als de door de Wwft vereiste evenredigheid van de te nemen maatregelen met elkaar verenigd worden. Het kan bovendien de noodzakelijke "soll-positie" beschrijven waartegen de interne en externe accountants de "ist-situatie" kunnen toetsen en daarover kunnen rapporteren.

Wellicht kan dit ook bijdragen aan het wegnemen van de zorgen van de NBA in dit verband, wanneer die stelt*: "De vereisten vanuit de Wwft worden regelmatig bijgesteld. Vanwege die bijstellingen en de complexiteit van de regelgeving blijkt in de praktijk dat volledige naleving van deze regelgeving een moeilijk uitvoerbare opdracht is voor de bancaire sector in haar functie als poortwachter."*[4]

De aan de Wwft gerelateerde strafrechtelijke interventies van het Openbaar Ministerie hebben de noodzaak van heldere en juridisch verbindende risico-criteria voor de bestuurders en commissarissen van instellingen alleen nog maar groter gemaakt.

Het OM heeft haar conclusies immers niet gebaseerd op het eventuele tekortschieten van de naleving van *het principe van een risico-gebaseerde* benadering door ING en ABN AMRO. Zij is bij haar handhaving, voor zover dat blijkt uit het respectievelijke 'feitenrelaas', uitgegaan van een algehele resultaatsverplichting en een 100% controle door instellingen. Zij neemt daarmee kennelijk een *'zero failure'* benadering als uitgangspunt bij het beoordelen van de naleving van de Wwft.

Ook deze dreiging om door het OM van een overtreding van de WED beschuldigd te worden zal bij banken een meer risico-gebaseerde benadering van de naleving van de Wwft in de weg blijven staan, zolang zij zich niet tegenover het OM kunnen beroepen op vooraf overeengekomen concretere afbakeningen van hun verantwoordelijkheden voor het naleven van de Wwft.

<u>Conclusie en aanbeveling</u>

Vraag 1.1: Uit bovenstaande analyse blijkt mijns inziens dat er elementen in de beleidsuiting zijn die een risico-gebaseerde invulling in de weg staan, zonder dat dit wettelijk gezien noodzakelijk is.

Vraag 1.2: De beleidsuiting biedt met name bij de open normen nog onvoldoende aanknopingspunten om instellingen waar de wet dat toestaat risico-gebaseerd te laten werken.

[3] Dit zou een benadering kunnen zijn die vergelijkbaar is met het risico-gebaseerde controleprogramma van de externe respectievelijk de interne accountant van een instelling.

[4] Koninklijke Nederlandse Beroepsorganisatie voor Accountants (NBA), Herziene NBA handreiking 1145, *Specifieke verplichtingen vanuit de toezichtwet- en regelgeving voor de interne auditor en de externe accountant bij banken*, Amsterdam, 13 oktober 2021, p.5.

Vraag 1.3: De beleidsuiting is onvolledig met betrekking tot het afbakenen van open normen of het aangeven van een proces dat kan leiden tot een *common understanding* vooraf in de zin van de FATF. Het neemt daarmee nog steeds de noodzaak om te streven naar een maximale, in plaats van een risico-gebaseerde, benadering van het naleven van de open normen niet weg en leidt daarmee tot niet-risico-gebaseerde belasting van klanten, zolang voor instellingen onduidelijk is wat, bij de toetsing achteraf, precies de verwachtingen van DNB en het OM zullen blijken te zijn geweest.

Dit leidt wat mij betreft tot de aanbeveling om als DNB per instelling een op de SIRA gebaseerde, wederzijds verbindend, toezichts-convenant af te sluiten en deze periodiek te updaten, *voorafgaand* aan de periode waarover toezicht zal worden gehouden op de naleving van de Wwft.

Mr. Drs. J.S.T. (Tjalling) Tiemstra RA
(Voormalig) commissaris en toezichthouder.

Wassenaar, oktober 2023

Bijlage

Voorbeelden van Q&A's waaruit blijkt dat de verantwoording voor het bepalen van de bandbreedte en de inhoud van de bij de naleving van de open normen te hanteren risico-tolerantie zonder verdere rechtszekerheid gevende beleidsuitingen van DNB volledig bij de onder toezicht staande instelling blijft:[5]

QA3.58:
Vraag: Op welke wijze vindt de afweging plaats of de cliënt binnen de risicotolerantie valt?
Antwoord: *Een instelling legt in haar beleid vast welke risico's al dan niet acceptabel zijn*, rekening houdend met de wettelijke vereisten omtrent bijvoorbeeld HRTC.

QA3.60:
Vraag: Bepaalt DNB welke cliënten wel of niet aangenomen kunnen worden?
Antwoord: Nee, de instelling accepteert al dan niet de cliënt. De instelling baseert zich daarbij op de eisen die de Wwft stelt, *haar beheersmaatregelen en haar eigen risicobereidheid*.

QA4.4:
Vraag: De inrichting van transactiemonitoring is een dynamisch proces; wat betekent dat?
Antwoord: In hoofdstuk 2 wordt besproken dat de *risicoanalyse het uitgangspunt is voor de inrichting van de beheersing, inclusief transactiemonitoring.* De risicoanalyse brengt de relevante en belangrijkste risico's met betrekking tot witwassen en financieren van terrorisme in kaart. *Op basis hiervan bepaalt de instelling* hoe de transactiemonitoring moet worden ingericht om de risico's aantoonbaar te beheersen. Omdat risico's veranderen, is dit een dynamisch proces:

- Op basis van de aard en omvang van het risico (bijv. cash, betalingen naar hoog risicolanden). *bepaalt de instelling* welke business rules en modellen (met bijbehorende drempelwaarden) het risico kunnen detecteren.
- Aan de hand van (historische) transactiedatasets test de instelling of de risico's voldoende worden gedetecteerd met *de gekozen business rules*, modellen en grenswaarden, waarna wordt overgegaan tot implementatie in de bedrijfsvoering.

[5] Cursivering en onderstreping JSTT.

- Na de implementatie van een *passende set aan maatregelen*, monitort de instelling of de output van het transactiemonitoringsysteem aansluit bij de geïdentificeerde risico's en legt de overwegingen daarbij vast.
- De vaststelling dat een risico nog onvoldoende wordt gedetecteerd kan leiden tot aanvullende mitigerende maatregelen door de instelling.

Noodzaak voor maatwerk of "common understanding":

QA4.3:
Vraag: Moet transactiemonitoring altijd geautomatiseerd plaatsvinden?
Antwoord: Nee. Instellingen richten het transactiemonitoringsproces risicogebaseerd in. *De inrichting hangt onder meer af van de aard en omvang van de instelling, van de risico's waar de instelling mee geconfronteerd wordt en van het aantal transacties dat door de instelling wordt uitgevoerd.*

4.1.1 Business rules & modellen: De kennis die de instelling toepast om ongebruikelijke of verdachte transacties te kunnen detecteren, is *toegesneden op de risico's die de instelling loopt.*

QA4.5:
Vraag: Is het voldoende als een instelling standaardmodellen toepast voor het detecteren van ongebruikelijke transacties?
Antwoord: Nee. *Standaardmodellen kunnen een startpunt zijn, maar een instelling kan hier niet enkel op vertrouwen.* Een transactiemonitoringsysteem dient te *passen bij het risicoprofiel van de instelling*, en gevoed te worden door toegepaste kennis (intelligence) vanuit de instelling. De business rules van het transactiemonitoringsyteem dienen passend te zijn om de risico's die de instelling loopt effectief te mitigeren. De instelling legt het verband tussen de risicoanalyse en het transactiemonitoringssysteem vast.

QA4.8:
Vraag: Is er een model dat voor alle instellingen toepasbaar is?
Antwoord: Nee. De business rules en de modellen zijn toegespitst op de *risico's die van toepassing zijn op de instelling*. Dat betekent dat een instelling zelf analyseert welke business rules en modellen voor haar relevant zijn.

QA4.16:
Vraag: Wanneer is een transactie ongebruikelijk?
Antwoord: De subjectieve indicator vraagt om een *eigen beoordeling door de instelling*. Dit past in de risicogebaseerde benadering.

QA4.18:
Vraag: In hoeverre kan een alert automatisch gesloten worden?
Antwoord: De instelling heeft een expliciete overweging ten aanzien van *haar risk appetite* met betrekking tot bepaalde transacties.

QA3.59:
Vraag: Moet een instelling elk risico op betrokkenheid bij witwassen of financieren van terrorisme uitsluiten?

Antwoord: Van instellingen wordt daarmee verwacht dat zij *alle redelijke maatregelen* hebben getroffen om te voorkomen dat zij betrokken raken bij witwassen of financieren van terrorisme. De risicobenadering houdt ook in dat geaccepteerd wordt dat nooit volledig kan worden voorkomen dat, ondanks mitigerende maatregelen, toch criminele geldstromen door het financiële systeem gaan. Van instellingen wordt niet verwacht dat zij dit volledig kunnen uitsluiten, er is dus een geaccepteerd 'restrisico'.