CONCEPT - GUIDANCE

Guidance thema onderzoek post-event transactiemonitoringsproces bij banken

Inhoud

SAMENVATTING

Transactiemonitoring is een essentiële maatregel om integriteitrisico's op het gebied van witwassen en terrorismefinanciering te beheersen. DNB heeft bij het in 2016 uitgevoerde thema-onderzoek naar transactiemonitoring bij banken en andere instellingen geconstateerd dat de onderzochte banken hun post-event transactiemonitoringsproces nog niet op orde hebben. Onze belangrijkste bevindingen zijn als volgt:

1. DNB heeft geconstateerd dat alle onderzochte banken hun financieel economische criminaliteitsrisico's die uit de SIRA voortvloeien niet voldoende doorvertalen naar het transactiemonitoringsproces. DNB constateert verder dat de onderzochte banken bij de bepaling van het risicoprofiel van de cliënt het verwachte transactiegedrag van de cliënt niet meenemen.
2. Gebleken is dat niet alle onderzochte banken voldoende beleid voor transactiemonitoring hebben opgesteld en dit derhalve ook niet hebben uitgewerkt in onderliggende procedures en werkprocessen.
3. De onderzochte banken beschikken over een geautomatiseerd transactiemonitoringssysteem, maar zij hebben veelal niet een onderbouwde en toereikende set aan business rules (detectieregels met scenario's en grenswaarden) om witwas- en terrorismefinancieringsrisico's te detecteren.
4. Gebleken is dat de onderzochte banken voorgenomen en uitgevoerde ongebruikelijke transacties niet altijd onverwijld en volledig aan de FIU-NL melden, conform een gedocumenteerd meldproces. Het alertafhandelingsproces bleek niet altijd adequaat te zijn gedocumenteerd, met name overwegingen tot het sluiten dan wel escaleren van alerts en conclusies daaromtrent ontbraken.
5. De governance ten aanzien van transactiemonitoring bleek niet altijd op orde te zijn, met name wat betreft een duidelijke rolverdeling tussen de *three lines of defense*.
6. Het onderzoek liet zien dat banken niet altijd beschikken over een toegesneden trainingsprogramma voor hun medewerkers en de medewerkers zich niet altijd bewust toonden van witwas- en terrorismefinancieringsrisico's.

De uitkomsten van het thema-onderzoek laten zien dat de banken ten aanzien van transactiemonitoring nog niet op het niveau zijn dat de financieel economische criminaliteitsrisico's adequaat worden beheerst.

In het bijgevoegde volwassenheidsmodel staan de niveaus van volwassenheid die DNB voor de sector heeft opgesteld. Vanzelfsprekend verwacht DNB dat u aan de minimale eisen voldoet. Daarnaast verwacht DNB dat u aan de hand van het volwassenheidsmodel en de in dit document opgenomen handvatten – waar nodig - verbeteringen doorvoert in uw bestaande transactiemonitoringsproces.

1. Inleiding

1.1 Waarom deze guidance?

Financieel economische criminaliteit is van alle dag: de krantenkoppen laten zien dat de samenleving ongewild slachtoffer kan worden van deze vorm van criminaliteit, denk aan recente incidenten als de Panama Papers en terroristische aanslagen in West-Europa. Financiële ondernemingen, waaronder banken, hebben een belangrijke rol om financieel economische criminaliteit te bestrijden. Daartoe voeren banken onder meer cliëntenonderzoek uit, door middel van zogenoemde *customer due diligence* en monitoren zij de uitgevoerde transacties van cliënten. Dit laatste, de transactiemonitoring, is onderwerp van deze guidance.

Een bank die adequaat monitort welke transacties in het kader van haar dienstverlening worden uitgevoerd, kan tijdig ingrijpen als sprake is van een (mogelijk) ongebruikelijke transactie of een afwijkend transactiepatroon. Gebeurt dit niet, of niet goed, dan kan het zijn dat u als bank (ongewild) bijdraagt aan het financieren van terrorisme, of dat via uw kantoor crimineel geld witgewassen wordt. Uw functie als poortwachter van het Nederlandse financiële systeem vergt onder meer dat u adequaat transacties monitort. Continu en alert. De wetgever heeft op dit gebied eisen geformuleerd waaraan uw bank moet voldoen. DNB heeft de wettelijke taak om toe te zien op naleving van de wet- en regelgeving in dit verband. Transactiemonitoring is verplicht voor iedere bank; de praktische invulling hiervan wordt echter niet in detail voorgeschreven door wet- en regelgeving.

Het onderwerp transactiemonitoring is voor banken niet nieuw. De in dit document opgenomen aandachtspunten en voorbeelden zijn specifiek bedoeld als handvatten voor het transactiemonitoringsproces van banken en gelden daarmee als een aanvulling op geldende wet- en regelgeving en eerder uitgebrachte leidraden over dit onderwerp, zoals de *DNB Leidraad Wwft en SW, versie 3.0; april 2015*[1]*; Voorkoming misbruik financiële stelsel voor witwassen en financieren van terrorisme en beheersing van integriteitrisico* en de *Q&A Beoordeling Ongoing Due Diligence Proces (WWFT en SW)* (van december 2013).

De in dit document opgenomen handvatten kunnen uw bank helpen met het op orde brengen van uw transactiemonitoringsproces. DNB verwacht dan ook dat u hier als sector goed kennis van neemt en daar waar nodig verbeteringen implementeert in uw bedrijfsvoering.

1.2 Transactiemonitoring: wettelijke verplichting tot voortdurende controle op transacties

Banken zijn wettelijk verplicht maatregelen te nemen om witwassen en terrorismefinanciering te voorkomen. Hierdoor moeten zij bijzondere aandacht besteden aan ongebruikelijke transactiepatronen en transacties van cliënten, die naar hun aard een hoger risico op witwassen of het financieren van terrorisme met zich meebrengen. Indien er aanleiding is om te veronderstellen dat een transactie verband houdt met witwassen of terrorismefinanciering, dan moet u als bank deze als ongebruikelijke transactie melden bij de Financial Intelligence Unit – Nederland (FIU-NL).[2] Om dit te kunnen doen is het van cruciaal belang dat banken beschikken over een effectief transactiemonitoringsproces.[3]

Om een adequate voortdurende controle uit te oefenen, dienen banken op grond van artikel 10 Besluit prudentiële regels Wft (Bpr) allereerst zorg te dragen voor een systematische integrititeitrisicoanalyse (SIRA). Integriteitsrisico's zijn daarbij gedefinieerd als het "gevaar voor aantasting van de reputatie of bestaande of toekomstige bedreiging van vermogen of resultaat van een financiële onderneming als gevolg van een ontoereikende naleving van hetgeen bij of krachtens enig wettelijk voorschrift is voorgeschreven".[4] Daartoe behoren dus ook de risico's op witwassen en financieren van terrorisme. Indien naar aanleiding van de analyse (rest)risico's gesignaleerd worden, moeten banken hiervoor beleid formuleren, procedures instellen en maatregelen treffen.

Specifiek ten aanzien van de risico's op witwassen en terrorismefinanciering bepaalt de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) dat een bank ter voorkoming

[1] Wwft: Wet ter voorkoming van witwassen en financieren van terrorisme; SW: Sanctiewet 1977
[2] Kort gezegd spreken wij hierna in dit document over "ongebruikelijke transacties"
[3] Artikel 14, lid 4 Bpr, artikelen 2a, lid 1 en 3, lid 2 sub d Wwft.
[4] Art. 1 Bpr

daarvan onderzoek moet doen naar zijn cliënten.[5] Daarbij dient de bank het doel en de beoogde relatie van de zakelijke relatie vast te stellen. Ook moet de bank een voortdurende controle op de zakelijke relatie en de tijdens de duur van deze relatie verrichte transacties uitoefenen.[6] Zo kunnen banken verzekeren dat deze transacties overeenkomen met de kennis die de bank heeft van de cliënt en diens risicoprofiel, met zo nodig een onderzoek naar de bron van de middelen die bij de zakelijke relatie of de transactie gebruikt worden.[7]

Het begrip ”voortdurende controle” staat centraal in het proces van transactiemonitoring en kan door uw bank op eigen wijze worden ingevuld. Verwacht mag worden dat uw bank beschikt over een transactiemonitoringssysteem waarbij transacties worden gemonitord en mogelijk ongebruikelijke transactiepatronen en transacties worden ingebracht in een alertafhandelingsproces. Om dergelijke transactiepatronen en transacties te kunnen identificeren, heeft uw bank indicatoren en red flags opgesteld. Bij dit proces dient u bijzondere aandacht te hebben besteed aan ongebruikelijke transactiepatronen en transacties die naar hun aard een hoger risico op witwassen of financieren van terrorisme met zich meebrengen.[8]

Een verrichte of voorgenomen ongebruikelijke transactie moet onverwijld worden gemeld aan de FIU-NL zodra het ongebruikelijke karakter van de transactie bekend is geworden.[9] De bank dient dan ook specifieke procedures en werkprocessen te hebben opgesteld om transactiealerts te beoordelen, af te handelen en ongebruikelijke transacties te melden.[10] Ter waarborging van deze procedures en maatregelen dient een bank er zorg voor te dragen dat haar werknemers, voor zover relevant voor de uitoefening van hun taken, bekend zijn met de Wwft en periodiek training krijgen. Dit moet hen in staat stellen het cliëntenonderzoek goed en volledig uit te voeren en ongebruikelijke transacties te herkennen.[11]

DNB heeft in 2016 onderzoek uitgevoerd naar het transactiemonitoringsproces bij banken. De uitkomsten van het onderzoek laten zien dat de onderzochte banken op een aantal belangrijke onderdelen dit proces nog niet op orde hebben. In dit document wordt uiteengezet aan welke wettelijke vereisten banken dienen te voldoen en hoe DNB de invulling van deze norm, conform internationale standaarden en good practices, voor ogen heeft. Wij illustreren dit aan de hand van onze onderzoeksuitkomsten, waarbij wij zowel good practices geven als voorbeelden waarbij de norm volgens DNB onjuist is ingevuld. In verband met de continu verhoogde terreurdreiging in Nederland en Europa lag in het onderzoek extra focus op de wijze van transactiemonitoring in relatie tot risico’s op terrorismefinanciering, vandaar dat wij daar ook specifieke uitkomsten over delen.

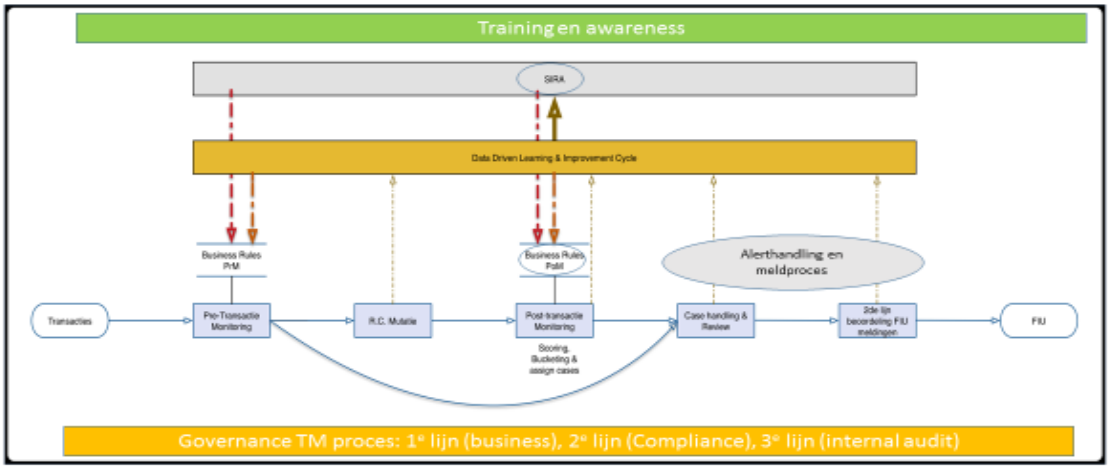
Dit document is als volgt opgebouwd. In hoofdstuk 2 geven wij een schematische weergave van hoe een transactiemonitoringsproces eruit kan zien. Ook kunt u daar het door DNB bij het onderzoek gehanteerde volwassenheidsmodel vinden. In hoofdstuk 3 leest u onze belangrijkste bevindingen, good practices en voorbeelden hoe het niet moet.

2. Transactiemonitoring

2.1 Het transactiemonitoringsproces

Het transactiemonitoringproces kan er als volgt uitzien[12]:

[5] Art. 2a, lid 1 en art. 3, lid 1 Wwft.
[6] In artikel 1, lid 1, sub m, Wwft, wordt een transactie als volgt gedefinieerd: een transactie is een handeling of samenstel van handelingen van of ten behoeve van een cliënt, waarvan een instelling ten behoeve van haar dienstverlening aan die cliënt heeft kennisgenomen
[7] Art. 3, lid 2, sub d Wwft.
[8] Art. 2a, lid 1 Wwft.
[9] Art. 16 Wwft.
[10] Art. 16 Wwft jo. artt. 17 en 18 Bpr.
[11] Art. 35 Wwft.
[12] Onderstaand figuur hebben wij – omwille van de leesbaarheid als bijlage aan dit document toegevoegd.



Transactiemonitoring kan op verschillende manieren worden uitgevoerd. Zoals uit het schema blijkt, kan sprake zijn van pre-transactiemonitoring en post-event transactiemonitoring, en liefst van beide, dat wil zeggen dat zowel vooraf als achteraf transacties worden gemonitord.

Pre-transactiemonitoring
Pre-transactiemonitoring vindt plaats voordat de transactie is uitgevoerd. Een cliënt komt bijvoorbeeld bij de balie van een bankkantoor en wil bepaalde coupures of vreemde valuta omwisselen of een chartale hoeveelheid geld op een bankrekening storten. Bij post-event transactiemonitoring is de transactie reeds door de bank uitgevoerd en vindt de transactiemonitoring achteraf plaats. DNB is van oordeel dat pre-transactiemonitoring een effectieve bijdrage kan leveren, met name wanneer bij aanvang van de cliëntrelatie een duidelijk profiel van verwachte transacties wordt gemaakt dat vervolgens gebruikt kan worden voor monitoring. Hierdoor kan een instelling ongebruikelijke transacties mogelijk reeds voor effectuering detecteren en deze voorgenomen transactie onverwijld melden aan de FIU-NL

Post-event transactiemonitoring
Ons themaonderzoek had specifiek betrekking op het post-event transactiemonitoringproces, omdat banken vooral op deze wijze witwas- en terrorismefinancieringsrisico's kunnen detecteren. Wij benadrukken echter dat banken ook moeten beschikken over een pre-transactiemonitoringsproces, waarbij het van belang is dat banken adequate maatregelen treffen om ongebruikelijke transacties te detecteren voordat deze uitgevoerd worden dan wel ten tijde van de uitvoering.

Het transactiemonitoringproces is onderdeel van het cliëntenonderzoek. Door het cliëntenonderzoek verkrijgt u als bank doorlopend kennis van de cliënt, waaronder het doel en de beoogde aard van de zakelijke relatie met de cliënt. De bank beoordeelt daarbij systematisch of er bij de door de cliënt uitgevoerde transacties sprake is van ongebruikelijke patronen die kunnen duiden op witwassen of terrorismefinanciering. Het monitoren van de transacties van de cliënt moet worden afgestemd op de cliënt zelf: het soort cliënt, het type dienstverlening aan de cliënt en het risicoprofiel van de cliënt. Per cliënt en per product kan de monitoring verschillend ingericht worden.

De eerste stap in het transactiemonitoringsproces is dat u als bank systematisch de witwas- en terrorismefinancieringsrisico's analyseert die uw verschillende soorten cliënten, producten, distributiekanalen en transacties met zich meebrengen. De uitkomsten van deze analyse legt u vast in de zogenoemde SIRA en vertaalt u vervolgens door naar uw beleid, processen en procedures omtrent transactiemonitoring. Daarbij deelt u de cliënten van uw bank in risicocategorieën (bijvoorbeeld hoog, midden en laag) in, op grond van de witwas- en terrorismefinancieringsrisico's die de zakelijke relatie met de cliënt met zich meebrengt. Voor het risicoprofiel van een cliënt maakt u een transactieprofiel op basis van de *verwachte* transacties van een cliënt of het verwachte gebruik

van de rekening.[13] Door een transactieprofiel aan te maken, kan uw bank zich er in voldoende mate van verzekeren dat de tijdens de duur van de relatie verrichte transacties overeenkomen met de kennis die u heeft van de cliënt en diens risicoprofiel. Door het *verwachte* transactiegedrag van de cliënt mee te nemen, kunt u toetsen of de door de cliënt uitgevoerde transacties overeenkomen met de kennis die u heeft van de cliënt.

Voor de tweede stap, het detecteren van ongebruikelijke transactiepatronen en transacties die kunnen duiden op witwassen of financieringen van terrorisme, maakt u gebruik van een (post-event) transactiemonitoringssysteem. Informatie en data over de cliënt, diensten aan de cliënt en diens transacties gebruikt u in uw transactiemonitoringssysteem. Indien sprake is van grotere hoeveelheden transacties, ligt het in de rede om de transactiemonitoring geautomatiseerd te laten plaatsvinden om de effectiviteit, consistentie en doorlooptijd van monitoring te kunnen borgen. In het systeem zijn op zijn minst vooraf gedefinieerde *business rules* opgenomen: detectieregels in de vorm van scenario's en grensbedragen. Daarnaast zijn ook meer geavanceerde systemen, zoals *artificial intelligence*-systemen, gewenst, en in voorkomende gevallen noodzakelijk, afhankelijk van onder meer aard en omvang van transacties. Zo zal bij een bank met bijvoorbeeld een eenvoudig bedrijfsmodel en een beperkt aantal eenvoudige transacties, een geavanceerd systeem mogelijk minder noodzakelijk zijn.

Met behulp van uw transactiemonitoringssysteem en gebruik van intelligente software kunt u – als derde stap - deze data continu analyseren. Het systeem genereert op basis van deze *business rules* vervolgens alerts. Met een alert wordt een signaal bedoeld dat duidt op een mogelijk ongebruikelijke transactie dan wel een transactie met hoogrisico-karakter die u als bank moet onderzoeken. De bevindingen van uw onderzoek van de alerts worden adequaat en duidelijk vastgelegd. Als uit de onderzoeksbevindingen blijkt dat de transactie ongebruikelijk is, meldt u deze transactie onverwijld aan de FIU-NL. De overwegingen en besluitvorming om een transactie wel of niet te melden, heeft u voldoende inzichtelijk gemaakt. Op het moment dat een bank – al dan niet opzettelijk- niet voldoet aan de meldplicht, dan kan dat een economisch delict zijn.

U beoordeelt de gevolgen van een melding aan de FIU-NL en een eventuele terugmelding van de FIU-NL voor het risicoprofiel van de cliënt en eventuele aanvullende beheersmaatregelen. Sluitstuk van het transactiemonitoringsproces is de bewaring van gegevens die u verkrijgt in het kader van transactiemonitoring.

2.2 Volwassenheidsmodel

Het themaonderzoek (post-event) transactiemonitoring bij banken zag toe op het beoordelen van de opzet, het bestaan en de werking van hun post-event transactiemonitoringsproces. Bij de uitvoering van dit themaonderzoek hebben we gebruik gemaakt van een door DNB ontwikkeld volwassenheidsmodel voor transactiemonitoring. Dit model houdt rekening met de relevante vereisten uit de Wft en Wwft en is bedoeld om aan te geven waar een bank zich qua volwassenheid in het transactiemonitoringsproces bevindt. In dit model wordt de mate van naleving (van non-compliance tot best practice) op zes gebieden toegelicht aan de hand van een vierpuntschaal:

- Rode kwalificatie: is geheel non-compliant
- Oranje score: is onvoldoende compliant
- Gele score: is in voldoende mate compliant
- Groene score: is best practice

In onderstaand figuur[14] ziet u het volwassenheidsmodel nader uitgewerkt, inclusief de mogelijke scores op de zes toetsingselementen.

[13] DNB verwijst in deze naar de Leidraad Wwft en SW, versie 3.0, april 2015, pagina's 29-32, waar guidance wordt gegeven hoe een instelling dit zou kunnen doen.
[14] Omwille van de leesbaarheid hebben wij dit figuur separaat als bijlage aan dit document toegevoegd.

Volwassenheidsmodel voor (post-event) transactiemonitoring

SIRA / risicoprofiel (1)	Opzet beleid en procedures (2)	TM systeem/ business rules (3)	Alert afhandeling en meldproces (4)	Governance: 1e, 2e en 3e lijn (5)	Training en awareness (6)
• SIRA niet uitgevoerd • Geen clientrisico profielen	• Geen transactiemonitoring beleid en procedures	• Geen systeem aanwezig voor transactiemonitoring dat passend is bij risicoprofiel van de instelling • Geen AML/CFT indicatoren en business rules om ongebruikelijke transacties te herkennen	• Geen alert afhandelings- en meldproces gedefinieerd • Afhandeling transactiemonitoring alerts wordt niet vastgelegd en opgevolgd • (Voorgenomen) ongebruikelijke transacties worden structureel niet onverwijld gemeld aan de FIU	• Geen functiescheiding 1e, 2e, 3e lijn • Verantwoordelijkheden van 1e, 2e en 3e lijn niet beschreven • Geen second line monitoring • Geen onafhankelijke interne controle • Periodieke managementinformatie over uitkomsten TM niet beschikbaar	• Geen kennis en awareness ten aanzien van witwas- en/of terrorismefinancieringsrisico's en controls bij relevante medewerkers • Geen trainingen op het gebied van AML/CFT beschikbaar
• Er is een SIRA uitgevoerd, echter onvoldoende diepgang in scenario's en risico's • Scenario's en risico's uit de SIRA zijn niet vertaald naar transactiemonitoring beleid en procedures • Er zijn clientsicoprofielen, echter geen ex-ante transactierisicoprofielen	• Instelling heeft in opzet transactiemonitoring beleid en procedures, echter dit is te algemeen en onvoldoende uitgewerkt waardoor materiële onderdelen ontbreken	• Systeem voor transactiemonitoring sluit onvoldoende aan bij het risicoprofiel van de instelling • Instelling hanteert een te beperkt aantal (enkele) AML/CFT indicatoren en business rules om ongebruikelijke transacties te herkennen	• Alert afhandelings- en meldproces is capaciteit gedreven en niet risico gebaseerd • Afhandeling alerts wordt onvoldoende vastgelegd (geen overwegingen / conclusies)en er vindt geen opvolging plaats • (Voorgenomen) ongebruikelijke transacties worden incidenteel (onverwijld) gemeld aan de FIU	• Functiescheiding 1e, 2e en 3e lijn in opzet aanwezig • Onvoldoende beschrijving van de verantwoordelijkheden van 1e, 2e en 3e • In opzet is er second line monitoring (SLM) en onafhankelijke interne controle, echter in werking onvoldoende in frequentie en/of kwaliteit (SLM programma, testwerkzaamheden, rapportage) • Periodieke managementinformatie over uitkomsten TM in beperkte mate beschikbaar	• Onvoldoende kennis en awareness ten aanzien van witwas en/of terrorismefinancieringsrisico's en controls bij de medewerkers • Incidentele trainingen op het gebied van AML/CFT (reactief bv naar aanleiding van audit bevindingen of incidenten) en/of inhoud is van onvoldoende kwaliteit (ontbreken materiële onderdelen)
• Er is een SIRA uitgevoerd waarin voldoende diepgang zit in scenario's en risico's • Scenario's en risico's uit de SIRA zijn in voldoende mate vertaald naar transactiemonitoring beleid en procedures, echter op een generiek niveau • Instelling heeft clienten vertaald naar groepen van transactierisico profielen	• Instelling heeft in opzet en bestaan transactiemonitoring beleid en procedures welke voldoende uitgewerkt zijn en waarin materiële onderdelen aanwezig zijn • Instelling is op basis van het raamwerk in staat om de transacties op een juiste, tijdige en volledige manier te monitoren	• Systeem voor transactiemonitoring is voldoende passend bij risicoprofiel van de instelling • De instelling hanteert volledige set aan AML/CFT indicatoren en business rules om ongebruikelijke transacties te herkennen • Aanpassen van systeem en business rules naar aanleiding van ontwikkelingen t.a.v. witwassen en terrorismefinanciering gebeurt reactief	• Alert afhandelings- en meldproces is voldoende gedefinieerd, inclusief escalatie naar de 2e lijn • Afhandeling transactiemonitoring alerts wordt voldoende vastgelegd en opgevolgd • (Voorgenomen) ongebruikelijke transacties worden onverwijld gemeld aan de FIU	• Functiescheiding 1e, 2e en 3e lijn is in opzet en bestaan aanwezig • Verantwoordelijkheden van 1e, 2e en 3e lijn zijn voldoende beschreven • In opzet en bestaan is er second line monitoring en onafhankelijke interne controle, voldoende in frequentie en kwaliteit (werking suboptimaal) • Bevindingen uit 2e en 3e lijns monitoring activiteiten worden adequaat opgevolgd door de 1e lijn (reactief) • Managementinformatie over uitkomsten toereikend, in de basis sturend	• Voldoende kennis en awareness ten aanzien van witwas- en terrorismefinancieringsrisico's en controls bij alle medewerkers incl. senior management • Periodiek worden (verplichte) trainingen op het gebied van AML/CFT aangeboden en inhoud is van voldoende kwaliteit (bevat materiële onderdelen)
• Scenario's en risico's in de SIRA zijn een juiste en volledige afspiegeling van het specifieke risicoprofiel van de instelling • SIRA wordt 'a tempo' aangepast naar aanleiding van nieuwe ontwikkelingen op het gebied van witwassen en terrorismefinanciering • SIRA vormt de basis voor het periodiek updaten van het transactiemonitoring raamwerk • Gedetailleerde ex-ante transactierisico profielen	• Transactiemonitoring beleid en procedures zijn zichtbaar geincorporeerd in het werkproces van de instelling en de effectieve werking ervan is aangetoond • Transactiemonitoring beleid en procedures zijn actueel en volledig afgestemd op de meest recente ontwikkelingen op het gebied van witwassen en terrorismefinanciering	• Instelling heeft een geautomatiseerd en zelflerend transactiemonitoring systeem passend bij risicoprofiel van de instelling • Er wordt proactief ingespeeld op ontwikkelingen op het gebied van witwassen en terrorismefinanciering en daarmee aanpassingen van systeem en business rules • Instelling maakt gebruik van backtesting bij het toevoegen van nieuwe AML/CFT indicatoren en business rules • Er wordt structureel gebruik van patroonherkenning en netwerkanalyses om ongebruikelijke transacties te herkennen	• Alert afhandelings- en meldproces is gedefinieerd en er wordt proactief ingespeeld op ontwikkelingen m.b.t. witwassen en terrorismefinanciering • Afhandeling transactiemonitoring alerts wordt consequent vastgelegd en opgevolgd • Instelling fungeert als volwaardige gesprekspartner van opsporingsautoriteiten en ketenpartners	• Functiescheiding 1e, 2e en 3e lijn is in opzet, bestaan aanwezig en effectieve werking is aangetoond • Verantwoordelijkheden van 1e , 2e en 3e lijn zijn helder en volledig beschreven en 1e lijn neemt proactief eindverantwoordelijkheid voor transactiemonitoring • Second line monitoring wordt hoog frequent uitgevoerd en is van goede kwaliteit (effectieve werking) • Onafhankelijke interne controle op transactiemonitoring vindt regelmatig plaats en is van goede kwaliteit (effectieve werking) • Uitgebreide managementinformatie over TM uitkomsten beschikbaar, werkt sterk sturend	• Kennis en awareness ten aanzien van witwas- en terrorismefinancieringsrisico's en controls is in hoge mate aanwezig bij alle medewerkers en senior management • Senior management toont een voorbeeldhouding • Periodiek worden (verplichte) trainingen op het gebied van AML/CFT aangeboden waarvan de inhoud is toegesneden op casuïstiek relevant voor instelling • Nieuwe ontwikkelingen op het gebied van witwassen en terrorismefinanciering worden direct vertaald naar de organisatie

Uit het onderzoek is gebleken dat er verschillen bestaan tussen de scores van de onderzochte banken op alle zes toetsingselementen. In hoofdstuk 3 hierna leest u per toetsingselement onze uitkomsten en voorbeelden (goede en minder goede voorbeelden van de invulling van de norm). De goede voorbeelden illustreren hoe een bank erin geslaagd is om op dat gebied een gele of groene score te halen.

3. Guidance

3.1 SIRA

DNB heeft geconstateerd dat alle onderzochte banken hun financieel economische criminaliteitsrisico's die uit de SIRA voortvloeien niet voldoende doorvertalen naar het transactiemonitoringsproces.

DNB verwacht dat een bank borgt dat de uitkomsten van haar SIRA worden doorvertaald in haar beleid en procedures omtrent het transactiemonitoringsproces. Uw bank heeft immers te maken met verschillende integriteitrisico's, die afhankelijk zijn van de aard van uw dienstverlening en uw cliëntenportfolio. Integriteitrisico's worden in de wet omschreven als: gevaar voor aantasting van de reputatie of bestaande of toekomstige bedreiging van vermogen of resultaat van een financiële onderneming als gevolg van een ontoereikende naleving van hetgeen bij of krachtens enig wettelijk voorschrift is voorgeschreven".[15] Belangrijke integriteitrisico's voor banken zijn financieel-economische criminaliteitsrisico's, te weten witwassen, financieren van terrorisme, niet-naleving van sancties, corruptie/omkoping en belangenverstrengeling. Om te waarborgen dat uw bank de integriteitrisico's adequaat beheerst, heeft de wetgever verschillende verplichtingen opgenomen waaraan moet worden voldaan. Hierbij speelt de SIRA[16] een centrale rol. Deze risicoanalyse op organisatieniveau legt de basis voor uw (periodiek te herzien) integriteitbeleid en dient te worden vertaald naar procedures en maatregelen. De uitkomsten van de SIRA moeten binnen uw hele organisatie leven en moeten ook terug te vinden zijn in de risicoanalyses op cliëntniveau. In subparagraaf hieronder vindt u een voorbeeld.

3.1.1 Risicoprofiel: verwacht transactiegedrag

[15] Op grond van artikel 10, lid 1 en 2 Bpr dient een instelling te beschikken over een systematische integriteitrisicoanalyse en indien in de analyse (rest)risico's gesignaleerd worden, dienen deze omgezet te worden in beleid, procedures en maatregelen.
[16] Voor nadere toelichting op de SIRA zie het document: *De integriteitrisicoanalyse, meer waar dat moet, minder waar dat kan*, te raadplegen via http://www.toezicht.dnb.nl/2/50-234066.jsp

DNB constateert dat de onderzochte banken bij de bepaling van het risicoprofiel van de cliënt het verwachte transactiegedrag van de cliënt niet meenemen.

Op grond van de integriteitswetgeving moeten banken bij het cliëntenonderzoek een risicoprofiel opstellen van de cliënt. Hierbij worden verschillende factoren van de cliënt beoordeeld (zoals de sector(en) en landen waarin de cliënt actief is, de bij de bank afgenomen producten en diensten). Op basis hiervan bepaalt u de risicoclassificatie van uw cliënt. De review van de cliënt en actualisatie van de cliëntgegevens vindt vervolgens periodiek (en ook tussentijds op basis van relevante gebeurtenissen) plaats; hierbij is de risicoclassificatie een belangrijk uitgangspunt. Deze risicoclassificatie van de cliënt gebruikt u ook voor uw transactiemonitoringsproces. Wanneer cliënten geen risicoclassificatie hebben, is het niet mogelijk het transactiemonitoringssysteem risicogebaseerd in te richten. Op basis van de kennis over de cliënt, maakt u ook het verwachte transactiegedrag inzichtelijk om te zorgen dat de tijdens de duur van de relatie verrichte transacties overeenkomen met de kennis die u heeft van uw cliënt en zijn of haar risicoprofiel.

Om het transactiegedrag te bepalen kunt u als bank onder meer informatie inwinnen over:
- (verwachte) inkomende en uitgaande geldstromen, inclusief volumes, soorten tegenpartijen en landen
- soorten transacties, distributiekanalen en de mate waarin deze zullen voorkomen (creditcard, girale overboekingen, cash opnames en stortingen, financieringen, vreemde valuta, et cetera)

De bank toetst periodiek of de cliënt nog voldoet aan het risicoprofiel dat is opgesteld bij aanvang van de dienstverlening. Banken kunnen immers alleen ongebruikelijke transacties opmerken als ze een goed beeld hebben van de activiteiten van de cliënt. Indien uit specifieke transacties of het transactieverloop op de rekening blijkt dat het transactiegedrag van de cliënt afwijkt van het risicoprofiel, gaat de bank na of mogelijk sprake is van ongebruikelijke transacties, en of verdere acties moeten worden ondernomen, zoals bijvoorbeeld een herbeoordeling van het risicoprofiel. Daarbij is een goede samenwerking tussen verschillende personen of afdelingen essentieel.

Aangezien het verwachte transactiegedrag bij aanvang van de zakelijke relatie met de cliënt wordt opgesteld, is de bank primair afhankelijk van gegevens die door de cliënt over de verwachte transacties worden verstrekt. Verwacht mag worden dat banken na een aantal maanden (bijvoorbeeld na een kwartaal) beoordelen of het verwachte transactiegedrag (in hoge mate) overeenkomt met de werkelijkheid. Deze informatie kan ter verificatie worden vergeleken met transactiegedrag van cliënten in vergelijkbare sectoren of cliënten met een vergelijkbaar risicoprofiel.

DNB constateerde dat de meeste onderzochte banken de uitkomsten vanuit hun SIRA niet hadden doorvertaald naar hun transactiemonitoringsproces. Een onderzochte bank deed relatief veel zaken met een verhoogd risicoland, wat wel uit de SIRA kwam, maar niet was opgenomen in haar transactiemonitoringsproces. DNB constateerde bovendien dat de onderzochte banken in hun SIRA onderscheid maakten tussen witwassen en terrorismefinanciering, maar dat dit niet tot uitdrukking kwam in het transactiemonitoringsproces. Zo bleek dat onderzochte banken nauwelijks aandacht hadden voor terrorismefinancieringsscenario's.

3.2 **Beleid en procedures**

Uit het onderzoek is gebleken dat banken niet voldoende beleid voor transactiemonitoring hebben en dit derhalve ook niet hebben uitgewerkt in onderliggende procedures en werkprocessen.

Voor het detecteren van (potentieel) ongebruikelijke transactiepatronen of transacties, waarbij mogelijk sprake is van witwassen of terrorismefinanciering, moet een bank beschikken over beleid, procedures en processen. Dit is een wettelijk vereiste. Om te komen tot effectief beleid staat hier onder andere in dat een risicobeoordeling en risicoprofiel worden gemaakt van iedere cliënt en dat dat risicoprofiel ook een omschrijving omvat van het verwachte transactiegedrag: de bank legt expliciet vast dat een risicoscore en cliëntrisicoprofiel wordt gemaakt van iedere cliënt, inclusief een omschrijving van de verwachte cliëntactiviteiten en transacties, gegeven de afgenomen producten en diensten. Vervolgens wordt in procedures en werkprocessen dit beleid nader uitgewerkt, met name hoe in voorkomende gevallen door de organisatie en haar medewerkers dient te worden gehandeld.

DNB verwacht dat u de uitkomsten van uw SIRA zichtbaar vertaalt naar uw beleid en procedures ten aanzien van uw transactiemonitoringsproces.

Good practice
Een bank beschikt over een expliciet transactiemonitoringsbeleid en een procedure voor transactiemonitoring, zodat duidelijk wordt op welke wijze de bank operationeel invulling geeft aan de wijze van transactiemonitoring. Daarbij kunnen de belangrijkste uitkomsten uit de SIRA worden herleid naar haar transactiemonitoringsproces.

3.3 Het transactiemonitoringssysteem

De onderzochte banken hebben een geautomatiseerd transactiemonitoringssysteem, maar zij beschikken veelal niet over een onderbouwde en toereikende set aan business rules (detectieregels met scenario's en grenswaarden) om witwas- en terrorismefinancieringsrisico's te detecteren.

DNB verwacht dat een bank beschikt over een (geautomatiseerd) transactiemonitoringssysteem dat passend is bij haar eigen risicoprofiel. Doordat de hoeveelheid data waar een bank over beschikt en kan beschikken steeds groter wordt, gebruikt de bank in principe een geautomatiseerd systeem voor de transactiemonitoring. Het transactiemonitoringssysteem is bij voorkeur een zelflerend systeem waarin data vanuit meerdere bronnen (zoals open bronnen en gesloten bronnen) wordt geïmporteerd om (patronen van) transacties te detecteren die mogelijk verband houden met witwassen of terrorismefinanciering.

De vraag of een bank moet beschikken over een geautomatiseerd systeem voor (post-event) transactiemonitoring, is niet zonder meer met *ja* of *nee* te beantwoorden. Om te bepalen op welke wijze een bank moet monitoren, zal een afweging gemaakt moeten worden tussen kosten, risico's en de in te zetten methode. Dat hangt sterk af van de aard en omvang van de instelling, en van het aantal transacties dat dagelijks door de instelling wordt uitgevoerd. Van belang is op te merken dat de wetgever niet eist dat transactiemonitoring geautomatiseerd moet gebeuren. DNB verwacht dat een bank in staat is om uit te leggen waarom een handmatig transactiemonitoringssysteem nog volstaat indien de bank (tien)duizenden transacties op een dag verricht. Dat kan bijvoorbeeld als de bank kan aantonen dat zij beschikt over voldoende geschikte resources om handmatig te monitoren.

3.3.1 Gebruik van business rules

Tijdens het onderzoek constateerde DNB dat banken niet goed in staat waren een onderbouwing te geven van de gebruikte business rules. Tevens bleek dat banken beschikten over een te beperkt aantal business rules om ongebruikelijke transacties in relatie tot witwassen of terrorismefinanciering vast te stellen. DNB constateerde verder dat het periodieke onderhoud en het testen van de business rules bij alle onderzochte banken tekortschoot of zelfs geheel ontbrak.

Zoals uiteengezet in paragraaf 2.1, maakt een bank gebruik van een set aan business rules om ongebruikelijke transacties te detecteren. Met business rules wordt bedoeld de set aan detectieregels die in het transactiemonitoringssysteem wordt toegepast, die bestaan uit de toegepaste scenario's en bepaalde grenswaarden (zoals bedragen in valuta en aantallen transacties of combinaties van bedragen en aantallen transacties). De wijze waarop deze business rules zijn bepaald, is essentieel voor de effectiviteit van het transactiemonitoringsproces van een bank. DNB verwacht dat de in het transactiemonitoringssysteem opgenomen business rules risicogebaseerd zijn opgesteld en herleidbaar zijn tot de uitkomsten van de SIRA. Herleidbaar wil zeggen dat er een verband bestaat tussen de business rules en de restrisico's zoals deze uit de SIRA volgen. Bij het opstellen van de business rules wordt rekening gehouden met verschillende factoren, zoals:

- het soort cliënt, bijvoorbeeld een PEP
- het cliëntsegment, bijvoorbeeld onderscheid private banking of retail, of gesegmenteerde andere doelgroepen, zoals professionele sportbeoefenaars
- het land waar de transactie naartoe gaat of vandaan komt, bijvoorbeeld hoogrisico land, EU of non-EU land
- het product, bijvoorbeeld sparen, vastgoedfinanciering of handelsfinanciering
- de distributiekanalen, bijvoorbeeld fysieke aanwezigheid van de klant of online
- de aard van de transacties, bijvoorbeeld giraal of contant

De bank zorgt voor voldoende diversificatie in de business rules al naar gelang sprake is van meerdere cliëntsegmenten, landen, producten, distributiekanalen en soorten transacties.

Een voorbeeld van een business rule binnen het retailsegement is de volgende: cliënten binnen een bepaalde leeftijdscategorie, 18 – 25 jaar, met bepaalde grenswaarden van omvang van girale transacties en de frequentie van transacties.

Verder wordt bij het bepalen van de business rules ook gebruik gemaakt van vergelijkingen met andere transacties van de cliënt, bijvoorbeeld transacties over eerdere perioden, in relatie tot de maturiteit van de klantrelatie (dus hoe lang de klant al klant is bij uw bank) of leeftijdsgroep, de risicopostcode en/of risicoland. Van belang is dat een bank documenteert op welke wijze zij tot een definitie van een business rule is gekomen, en hoe de bank doorlopend haar business rules onderhoudt en periodiek test, bijvoorbeeld door gebruik te maken van *backtesting* (zie verder 3.3.3). Met backtesting wordt bedoeld het achteraf toetsen van de effectiviteit van de toegepaste business rules (en waar nodig de business rules aanpassen).

Good practice
Uit de uitkomsten van de SIRA van een bank volgde dat zij binnen het private banking segment veel buitenlandse politici bediende. De bank anticipeerde hierop in haar transactiemonitoringsproces door voor PEP's[17] een specifieke business rule te implementeren.

3.3.2 Business rules in relatie tot terrorismefinanciering

DNB constateerde bij een aantal onderzochte banken dat er nagenoeg geen business rules in het systeem waren voor detectie van terrorismefinanciering. DNB verwacht dat banken specifiek indicatoren voor terrorismefinanciering vertaald hebben in business rules die vervolgens in hun transactiemonitoringssystemen zijn opgenomen.

Tijdens de onderzoeken is gebleken dat in de transactiemonitoringssystemen veelal gebruik wordt gemaakt van hoge transactielimieten, terwijl terrorismefinanciering vaak gekenmerkt wordt door transacties met lage bedragen. Aangezien uitsluitend een laag transactiebedrag niet duidt op terrorismefinanciering, zouden banken dit moeten koppelen aan andere indicatoren van terrorismefinanciering (combinaties van verschillende indicatoren). Hierbij kan gedacht worden aan combinaties van lagere grensbedragen voor transacties met terrorisme gerelateerde landen in samenhang met bepaalde soorten cliënten, zoals stichtingen. Daarnaast kan op basis van het risicoprofiel van een cliënt een lagere limiet worden vastgesteld: voor een voor terrorismefinanciering hoogrisico cliënt is een relatief lagere limiet in het transactiemonitoringssysteem ingesteld.

Tijdens de onderzoeken is gebleken dat de selectie van risicolanden die in verband worden gebracht met terrorismefinanciering beperkt dan wel niet actueel is. Veelal is een risicolandenlijst opgesteld aan de hand van de FATF-waarschuwingslijsten en de Corruption Perception Index (CPI), maar is geen rekening gehouden met landen die in verband kunnen worden gebracht met terrorisme en terrorismefinanciering. Zo wijzen recente publicaties op mogelijke financiering van dubieuze Nederlandse charitatieve instellingen, kerkgenootschappen en/of non-profit organisaties, vaak in de vorm van stichtingen door personen of instellingen uit bepaalde landen, zoals de Golfstaten. Niet alle banken hebben deze landen (in combinatie met stichtingen) in de risicolandenlijst opgenomen. DNB verwacht dat banken de ontwikkelingen op het gebied van terrorisme en terrorismefinanciering nauwgezet volgen, haar risicolandenlijst hierop aanpassen en dit vervolgens vertalen naar haar transactiemonitoringssysteem.

3.3.3 Periodieke evaluatie van business rules: back testing

DNB constateerde dat banken hun business rules niet periodiek onderhouden noch testen op effectiviteit.

DNB verwacht dat banken de effectiviteit van het transactiemonitoringssysteem op het gewenste niveau krijgen en behouden. In dit verband verwacht DNB dat het systeem periodiek wordt

[17] PEP staat voor *Politically Exposed Persons*: voor deze cliënten dient het verscherpt cliënentonderzoek te worden uitgevoerd.

geëvalueerd. Doel van een dergelijke periodieke evaluatie is te beoordelen of in gebruik zijnde business rules te grofmazig zijn ingesteld, bijvoorbeeld of er sprake is van (te) hoge grenswaarden, waardoor nauwelijks sprake is van alerts op een bepaalde business rule. Deze evaluatie kan plaatsvinden door middel van het zogenoemde *back testing*. Op basis van de uitkomsten van de uitgevoerde back test brengt de bank eventuele aanpassingen of toevoegingen aan in de business rules van haar transactiemonitoringssysteem. Een bank kan verschillende manieren van back testing toepassen, zoals het uitvoeren van een back test waarbij business rules met veel of alleen maar *false positive* alerts worden geanalyseerd. Het doel van deze test is onder meer voor de toekomst meer *true positive* alerts te generen op de business rules, door deze na de test dusdanig aan te passen dat ze het gewenste resultaat bereiken. Doel van de back test is om de effectiviteit van business rules te testen.

3.3.4 Data-analyse

DNB constateert dat banken verschillende initiatieven nemen om te komen tot meer geavanceerde technologieën om transactiedata en cliëntdata te analyseren. Banken beschikken over een grote hoeveelheid (historische) data die kan worden ingezet om het transactiegedrag van individuele cliënten, dan wel transactiepatronen en netwerken van cliënten beter te kunnen voorspellen, te analyseren en uiteindelijk ook te beoordelen. DNB moedigt banken aan geavanceerde data-analyse en *artificial intelligence*[18] in te zetten bij de uitvoering van haar transactiemonitoring. Geavanceerde technologie (zoals gebruik van 'big data' en data modeling technieken) vergroot de mogelijkheden van een instelling om ongebruikelijke transactiepatronen en afwijkend transactiegedrag op te sporen.

Door het gebruik van meer geavanceerde technologie in haar transactiemonitoringsproces zal een bank haar witwas- en terrorismefinancieringsrisico verminderen: de bank is effectiever in staat om mogelijk ongebruikelijk gedrag van een cliënt te detecteren. De technologie kan zich richten op verschillende onderdelen van beschikbare data, zoals:

- door middel van *tekst mining van free-form*[19] tekst doorzoeken op kernwoorden en andere belangrijke woordpatronen in transactiegegevens (voor terrorismefinanciering bijvoorbeeld "Family Support" of "Gift"[20])
- patroonanalyses en netwerkanalyses uitvoeren om onderlinge verbanden tussen transacties te detecteren.

DNB trof het navolgende voorbeeld aan als een 'good practice' van data-analyse.

Good practice
Een bank beschikt over een zelflerend systeem (gebaseerd op 'artificial intelligence') waarin data vanuit meerdere bronnen geïmporteerd wordt om vervolgens real-time geldstromen tussen individuen en organisaties in kaart te brengen. Hierbij zijn historische transacties bepalend om het mogelijk ongebruikelijke karakter van te verwachten transacties vast te stellen.

3.3.5 Transactiepatroonanalyses

Met behulp van het transactiemonitoringssysteem kunnen banken transactiepatronen of netwerken en combinaties van transacties detecteren. Hieronder wordt verstaan een samenstel van transacties van een of meerdere cliënten die op geaggregeerd niveau op witwassen of terrorismefinanciering (kunnen) duiden. DNB moedigt het gebruik van voorspellende data-analyse (*predictive analytics*) aan om de effectiviteit van de transactiemonitoring te vergroten. Predictive analytics zou de mogelijkheid kunnen bieden om volledig geautomatiseerd en standaard bredere transactiepatronen en -structuren en netwerken van transacties te detecteren.

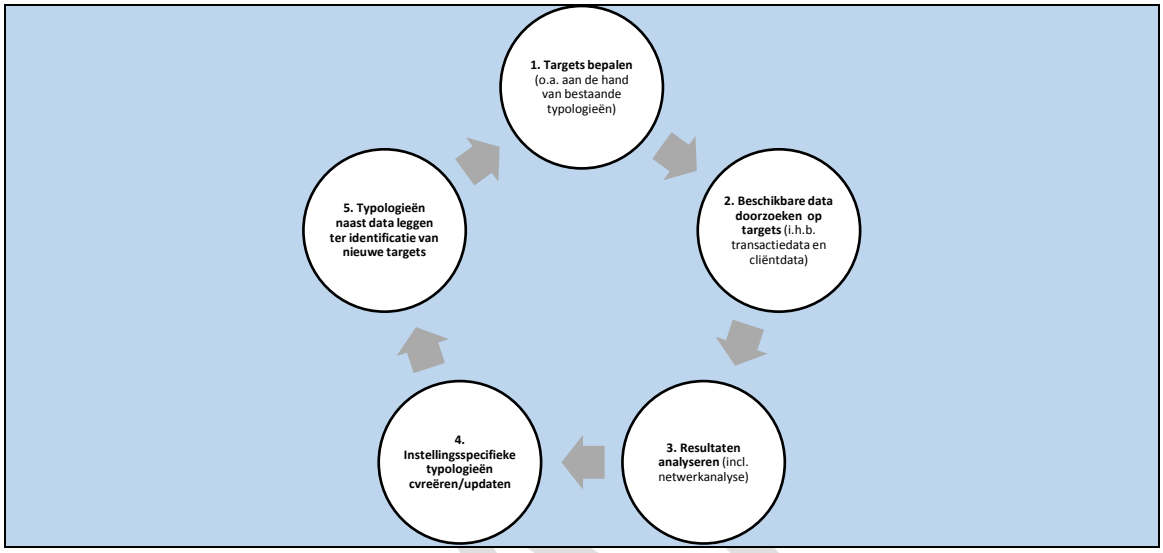
3.3.6 Data-analyse in relatie tot terrorismefinanciering

Data-analyse met behulp van targets[21] en typologieën[22] speelt een centrale rol bij het bestrijden van terrorismefinanciering. Banken beschikken over een grote hoeveelheid data en informatie waarmee

[18] De toepassing van kunstmatige intelligentie, waarbij aan de hand van beschikbare data de computer zelf algoritmen ontwikkelt. Een algoritme is een rekenwijze voor het berekenen van bepaalde grootheden en functies.
[19] Transacties omvatten teksten in zogenoemde *vrije format* velden: met behulp van software-technieken kan waardevolle informatie gehaald worden uit grote hoeveelheden tekstmateriaal. Met deze technieken wordt gepoogd patronen en tendensen te ontwaren. Concreet gaat men teksten softwarematig structureren en ontleden, transformeren, vervolgens inbrengen in databanken, en ten slotte evalueren en interpreteren.
[20] Bron: The Egmont Group of Financial Intelligence Units, A global Financial Typology of Foreign Terrorist Fighters; November 2015
[21] Targets zijn subjecten die in verband worden gebracht met (de financiering van) terrorisme.
[22] (Groepen van) kenmerken die duiden op het financieren van terrorisme.

terrorismefinanciering kan worden gedetecteerd. Van belang is om een proces in te richten waarbinnen data continu wordt geanalyseerd om te komen tot genoemde targets en typologieën.

Hieronder is een voorbeeld weergegeven van een processchema[23] afkomstig van een geldtransactiekantoor, op grond waarvan het geldtransactiekantoor de gedragingen van targets analyseert en daarmee nieuwe typologieën identificeert. Een dergelijke analyse kan ook voor banken nuttig zijn.



Stap 1: Op basis van openbare informatie of bestaande typologieën is een target in beeld gekomen. Stap 2: De bank doorzoekt of de target voorkomt in haar bestanden. Stap 3: Indien de target voorkomt in de bestanden, worden de transacties geanalyseerd waarbij gekeken wordt naar bijvoorbeeld de specifieke kenmerken van de uitgevoerde transacties, betrokken landen en/of gerelateerde personen of entiteiten. Stap 4: Indien is vastgesteld dat deze nieuwe transactiepatronen kunnen duiden op terrorismefinanciering, worden deze patronen vertaald in nieuwe typologieën. Stap 5: Tot slot vertaalt de bank de typologieën in scenario's voor haar transactiemonitoring. Met de transactiemonitoring worden vervolgens weer nieuwe targets geïdentificeerd en vangt het proces weer van voren af aan. Dit continue proces is zeer waardevol gebleken voor het detecteren van ongebruikelijke transacties.

3.3.7 IT-beheersingsmaatregelen transactiemonitoring

DNB heeft geconstateerd dat de kwaliteit van de data die gebruikt wordt in het transactiemonitoringssysteem niet altijd is geborgd, bijvoorbeeld doordat technische functiescheiding ontbrak.

DNB verwacht dat de kwaliteit van de data bij het gebruik van het geautomatiseerde transactiemonitoringssysteem adequaat is geborgd. Daarbij is (technische) functiescheiding een wezenlijk onderdeel van de beheersing van processen in betalingsverkeer om te zorgen dat geen ongewenste en ongecontroleerde aanpassingen plaats vinden. Functiescheiding kan op meerdere manieren plaatsvinden, dat wil zeggen functiescheiding tussen invoeren en autorisatie, maar ook technische functiescheiding tussen de testomgeving en de productieomgeving.

Tijdens het onderzoek heeft DNB bij enkele banken vastgesteld dat de ontwikkelaars van business rules toegang hebben tot de productie-, de test- en acceptatieomgeving van het transactiemonitoringssysteem. Daarmee zijn ontwikkelaars in staat om met hun rechten direct, zonder tussenkomst van de verantwoordelijke eigenaar, de business rules voor transactiemonitoring in de productieomgeving aan te passen. Het zonder controle doorvoeren van aanpassingen door ontwikkelaars van business rules kan alleen gewaarborgd worden door de interne procedures na te leven (en periodieke controle hierop). Daarnaast is een belangrijke beheersmaatregel dat de bank

[23] Bron: Western Union.

beschikt over een end-to-end controle tussen bronsystemen en het transactiemonitoringssysteem. Als deze end-to-end controle ontbreekt, is er geen controle op de volledigheid van de transacties uit de bronsystemen die worden ingelezen in het transactiemonitoringssysteem. Daarmee bestaat het risico dat niet alle transacties worden gemonitord. Tevens wordt hierdoor een onvolledige historie opgebouwd.

Tijdens het onderzoek constateerde DNB dat bij het merendeel van de onderzochte banken een zogenoemd *key-man exposure*-risico aanwezig was met betrekking tot het transactiemonitoringssysteem: de kennis van het systeem was bij één of twee medewerkers aanwezig. Het risico van kennisverlies is groot als weinig medewerkers kennis hebben van de systemen, wat als gevolg kan hebben dat deze systemen niet goed onderhouden kunnen worden, of dat incidenten niet opgelost kunnen worden.

3.4 Alertafhandelings- en meldproces

Zoals eerder in dit document gesteld, moeten banken een verrichte of voorgenomen ongebruikelijke transactie onverwijld melden aan de FIU-NL zodra het ongebruikelijke karakter van de transactie bekend is geworden. Het melden van ongebruikelijke transacties aan de FIU-NL is een belangrijk onderdeel van de bestrijding van witwassen en terrorismefinanciering. De FIU-NL onderzoekt alle gemelde transacties. Indien dit onderzoek ertoe leidt dat de gemelde transactie verdacht verklaard wordt, wordt deze transactie doorgemeld aan de opsporingsinstanties. Zo kunnen uw meldingen van ongebruikelijke transacties leiden tot strafrechtelijk onderzoek. De meldingsplicht vormt daarmee een essentiële rol voor opsporen van witwassen en financiering van terrorisme.

De onderzochte banken bleken ongebruikelijke voorgenomen transacties of uitgevoerde transacties niet altijd onverwijld en volledig aan de FIU-NL te melden conform een gedocumenteerd meldproces. Ook het alertafhandelingsproces en meldproces bleken niet altijd adequaat te zijn gedocumenteerd. In onderstaande paragrafen leest u onze uitkomsten en handvatten voor het alertafhandelingsproces en het meldproces.

3.4.1 Alertafhandelingsproces

Het alertafhandelingsproces bleek niet altijd adequaat te zijn gedocumenteerd: met name overwegingen om alerts en conclusies te sluiten of te escaleren ontbraken.

Een bank beschikt over procedures en werkprocessen om alerts te beoordelen en af te handelen. DNB verwacht dat een bank beschikt over een workflow-managementsysteem dat de bank voldoende inzicht geeft in de *audit trail* en doorlooptijden van vervolgacties naar aanleiding van een alert. Het gevolg is dat de doorlooptijden vanaf het genereren van de alerts tot het sturen van een (eventueel) informatieverzoek aan de cliënt tot aan de onverwijlde melding aan de FIU-NL beperkt blijven en dat de juiste prioriteiten in de afhandeling van de alerts kunnen worden gesteld.

Voorts verwacht DNB dat een bank voor iedere alert vastlegt wat de overwegingen en conclusies zijn om een alert te sluiten of om de transactie als ongebruikelijk te melden aan de FIU-NL. Bij het alert onderzoek is het van belang om niet alleen te kijken of de betreffende transactie past in het transactiegedrag van cliënt; ook is het van belang of een dergelijke transactie logisch en plausibel is voor het soort cliënt, de sector waarin de cliënt actief is en bijvoorbeeld het coupuregebruik bij contante transacties. Immers, de transacties van een cliënt die alleen maar witwastransacties en / of transacties in verband met terrorismefinanciering uitvoert, zullen altijd binnen het transactiepatroon vallen.

DNB constateert dat escalatie van alerts naar de 2e lijn veelal ontbrak: compliance was veelal niet betrokken bij het alertafhandelingsproces. Van belang is dat banken concrete handvatten bieden wanneer escalatie vanuit de 1e lijn naar de 2e lijn (Compliance) moet plaatsvinden. Deze handvatten ontbraken nu veelal.

Ook verwacht DNB dat de bank beschikt over een adequate onderbouwing van de conclusie van een alert *om juist niet* over te gaan tot melding aan FIU-NL.

DNB trof de volgende voorbeelden aan zoals het niet moet:

Bij een onderzochte bank wordt een alert gegenereerd op basis van twee contante stortingen door een tweedehands autobedrijf. De bank sluit het alert om twee redenen: ten eerste op basis van het feit dat de contante transacties passen binnen het transactiepatroon van de cliënt (er vonden immers vaker contante transacties plaats), en bovendien vanwege het feit dat de hoogte van de transacties overeenkomt met de prijzen van de tweedehands auto's (circa EUR 20.000). In het alertdossier is geen onderbouwing gegeven of het gebruikelijk is om auto's in deze prijsklasse contant af te rekenen. Uit een door DNB opgevraagd transactieoverzicht volgt dat in negen maanden tijd meer dan EUR 550.000 contant bij de bank is gestort. Naar de plausibiliteit van de contante storingen heeft de bank geen (zichtbaar) verder onderzoek gedaan.

Het sluiten van de alert, alleen omdat contant geld past in het transactieprofiel geldt als onvoldoende onderzoek. Frequentie van stortingen en of deze qua omvang aannemelijk zijn, zijn factoren die meegenomen moeten worden in het onderzoek. DNB verwacht in een dergelijk geval dan ook ten minste dat de bank een uitgebreidere analyse doet naar de contante stortingen door een cliënt, om te komen tot een onderbouwde conclusie over het al dan niet melden bij de FIU-NL.

Bij een onderzochte bank constateerde DNB het volgende: de afgelopen periode heeft een particuliere cliënt 20 kasstortingen verricht voor een totaalbedrag van EUR 50.000. De klant doet een kasstoring van EUR 25.000, die vervolgens direct van de betaalrekening van de klant wordt afgeboekt. Op dezelfde dag verricht de klant weer een kasstorting van EUR 20.000. Ook worden op dezelfde dag verschillende stortingen gedaan met EUR 500-biljetten. De alert-behandelaar concludeert dat de transacties niet meldenswaardig zijn, echter uit het alertdossier blijkt niet hoe tot deze conclusie is gekomen.

3.4.2 Capaciteit en middelen om alerts te beoordelen

DNB verwacht dat banken voldoende capaciteit en middelen beschikbaar hebben om risicogebaseerd hun transactiemonitoring en in het bijzonder hun alertafhandeling te verrichten. Daarbij dient de afdeling die belast is met alertafhandeling te beschikken over realistische targets, gezien de omvang en het risicoprofiel van de instelling. Om dit te bewerkstelligen kan de instelling zogenoemde kpi's opstellen waarin tijdsinschattingen voor de afhandeling van ieder type alert zijn gedefinieerd. Het spreekt voor zich dat deze ook periodiek worden geëvalueerd.

Good practice
Uit het thema-onderzoek bleek dat een van de onderzochte banken in de praktijk bij de alertafhandeling het volgende uitgangspunt hanteert "kwaliteit gaat voor snelheid[24]". Analisten van alerts krijgen voldoende tijd voor een gedegen onderzoek en vastlegging van hun onderzoek, en hebben daarbij de beschikking over voldoende middelen en toegang tot interne en externe systemen en informatiebronnen. Onderdeel daarvan is dat de analisten bij de beoordeling van alerts het cliëntendossier moeten kunnen raadplegen. Informatie in het cliëntendossier kan aanvullende informatie geven om een transactie met een verhoogd risico voor witwassen en terrorismefinanciering te detecteren. Met informatie uit het cliëntendossier kan de analist bijvoorbeeld beoordelen of de transacties passen bij de activiteiten van een cliënt. Een andere informatiebron is bijvoorbeeld inzicht in de gebruikte coupures voor de opnames of stortingen.

3.4.3 Alerts in relatie tot risico op terrorismefinanciering

DNB verwacht bij het detecteren van terrorismefinanciering dat een bank beschikt over een lijst met *red flags* en mogelijke indicatoren die kunnen duiden op terrorismefinanciering. Deze lijst is toegespitst op het risicoprofiel van de bank en – indien mogelijk – worden indicatoren vertaald naar business rules om risico's op terrorismefinanciering te detecteren.

Good practice: Publieke informatie mogelijke terrorismefinanciering
Op basis van berichtgeving uit de pers signaleert een bank dat een cliënt mogelijk banden zou hebben met jihadstrijders. Hierop heeft de instelling een alert aangemaakt. Dit is een goed voorbeeld van een instelling die de ontwikkelingen via de media nauwgezet volgt en hierop actie onderneemt door een alert op te stellen voor deze cliënt.

[24] Snelheid wil zeggen zo snel mogelijk afwerken van de alerts teneinde achterstanden te voorkomen

Good practice: De bank heeft een alert via een pintransactie in Oost-Turkije
Een bank wordt geconfronteerd met een door een cliënt uitgevoerde pintransactie in Oost-Turkije. Deze transactie vond plaats in het grensgebied met Syrië. Het monitoringssysteem genereert voor deze transactie een zogenaamd terrorismefinancieringsalert. Dit is een nuttige alert en voor het signaleren van dergelijke alerts heeft de FIU-NL in een van haar nieuwsberichten een lijst met plaatsnamen in het grensgebied Syrië-Turkije beschikbaar gesteld.

Good practice: De bank combineert red flags
Twee maanden na de pin-transactie in Oost-Turkije (zoals hierboven beschreven) vraagt de cliënt een lening aan van EUR 10.000. De medewerker van de bank stelt vast dat vier maanden eerder aan deze cliënt reeds een lening is verstrekt van EUR 10.000, waarbij de cliënt had aangegeven dat de lening bedoeld was voor onder andere de aankoop van een auto. De bank besluit vervolgens nader onderzoek te doen en stelt vast dat het geld van de eerste lening vrijwel direct van de rekening is gehaald en in verschillende transacties naar Turkije is gestuurd. Ook stelt de bank vast dat er verband bestaat met de eerdere alert, de pintransactie in Turkije. Naar aanleiding hiervan stelt de bank diverse vragen aan de cliënt, maar die kan geen duidelijke reden geven voor de transacties. De tweede lening wordt hierop geweigerd en na het verzoek voor de tweede lening worden de transacties als ongebruikelijk gemeld aan de FIU-NL.

In deze casus zijn de volgende red flags aanwezig:
- een pin-transactie in het grensgebied Turkije-Syrië
- afsluiten van een lening die in een zeer kort tijdsbestek geheel wordt opgenomen
- besteding van de lening correspondeert niet met de verklaring van de cliënt
- opknippen van gelden in kleinere bedragen voor overboekingen
- gelden verkregen via een lening overboeken naar bepaalde landen

3.4.4 Meldproces

Uit het onderzoek bleek dat banken niet altijd ongebruikelijke voorgenomen transacties of uitgevoerde transacties onverwijld en volledig aan de FIU-NL melden conform een gedocumenteerd meldproces.

DNB stelde vast dat banken niet altijd onverwijld melden als gevolg van achterstanden in de alertafhandeling en door reactieve opstelling van de alertbehandelaars. Volgens de wet moeten instellingen onverwijld melden, zodra het ongebruikelijke karakter van een transactie bekend is geworden. Het is denkbaar dat u als bank bij een sterk vermoeden van witwassen of financiering van terrorisme gelijktijdig aangifte doet bij de politie. Indien niet onverwijld wordt gemeld, bestaat immers het risico dat FIU-NL en de opsporingsdiensten relevante informatie mislopen.

Het spreekt voor zich dat u als bank ongebruikelijke voorgenomen en uitgevoerde transacties onverwijld en volledig aan de FIU-NL meldt conform een adequaat en gedocumenteerd meldproces. Belangrijk bij dit meldproces is dat eerdere en aanverwante transacties van de cliënt in het onderzoek worden betrokken en dat daarbij het risicoprofiel van de klant en het bijbehorende transactieprofiel wordt heroverwogen.

De bank draagt er zorg voor dat er adequate (beschreven) processen zijn om onverwijld transacties waarbij aanleiding is om te veronderstellen dat deze verband kunnen houden met witwassen of financieren van terrorisme aan de FIU-NL te melden. Dit betekent ook dat alle relevante informatie rondom een melding binnen de in de wet gestelde voorwaarden en uitzonderingen geheim wordt gehouden. De uitgangspunten daarvoor zijn in het beleid en procedures van de bank vastgelegd. DNB verwacht dat de bank erop toeziet dat beleid en procedures worden doorvertaald in bijvoorbeeld de juiste toegangsrechten van kernsystemen die worden gebruikt voor case management en meldingen, beveiliging van informatiestromen en dat hierover guidance en training wordt verstrekt aan betrokken medewerkers. Deze guidance en training is vooral van belang voor eerstelijnmedewerkers die contact hebben met cliënten. Voor deze medewerkers is het essentieel om te weten wanneer er mogelijk sprake is van ongebruikelijke transacties, welke vragen dan aan een cliënt gesteld moeten worden en welke informatie onder geen beding mag worden gegeven.

Good practice
Een goed voorbeeld uit de praktijk is dat een bank voldoende guidance geeft aan haar medewerkers over het melden van ongebruikelijke transacties door periodiek (op kwartaalbasis) voorbeelden te bespreken en op te nemen in het reguliere opleidingsprogramma. De gemelde transacties weegt de bank mee in de bestaande risicobeoordeling van de cliënt

De bank meldt onverwijld aan FIU-NL-Nederland
In de hierboven beschreven casus waarbij de bank vanuit berichtgeving een relatie van een cliënt met een uitreiziger had opgemerkt, werd deze informatie pas vijf maanden na het zien van de berichtgeving door de bank in behandeling genomen. Dit leidde uiteindelijk tot een melding aan de FIU-NL. De bank had deze zaak eerder moeten onderzoeken en melden aan de FIU-NL, zodat voorkomen wordt dat de FIU-NL en ook de opsporingsdiensten in deze periode relevante informatie mislopen over mogelijke terrorismefinanciering. De bank gaf als reden voor de late behandeling van de alert aan dat er enige tijd achterstanden zijn geweest in de afhandeling van alerts. Gezien de hoge risico's voor Nederland en haar inwoners mag van een instelling verwacht worden dat zij alerts met betrekking tot terrorismefinanciering zo snel mogelijk beoordeelt en meldt aan de FIU-NL. Banken dienen om die reden een hoge prioriteit te geven aan de afhandeling van alerts inzake terrorismefinanciering.

Melden van ongebruikelijk grote kasstortingen van grote coupures

In een casus van grote kasstortingen met onder andere 500-euro biljetten, bleek uit de beschrijving van het onderzoek naar de alert dat de medewerker van een kantoor geen guidance had verkregen of gemeld had moeten worden en op welke wijze dit zou moeten plaatsvinden. Hierdoor had de medewerker geen navraag gedaan naar de bron van de middelen en naar de reden van het gebruik van 500-euro biljetten. De onderzoeker van het alert had derhalve onvoldoende informatie om deze transacties te melden bij de FIU-NL, terwijl daar vanwege de grote kasstortingen en het gebruik van 500-euro biljetten voldoende aanleiding voor was.

3.4.5 Heroverwegen risicoclassificatie cliënt

Indien de bank transacties van een cliënt meldt aan de FIU-NL, verwacht DNB dat de instelling het bestaande risicoprofiel van de cliënt (opnieuw) bekijkt om te bepalen of er redenen bestaan om dit profiel aan te passen. Op deze wijze borgt de instelling dat het risicoprofiel van de cliënt en daarmee diens risicoclassificatie na melding van een ongebruikelijke transactie, aansluit bij de witwas- of terrorismefinancieringsrisico's van de cliënt. Ook indien de bank van de FIU-NL een terugmelding ontvangt dat de transactie als verdacht is doorgemeld naar de opsporingsautoriteiten, beoordeelt de instelling het risicoprofiel van de cliënt en past deze indien nodig aan.

DNB gaat ervan uit dat banken ervoor zorgen dat de analisten die de alerts beoordelen en terugmeldingen ontvangen, mogelijkheden hebben om zelf het risicoprofiel van de cliënt te herbeoordelen, of dat zij aan de medewerkers die verantwoordelijk zijn voor de klantbeoordeling aan kunnen geven dat herbeoordeling noodzakelijk is. DNB verwacht dat door middel van het quality assurance proces wordt gemonitord of dergelijke herbeoordelingen adequaat worden uitgevoerd.

Good practice

De bank heroverweegt haar risicoclassificatie cliënt naar aanleiding van melding bij FIU-NL-Nederland, dan wel terugmelding van FIU-NL

Een medewerker van een bank pikt uit lokale nieuwsberichten op dat er een hennepkwekerij is gevonden in het huis van een cliënt van de bank. Na onderzoek blijkt dat de cliënt verschillende contante stortingen op zijn rekening en de rekening van zijn stichting deed. De cliënt bevestigt dat hij de hennepteelt vanuit zijn eigen woning exploiteerde en de contante opbrengsten van deze illegale activiteiten op zijn rekening en die van zijn stichting stortte. De cliënt geeft als verklaring op dat hij zich in een moeilijke financiële situatie bevond en om die reden overging tot deze illegale activiteiten. Naar aanleiding van voorgaande worden ongebruikelijke

transacties gemeld bij de FIU-NL en wordt de risicoclassificatie van deze cliënt heroverwogen en wordt deze op onacceptabel geplaatst.

3.4.6 Objectieve indicatoren

Diverse banken hebben gezien de aard van hun werkzaamheden vaak te maken met transacties die voldoen aan één van de objectieve indicatoren voor het melden van ongebruikelijke transacties. Om ervoor te zorgen dat deze onverwijld aan de FIU-NL gemeld worden, zou een tool of functionaliteit binnen het transactiemonitoringssysteem ingesteld kunnen worden, waardoor transacties die aan deze objectieve indicator voldoen, automatisch worden gemeld aan de FIU-NL. Hiermee voorkomen deze instellingen dat deze transacties mogelijk niet onverwijld gemeld worden en halen ze een administratieve last weg bij degene die hiervoor verantwoordelijk is.

3.5 Governance

De governance ten aanzien van transactiemonitoring bleek met name wat betreft de rolverdeling van de lines of defense niet op orde te zijn

Uit de onderzoeken is gebleken dat banken de governance omtrent transactiemonitoring op verschillende wijzen hadden ingericht. Bij meerdere banken ontbrak de controle door deze tweede lijn ten aanzien van de door de eerste lijn uitgevoerde transactiemonitoring activiteiten. Wel hadden banken veelal een controleprogramma voor het cliëntenonderzoek door de tweede lijn ingericht, maar de alerts vanuit het transactiemonitoringssysteem werden niet door de tweede lijn getoetst.

Good practice
Tijdens het onderzoek heeft DNB geconstateerd dat alle onderzochte instellingen beschikten over een onafhankelijke interne controle functie (de derdelijnsfunctie, veelal de interne accountantsfunctie) die door middel van audits periodiek een oordeel vormt over de opzet, bestaan en werking van het transactiemonitoringssysteem en -proces. Deze audits waren over het algemeen van goede kwaliteit en bevindingen werden adequaat opgevolgd. Een instelling monitorde daarnaast maandelijks de voortgang van de actiepunten die door de business waren opgesteld naar aanleiding van de auditrapportage.

DNB verwacht dat de organisatie van de bank zodanig is ingericht dat de eerste lijn een duidelijke verantwoordelijkheid heeft voor de transactiemonitoring en dat de tweede lijn (compliance) een adviserende en controlerende taak heeft, maar daarbij ook een taak kan hebben bij het melden van ongebruikelijke transacties aan de FIU-NL. De bank heeft binnen de tweede lijn de controlerende taak (quality assurance) voor transactiemonitoring belegd. In de praktijk noemt men dit veelal *Second Line Monitoring*. In het verlengde hiervan is het van belang de procedures en processen periodiek en op systematische wijze te toetsen. Compliance voert als tweedelijnsorganisatieonderdeel structureel een monitorende rol uit en test daarnaast periodiek of maatregelen adequaat zijn of moeten worden aangepast. Vervolgens verwacht DNB dat de derdelijnsfunctie, de onafhankelijke internecontrolefunctie, met voldoende frequentie het functioneren van de eerste en tweede lijn controleert. Daarbij zorgt de organisatie ervoor dat zij voldoende capaciteit beschikbaar stelt om invulling te geven aan deze rollen en taken.

DNB verwacht dat signalen uit de eerste, tweede en derde lijn over mogelijke tekortkomingen in het transactiemonitoringsproces en de uitkomsten hiervan door het senior management worden opgepakt. Daarom is het van belang dat een bank beschikt over adequate en periodieke managementinformatie die inzicht geeft in deze signalen en uitkomsten opdat zij daarop tijdig kan sturen. Zodoende vervult Compliance naast haar adviserende en controlerende rol, tevens een rapporterende rol ten aanzien van transactiemonitoring.

3.6 Training en awareness

Het onderzoek liet zien dat de onderzochte banken niet altijd beschikten over een toegesneden trainingsprogramma en dat banken zich niet altijd bewust toonden van witwas- en terrorismefinancieringsrisico's.

DNB constateert dat de meeste banken trainingen ten aanzien van Wwft hebben opgenomen in het (jaarlijkse) trainingsprogramma. DNB verwacht dat hierbij de inhoud van dit programma is afgestemd

op competenties en ervaring van de medewerker (van bestuur en senior management tot junior medewerker) en gebruik wordt gemaakt van casuïstiek vanuit het eigen transactiemonitoringsproces.

Good practice

Een van de onderzochte banken beschikte over een trainingsprogramma voor de alertafhandelingsanalisten gebaseerd op vier verschillende ervaringsniveaus. In het trainingsprogramma waren de verwachte competenties per ervaringsniveau vastgelegd, alsmede de doelen die met training moeten worden behaald. Ook was in het trainingsprogramma vastgelegd hoe gemeten werd of deze doelen behaald werden

Een andere onderzochte bank had zowel voor de eerste, tweede als derde lijn een (jaarlijks) trainingsprogramma beschikbaar. Daarin werd aan de hand van casuïstiek uit de praktijk doorgenomen wat de nieuwste ontwikkelingen waren, zowel qua wet- en regelgeving, als praktijkvoorbeelden rondom mogelijk witwassen en financiering van terrorisme en hoe de instelling hiermee omgaat. Dat wil zeggen dat de vertaling werd gemaakt naar beleid, procedures en onderliggende werkprocessen. Daarmee werd duidelijkheid gecreëerd over hoe in voorkomende gevallen gehandeld diende te worden.

Een aantal banken beschikte over een *dedicated* expert op het gebied van terrorismefinanciering.

Disclaimer

In deze brochure geeft De Nederlandsche Bank N.V. (DNB) haar bevindingen weer over door haar geconstateerde of verwachte gedragingen in de toezichtpraktijk, die naar haar oordeel een goede toepassing inhouden van het wettelijk kader met betrekking tot de vereisten van transactiemonitoring. Voor een betere duiding worden in deze brochure ook praktijkvoorbeelden gegeven.

Deze brochure dient altijd tezamen met de regelgeving en de DNB Leidraad Wwft en SW, versie april 2015, te worden gelezen. U kunt de good practices uit deze brochure meenemen bij uw invulling van uw transactiemonitoring. Daarbij kunnen eigen omstandigheden in aanmerking worden genomen. Niet uitgesloten is dat in voorkomende gevallen een strengere toepassing van onderliggende regels geboden is.

Dit document is geen juridisch bindend document of beleidsregel van DNB als bedoeld in artikel 1:3 lid 4 Algemene Wet Bestuursrecht en heeft of beoogt geen rechtsgevolg. Dit document komt niet in de plaats van wet- en regelgeving en beleids- of toezichthouderregelingen op dit gebied. De in dit document opgenomen voorbeelden zijn niet uitputtend en zullen niet per definitie in alle gevallen als voldoende zijn aan te merken. Zij zijn een handreiking voor de uitleg en toepassing van de wettelijke verplichtingen.