Post-event transactie-monitoringsproces bij banken

Guidance

DeNederlandscheBank
EUROSYSTEEM

30 augustus 2017

Westeinde 1, 1017 ZN Amsterdam – Postbus 98, 1000 AB Amsterdam
Telefoon 020 524 91 11 – E-mail: info@dnb.nl
Website: www.dnb.nl

Inhoud

1 Inleiding

1.1 Waarom deze guidance?

Financieel-economische criminaliteit is een groot probleem in onze huidige maatschappij. Krantenkoppen laten zien dat de samenleving ongewild slachtoffer is geworden van deze vorm van criminaliteit, denk aan recente incidenten als de Panama Papers en terroristische aanslagen in West-Europa. Financiële instellingen, waaronder banken, spelen een belangrijke rol bij het voorkomen van witwassen en terrorismefinanciering. Daartoe voeren banken onder meer cliëntenonderzoek uit: door middel van zogenoemde customer due diligence (CDD) en door transacties van cliënten te monitoren met als doel ongebruikelijke transacties te identificeren. 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 actie ondernemen als sprake is van een mogelijk ongebruikelijke transactie of van een meldenswaardig transactiepatroon. Die kan de bank dan nader onderzoeken en eventueel melden. Gebeurt die monitoring niet of niet goed, dan kan het zijn dat een bank ongewild bijdraagt aan het financieren van terrorisme of het witwassen van geld.

Deze functie als poortwachter van het Nederlandse financiële systeem vergt onder meer dat banken adequaat transacties monitoren. Continu en alert. Daarom heeft de wetgever op dit gebied eisen geformuleerd waaraan een bank moet voldoen en DNB heeft de wettelijke taak om toe te zien op naleving van de wet- en regelgeving. Transactiemonitoring is dus verplicht voor iedere bank, maar deze verplichting alsook het toezicht hierop is principle-based. Dat wil zeggen dat de praktische invulling hiervan niet in detail voorgeschreven is door wet- en regelgeving of door de toezichthouder. Als bank maakt u uw eigen keuzes over de precieze invulling. De toezichthouder beoordeelt het resultaat.

Het onderwerp transactiemonitoring is voor banken niet nieuw. De in dit document opgenomen aandachtspunten en voorbeelden gelden als 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.

1 Wwft: Wet ter voorkoming van witwassen en financieren van terrorisme; SW: Sanctiewet 1977.

1.2 Leeswijzer

Met dit document biedt DNB u guidance over hoe u uw transactiemonitoringsproces kunt inrichten en verbeteren. Voor deze guidance heeft DNB gebruik gemaakt van de belangrijkste bevindingen van het in 2016 uitgevoerde thema-onderzoek "post-event transactiemonitoring bij banken".[2] 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 good practices over delen. Het spreekt voor zich dat u de eigen omstandigheden van uw bank in aanmerking neemt bij de oplossingen en maatregelen die u treft. U maakt hierin uw eigen afweging.

In dit document leest u aan welke wettelijke vereisten banken dienen te voldoen en hoe DNB de invulling van transactiemonitoring, conform internationale standaarden en good practices, voor ogen heeft. DNB verwacht dat de sector hier goed kennis van neemt en daar waar nodig verbeteringen implementeert in de bedrijfsvoering.

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 volwassenheidsmodel vinden dat wij hanteerden bij het onderzoek in 2016.
In hoofdstuk 3 leest u per onderdeel van dit model good practices en voorbeelden hoe het niet moet.
U treft tot slot een lijst aan van de belangrijkste gebruikte begrippen.

2 Het thema Transactiemonitoring was een zogenaamd cross-sectoraal onderzoek, uitgevoerd in verschillende sectoren (vier banken, vier betaalinstellingen, drie money transferkantoren en zes trustkantoren). Voor de overige sectoren is een vergelijkbare guidance opgesteld.

2 Samenvatting

Transactiemonitoring is een essentiële maatregel om onder meer mogelijk ongebruikelijke transacties te melden bij de FIU-NL, om zo de integriteitrisico's op het gebied van witwassen en terrorismefinanciering te beheersen.

Samengevat betekent dit het volgende:

1. Banken vertalen de risico's op witwassen en terrorismefinanciering die uit de SIRA voortvloeien zichtbaar door naar het transactiemonitoringsproces. Bij de bepaling van het risicoprofiel van de cliënt en/of 'cliënt peergroups' betrekken banken ook het verwachte transactiegedrag.
2. Banken hebben voldoende beleid voor transactiemonitoring opgesteld en hebben dit beleid voldoende uitgewerkt in onderliggende procedures en werkprocessen.
3. Banken beschikken over een (geautomatiseerd) transactiemonitoringssysteem en hebben een onderbouwde en toereikende set aan business rules (detectieregels met scenario's en grenswaarden) om witwas- en terrorismefinancieringsrisico's te detecteren. Banken testen deze business rules periodiek, zowel op technische aspecten als effectiviteit.
4. Banken beschikken over een adequaat meld- en alertafhandelingsproces. Banken zorgen ervoor dat voorgenomen en uitgevoerde ongebruikelijke transacties onverwijld en volledig aan de FIU-NL worden gemeld. In dit proces zijn per alert overwegingen en conclusies vastgelegd om te komen tot het sluiten dan wel escaleren van alerts.
5. Banken hebben hun governance ten aanzien van transactiemonitoring zodanig ingericht dat sprake is van een duidelijke functiescheiding, bijvoorbeeld via het three lines of defense model.
6. Banken beschikken over een toegesneden trainingsprogramma voor hun medewerkers. De medewerkers zijn zich bewust van witwas- en terrorismefinancieringsrisico's.

3 Wettelijke context en reikwijdte

3.1 Transactiemonitoring: wettelijke verplichting tot voortdurende controle

Banken zijn wettelijk verplicht maatregelen te nemen om witwassen en terrorismefinanciering tegen te gaan. 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 brengen. Is er aanleiding om te veronderstellen dat een (voorgenomen) transactie verband houdt met witwassen of terrorismefinanciering, dan moet u als bank deze transactie als ongebruikelijk melden bij de Financial Intelligence Unit – Nederland (FIU - NL).[3] Om dit te kunnen doen is het van cruciaal belang dat banken beschikken over een effectief transactiemonitoringsproces.[4]

Onder verwijzing naar de DNB Leidraad Wwft en SW, versie 3.0, april 2015, bevestigen wij het volgende[5]: aangezien de Wft (integere bedrijfsvoering) en de Wwft hetzelfde doel beogen, kunnen de maatregelen die een bank neemt op grond van de Wft en de Wwft worden geïntegreerd en kunt u als bank op een zelfde wijze invulling geven aan de vereisten van de Wwft en Wft. Maatregelen ter bestrijding van witwassen en het financieren van terrorisme op grond van de Wft worden gepreciseerd in de Wwft. Het hoofddoel blijft dat uw bank weet met wie zij zaken doet en waarvoor de zakelijke relatie gebruikt wordt.

Om een adequate voortdurende controle uit te oefenen, moet u als bank op grond van artikel 10 Besluit prudentiële regels Wft (Bpr) allereerst zorgdragen voor een systematische integriteitsrisicoanalyse (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".[6] Daartoe behoren dus ook de risico's op witwassen en financieren van terrorisme. Signaleert een bank naar aanleiding van deze analyse (rest)risico's, dan moet die bank hiervoor beleid formuleren, procedures instellen en maatregelen treffen.

Specifiek ten aanzien van de risico's met betrekking tot witwassen en terrorismefinanciering bepaalt de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) verder nog dat een bank onderzoek moet doen naar zijn cliënten.[7] Daarbij dient de bank het doel en de beoogde aard van de zakelijke relatie vast te stellen. Ook moet de bank een voortdurende controle uitoefenen

3 Kort gezegd spreken wij hierna in dit document over "ongebruikelijke transacties".
4 Artikel 14, lid 4 Bpr, artikelen 2a, lid 1 en 3, lid 2 sub d Wwft.
5 Zie pagina's 5 en 6 van deze Leidraad.
6 Art. 1 Bpr.
7 Art. 2a, lid 1 en art. 3, lid 1 Wwft.

op de zakelijke relatie en de tijdens de duur van deze zakelijke relatie verrichte transacties.[8] Op deze manier kunnen banken verzekeren dat de uitgevoerde 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.[9] DNB realiseert zich dat het niet altijd mogelijk is om voor iedere individuele relatie op voorhand een risicoprofiel op te stellen, gelet op de omvangrijke hoeveelheid relaties voor bepaalde klantsegmenten, bijvoorbeeld bancaire dienstverlening aan particulieren of klein MKB-bedrijf. Om dit praktisch te kunnen doen, kan een bank haar zakelijke relaties indelen naar bijvoorbeeld zogenoemde 'peergroups'. Daarbij definieert de bank haar eigen peergroups aan de hand van een aantal cliëntkenmerken, bijvoorbeeld sectoren, rechtsvormen, leeftijden natuurlijke personen, landen, et cetera.

Het begrip 'voortdurende controle' staat centraal in het proces van transactiemonitoring en kan door uw bank op eigen wijze risicogebaseerd worden ingevuld. Risicogebaseerd wil in dit verband zeggen dat uw bank de meeste aandacht zal besteden aan hetgeen zij als grootste risico's heeft geïdentificeerd. Deze risicogebaseerde aanpak moet te allen tijde onderbouwd kunnen worden met de uitkomsten van uw integriteitsrisicoanalyse. 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 'red flags' geïdentificeerd en deze uitgewerkt in business rules. 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 brengen.[10]

Een verrichte of voorgenomen ongebruikelijke transactie moet onverwijld gemeld worden aan de FIU-NL zodra het ongebruikelijke karakter van de transactie bekend is geworden.[11] Uw bank dient dan ook specifieke procedures en werkprocessen te hebben opgesteld om transactiealerts te beoordelen, af te handelen en ongebruikelijke transacties te melden.[12] Ter waarborging van deze procedures en maatregelen dient een bank zorg te dragen dat haar werknemers, voor zover relevant voor de uitoefening van hun taken, bekend zijn met

8 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.

9 Art. 3, lid 2, sub d Wwft.

10 Art. 2a, lid 1 Wwft.

11 Art. 16 Wwft.

12 Art. 16 Wwft jo. artt. 17 en 18 Bpr.

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 en door te leiden.[13]

3.2 Reikwijdte guidance

Deze guidance is van toepassing op:

- In Nederland gevestigde banken zoals gedefinieerd in artikel 1, lid 1 van de Wwft;
- Bijkantoren van buitenlandse banken die in Nederland zijn gevestigd zoals gedefinieerd in artikel 1, lid 1 van de Wwft;
- Voor internationaal opererende banken zoals bedoeld in artikel 2, lid 1 van de Wwft. Dat wil zeggen dat wanneer deze banken bijkantoren of dochtermaatschappijen hebben in een staat die geen EU/EER lidstaat is, dit betreffende bijkantoor of dochtermaatschappij zijn of haar transactiemonitoringsproces zo moet inrichten dat deze gelijkwaardig is aan de eisen die de Wwft stelt.

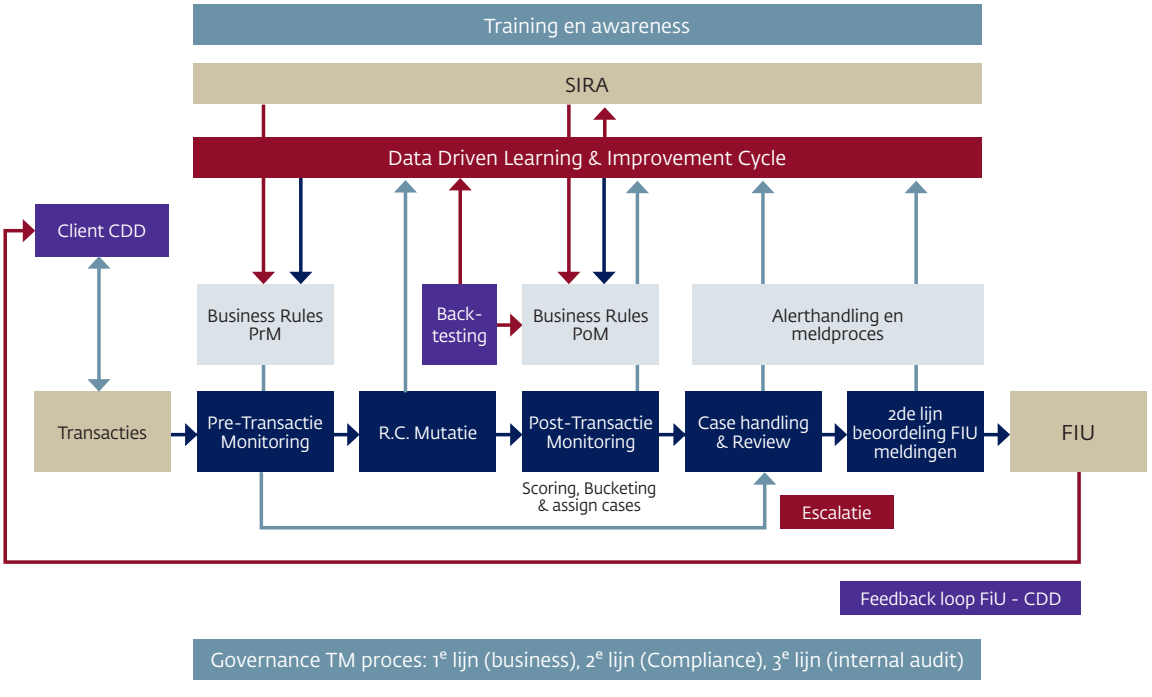
13 Art. 35 Wwft.

4 Transactiemonitoring

4.1 Het transactiemonitoringsproces

Het transactiemonitoringproces kan er als volgt uitzien:

Figuur 1 Het transitiemonitoringsproces



Transactiemonitoring kan op verschillende manieren worden uitgevoerd. Zoals uit het schema blijkt, kan sprake zijn van pre-transactiemonitoring[14] en post-event transactiemonitoring, dat wil zeggen dat zowel vooraf als achteraf transacties worden gemonitord.

Pre-transactiemonitoring

Pre-transactiemonitoring vindt plaats voordat de transactie is uitgevoerd en heeft met name betrekking op die situaties waarbij face-to-face contact plaatsvindt tussen cliënt en de bank-medewerker. Denk hierbij aan een cliënt die bij de balie van een bankkantoor komt en bepaalde coupures of vreemde valuta wil omwisselen of een chartale hoeveelheid geld op een bankrekening wil storten. Een ander voorbeeld is de bancaire activiteit handelsfinanciering of 'trade finance', waarbij een bank geacht wordt een bepaalde voorgenomen transactie uit te voeren. Bij post-event transactiemonitoring is de transactie reeds door de bank uitgevoerd en vindt de transactiemonitoring achteraf plaats.

Wij benadrukken 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 of tijdens de uitvoering.

DNB is van oordeel dat pre-transactiemonitoring, als geautomatiseerd proces of handmatig, een effectieve bijdrage levert omdat juist hier het klantcontact plaatsvindt. De front-office heeft zodoende een grote verantwoordelijkheid in het detecteren van mogelijk ongebruikelijke transacties, waaronder witwassen en terrorismefinanciering. Met name is dit van belang 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 al voor effectuering detecteren en deze voorgenomen transactie onverwijld melden aan de FIU-NL.

Good practice

Een bank signaleert bij een aanvraag voor een transactie vanuit haar afdeling Trade Finance Services dat de aangekochte producten afwijken van de reguliere business van de klant. De transactie wordt op 'on hold' gezet en bij de MLRO[15] gemeld. Na navraag bij de cliënt blijkt deze zijn business te hebben verlegd naar een nieuwe markt. Bewijs van de portfoliowijziging wordt aangeleverd en overgelegd aan de MLRO. Na akkoord van de MLRO wordt de transactie alsnog uitgevoerd.

14 Bij post-event transactiemonitoring is de transactie reeds door de bank uitgevoerd en vindt de transactiemonitoring achteraf plaats, bij pre-transactiemonitoring is de transactie nog niet uitgevoerd.

15 MLRO staat voor "Money Laundering Reporting Officer". Deze functie maakt deel uit van de 2e lijn.

Post-event transactiemonitoring

Deze guidance beschrijft het post-event transactiemonitoringproces, omdat banken vooral op deze wijze, in het kader van met name de girale afwikkeling van transacties, witwas- en terrorismefinancieringsrisico's kunnen detecteren.

Het cliëntenonderzoek is onderdeel van het transactiemonitoringsproces. Door cliëntenonderzoek verkrijgt u als bank kennis van de cliënt, waaronder het doel en de beoogde aard van de zakelijke relatie met de cliënt. Met die kennis kunt u risicogebaseerd beoordelen of 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 uw bank afstemmen op de cliënt zelf: het soort cliënt, het type dienstverlening aan de cliënt en het risicoprofiel van de cliënt of het cliëntsegment. Per cliëntsegment en per product kunt u de monitoring op verschillende wijzen inrichten.

Stap 1: risico-identificatie

De eerste stap in het transactiemonitoringsproces is risico-identificatie. Tijdens het identificatieproces analyseert u als bank systematisch de witwas- en terrorismefinancieringsrisico's die uw verschillende soorten cliënten, producten, distributiekanalen en transacties met zich brengen. De uitkomsten van deze analyse legt u vast in de zogenoemde SIRA. Deze SIRA vertaalt u vervolgens door naar beleid, bedrijfsprocessen en procedures omtrent transactiemonitoring. Een bank kan overigens beschikken over verschillende SIRA's, denk aan een afzonderlijke SIRA voor dochtermaatschappijen, of een SIRA per business line. Het is van belang om de doorvertaling van de diverse SIRA-uitkomsten vast te leggen, waarbij u zowel de wijze waarop u doorvertaalt als de doorvertaling zelf, vastlegt.

Bij het identificeren en analyseren van de risico's hoort ook dat u de cliënten van uw bank indeelt in risicocategorieën, bijvoorbeeld hoog, midden en laag, op grond van de witwas- en terrorismefinancieringsrisico's die de zakelijke relatie met de cliënt met zich brengt. Voor de bepaling van het risicoprofiel van een cliënt maakt u een transactieprofiel op basis van de verwachte transacties of het verwachte gebruik van de rekening van een cliënt (of cliëntgroep).[16] Door (via zogenoemde 'peergrouping') een dergelijk transactieprofiel aan te maken, kan uw bank in voldoende mate monitoren dat de transacties die tijdens de duur van de relatie verricht worden, overeenkomen met de kennis die de bank heeft van de cliënt en diens risicoprofiel. Door het verwachte transactiegedrag van de cliënt in beeld te brengen, kunt u toetsen of de door de cliënt uitgevoerde transacties overeenkomen met de kennis die u heeft van de cliënt.

16 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.

Een goed werkbaar transactieprofiel voldoet in ieder geval aan de volgende zes eisen:

1. Actueel: het transactieprofiel is up-to-date en voorzien van een datum. Alle relevante wijzigingen worden tijdig verwerkt.
2. Volledig: alle bankrekeningnummers, alle namen van de begunstigden en betalingsbevoegden en alle relevante activiteiten zijn opgenomen.
3. Specifiek: de verwachte posten/geldstromen zijn duidelijk beschreven, onder andere de bedragen, diensten en de frequentie. Opgenomen (grens) bedragen zijn goed onderbouwd en kunnen daadwerkelijk bijdragen aan het herkennen van ongebruikelijke transacties.
4. Overzichtelijk: met inzichtelijke schema's zijn geldstromen op eenvoudige wijze goed en overzichtelijk weergegeven.
5. Onderbouwd: het transactieprofiel is onderbouwd met relevante stukken die de geprognosticeerde geldstromen toelichten en verklaren.
6. Vastgelegd: het transactieprofiel is vastgelegd in het cliëntendossier.

Stap 2: patronen en transacties detecteren

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. Alvorens hiervan gebruik te maken dient de bank te borgen dat alle bronsystemen van te monitoren transacties zijn geïdentificeerd en dat de data volledig en juist wordt meegenomen in het transactiemonitoringproces. Dit kan data betreffen over de cliënt, de diensten en de transacties. Is sprake van grotere hoeveelheden transacties, dan 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 kunnen ook meer geavanceerde systemen gewenst zijn, en in voorkomende gevallen noodzakelijk, afhankelijk van onder meer aard en omvang van de transacties en de aard van de betreffende instelling. Zo zal bijvoorbeeld bij een bank met een eenvoudig bedrijfsmodel en een beperkt aantal eenvoudige transacties, een zeer geavanceerd systeem mogelijk minder noodzakelijk zijn. Het kan ook zijn dat een bank het gebruik van zeer geavanceerde systemen noodzakelijk acht, bijvoorbeeld het gebruik van 'artificial intelligence'.[17]

17 De toepassing van kunstmatige intelligentie, waarbij aan de hand van beschikbare data en een herkennings- of cluster-algoritme de computer zelf leert om bepaalde patronen te herkennen of te ontdekken. Een algoritme is een rekenwijze voor het berekenen van bepaalde grootheden en functies.

De verantwoordelijkheid voor het effectief detecteren van ongebruikelijke transacties blijft hoe dan ook liggen bij uw bank. U dient de werking van de systemen goed te begrijpen en kunt daarom niet enkel steunen op door externe leveranciers aangeleverde algoritmes. Om gebruik te kunnen maken van artificial-intelligencesystemen kan het daarom raadzaam zijn medewerkers met artificial-intelligence-expertise aan te haken.

Stap 3: data-analyse

Met behulp van uw transactiemonitoringssysteem en gebruik van specifieke en intelligent ingerichte software analyseert u als bank uw transactiedata. Het systeem genereert op basis van business rules, zogenoemde 'alerts'. Met een alert wordt een signaal bedoeld dat duidt op een mogelijk ongebruikelijke transactie. Deze alerts worden aan onderzoek onderworpen. De bevindingen van uw onderzoek van de alerts dienen adequaat en duidelijk te worden vastgelegd. Wanneer 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 en vastgelegd. Op het moment dat een bank – al dan niet opzettelijk- niet of niet tijdig voldoet aan de meldplicht, dan kan dat een economisch delict zijn.

Stap 4: beoordeling, maatregelen en vastlegging

Vervolgens beoordeelt u de gevolgen van een melding aan de FIU-NL en een eventuele terug-melding van de FIU-NL voor het risicoprofiel van de cliënt en stelt u vast of eventuele aanvullende beheersmaatregelen genomen moeten worden. Sluitstuk van het transactiemonitoringsproces is de bewaring van gegevens die u verkrijgt in het kader van transactiemonitoring. In dit verband bewaart de bank de gegevens van de melding van de ongebruikelijke transactie en legt deze vast, op zodanige wijze dat die gegevens opvraagbaar zijn en de desbetreffende transactie re-construeerbaar is gedurende vijf jaar na het tijdstip van het doen van de melding.

4.2 Volwassenheidsmodel

Bij de uitvoering van het themaonderzoek (post-event) transactiemonitoring bij banken gebruikte DNB een zelf 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 op zes gebieden toegelicht aan de hand van een vierpuntsschaal:

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

Dit volwassenheidsmodel kunt u als bank gebruiken om de eigen ambities te bepalen, waarbij u minimaal 'geel' scoort. Het ambitieniveau van uw bank is afhankelijk van het risicoprofiel van uw instelling. Een gele score betekent dat een bank voldoet aan de minimale wettelijke vereisten (in voldoende mate compliant).

In het figuur op de volgende pagina ziet u het volwassenheidsmodel nader uitgewerkt, inclusief de mogelijke scores op de zes toetsingselementen.

In hoofdstuk 5 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.

Figuur 2 Volwassenheidsmodel voor (post-event) transactiemonitoring

1 SIRA / risicoprofiel	2 Opzet beleid en procedures	3 TM systeem/ business rules
■ 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
■ 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
■ Er is een SIRA uitgevoerd waarin voldoende diepgang zit in scenario's en risico's ■ Scenario's en risico's uit de SIRA (inclusief red flags en modus operandi witwassen / terrorismefinanciering)zijn in voldoende mate vertaald naar transactiemonitoring beleid en procedures, echter op een generiek niveau ■ Instelling heeft cliënten 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 (inclusief red flags en modus operandi witwassen / terrorismefinanciering) om ongebruikelijke transacties te herkennen ■ Instelling maakt gebruik van backtesting bij het periodiek evalueren van haar business rules ■ Aanpassen van systeem en business rules naar aanleiding van ontwikkelingen t.a.v. witwassen en terrorismefinanciering gebeurt reactief
■ 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 geïncorporeerd 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 ■ Actieve samenwerking met financiële instellingen over beleid	■ Instelling heeft een geautomatiseerd en zelflerend transactie-monitoring systeem passend bij risicoprofiel van de instelling ■ Er wordt proactief ingespeeld op ontwikkelingen op het gebied van witwassen en terrorismefinanciering en daarmee aanpassngen 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

4 Alert afhandeling en meldproces	5 Governance: 1e, 2e en 3e lijn	6 Training en awareness
■ 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
■ 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 lijn ■ 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)
■ 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 ■ Trainingsprogramma is ingericht op basis onderscheidende niveaus in de organisatie (van management tot medewerker) ■ Periodiek worden (verplichte) trainingen op het gebied van AML/CFT aangeboden en inhoud is van voldoende kwaliteit (bevat materiële onderdelen)
■ 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 terrorisme-financieringsrisico'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 terrorisme-financiering worden direct vertaald naar de organisatie (o.a. FIU-NL casuïstiek)

5 Guidance

5.1 SIRA

Banken vertalen de risico's op witwassen en terrorismefinanciering die uit de SIRA voortvloeien zichtbaar door naar het transactie-monitoringsproces.

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".[18] Hieronder vallen de financieel-economische criminaliteitsrisico's, witwassen, financieren van terrorisme, niet-naleving van sancties, corruptie/omkoping en belangen-verstrengeling. Om te waarborgen dat uw bank de integriteitrisico's adequaat beheerst, heeft de wetgever verschillende verplichtingen opgenomen waaraan uw bank moet voldoen. Hierbij speelt de SIRA[19] een centrale rol. Deze risicoanalyse op organisatieniveau, waarbij zowel eerste- als tweedelijns functionarissen betrokken zijn geweest, legt de basis voor uw periodiek te herzien integriteitsbeleid 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. Hieronder vindt u een voorbeeld van een bank die dat niet voldoende gedaan had.

DNB constateerde dat de meeste onderzochte banken de uitkomsten met betrekking tot de risico's op witwassen en financieren van terrorisme vanuit hun SIRA niet hadden doorvertaald naar hun transactiemonitoringsproces. Zo deed een onderzochte bank relatief veel zaken met een verhoogd risicoland, wat in haar SIRA wel was geïdentificeerd, maar niet was opgenomen in het transactiemonitoringsproces. DNB constateerde bovendien dat de onderzochte banken in hun SIRA onderscheid maakten tussen witwassen en terrorismefinanciering, maar dit onderscheid niet tot uitdrukking brengen in het transactiemonitoringsproces. Enkele van de onderzochte banken bleken nauwelijks aandacht te besteden aan terrorismefinancieringsscenario's.

18 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.

19 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.

5.1.1 Risicoprofiel: verwacht transactiegedrag

Bij de bepaling van de CDD-risicoclassificatie (laag, midden, hoog) van de cliënt betrekt de bank het verwachte transactiegedrag van de cliënt.

Op grond van de Wwft moeten banken bij het cliëntenonderzoek een cliëntrisicoprofiel opstellen van de cliënt. Hierbij dienen verschillende factoren van de cliënt te worden beoordeeld, zoals de sector(en) en landen waarin de cliënt actief is, de bij de bank afgenomen producten en diensten en het distributiekanaal. Op basis hiervan bepaalt u als bank de risicoclassificatie van uw cliënt. Afhankelijk van het risico, kunnen bijvoorbeeld zogenoemde 'mass retail cliënten' worden opgenomen in homogene cliëntgroepen, de zogenoemde 'peer grouping'.

De review van de cliënt en actualisatie van de cliëntgegevens vindt periodiek plaats en ook tussentijds op basis van relevante gebeurtenissen. De onderliggende redenen die geleid hebben tot een risicoclassificatie, gebruikt u ook voor uw transactiemonitoringsproces. Wanneer cliënten geen risicoclassificatie hebben, is het immers niet mogelijk het transactiemonitoringssysteem risicogericht in te richten. Op basis van uw kennis over uw cliënt kunt u bekijken of de transacties van die cliënt overeenkomen met het beeld dat uw bank heeft van uw cliënt en het verwachte transactieprofiel.

Om het verwachte transactiegedrag te bepalen, kunt u als bank tijdens periodieke monitoring (lees: periodieke CDD-review) van uw cliënt 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.

U kunt al of niet met toepassing van eerder-genoemde peergrouping, gebruik maken van geavanceerde data-analysetechnieken bij het opstellen van het verwachte transactieprofiel.

Een verwacht transactieprofiel is van groot belang bij het detecteren van ongebruikelijke transacties en daarmee bij het voorkomen van witwassen en terrorismefinanciering. Als bank kunt u immers alleen de ongebruikelijkheid van een transactie vaststellen wanneer u weet wat gebruikelijke transacties zijn. Indien uit specifieke transacties of het transactieverloop op de rekening blijkt dat het transactiegedrag van de cliënt afwijkt van het ex-ante opgestelde risicoprofiel, moet u als bank nagaan of mogelijk sprake is van ongebruikelijke transacties en of verdere acties moeten worden ondernomen, bijvoorbeeld een herbeoordeling van het cliëntrisicoprofiel. Daarnaast toetst uw bank de effectiviteit van alerts; bij mogelijke ongebruikelijkheid

wordt immers een alert gegenereerd. Daarbij is een goede samenwerking tussen verschillende personen of afdelingen essentieel.

Aangezien u het verwachte transactiegedrag opstelt bij aanvang van de zakelijke relatie met de cliënt, is de bank primair afhankelijk van gegevens die de cliënt zelf verstrekt over de verwachte transacties. Verwacht mag worden dat banken risicogebaseerd periodiek en bij een event-gedreven review beoordelen of het verwachte transactiegedrag nog steeds in voldoende mate overeenkomt met de werkelijkheid. Deze informatie kan ter verificatie worden vergeleken met transactiegedrag van andere cliënten in vergelijkbare sectoren of cliënten met een vergelijkbaar risicoprofiel.

Good practice

Om tot een verwacht transactiegedrag te komen heeft een bank haar cliëntportfolio aan de hand van diverse klantkenmerken opgedeeld in homogene klantgroepen, de 'peer groups'. Voor elk van deze klantgroepen is met behulp van data-analyse en op basis van meerdere relevante risico-indicatoren uit het klantprofiel een verwacht transactiepatroon vastgesteld. Wanneer deze vaststelling niet op basis van bekende klantkenmerken kan worden gedaan, doet de bank dit door middel van een analyse van historisch transactiegedrag, of door een uitvraag aan de klant. Voor iedere cliënt wordt continue het daadwerkelijke transactiegedrag vergeleken met dit verwachte transactiepatroon. In deze vergelijking worden meerdere risico-indicatoren betrokken, bijvoorbeeld cashstortingen en internationale betalingen. Statistisch significante afwijkingen van het verwachte transactiegedrag worden automatisch gedetecteerd door het transactiemonitoringsysteem, en worden conform het reguliere afhandelingsproces onderzocht om vast te stellen of dit mogelijk een risico op financieel-economische criminaliteit betreft.

5.2 Beleid en procedures

Banken hebben voldoende beleid voor transactiemonitoring opgesteld en dit voldoende uitgewerkt in onderliggende procedures en werkprocessen.

Om (potentieel) ongebruikelijke transactiepatronen of transacties, waarbij mogelijk sprake is van witwassen of terrorismefinanciering, goed te kunnen detecteren, is een bank wettelijk verplicht te beschikken over beleid, procedures en processen. Een effectief beleid houdt onder andere in dat van iedere cliënt of cliëntgroep een risicobeoordeling en risicoprofiel worden gemaakt en dat het verwachte transactiegedrag meeweegt in de risicobeoordeling. Ook dienen van iedere cliënt of cliëntgroep risicoscore en cliëntrisicoprofiel expliciet vastgelegd te worden, inclusief een omschrijving van de verwachte cliëntactiviteiten en transacties, gegeven de afgenomen producten en diensten. Beleid hierover moet nader worden uitgewerkt in procedures en werkprocessen, waarin u beschrijft hoe de organisatie en haar medewerkers in voorkomende gevallen moeten handelen.

DNB verwacht dat de uitkomsten van de SIRA met betrekking tot de risico's op witwassen en terrorismefinanciering zichtbaar vertaald worden naar beleid en procedures ten aanzien van uw transactiemonitoringsproces.

Good practice

Een bank heeft in haar beleid onder meer vermeld dat additionele beheersmaatregelen zijn genomen voor cliënten voor wie een verhoogd risicoprofiel vastgesteld is. Bij de uitvoering van de SIRA heeft deze bank geconstateerd dat cliënten met een PEP-status een inherent hoger risico vormen. Als onderdeel van haar SIRA-proces en conform het beleid, heeft de bank besloten dat het hogere risico gemitigeerd kan worden door de transacties van deze cliënten verscherpt te monitoren. Aan het reguliere transactiemonitoringsysteem worden daartoe additionele controlemaatregelen voor deze cliëntgroep toegevoegd, die de specifieke risicogedragingen monitoren die voor deze cliënten onderkend zijn.

5.3 Het transactiemonitoringssysteem

Banken beschikken over een (geautomatiseerd) transactiemonitoringssysteem en hebben een onderbouwde en toereikende set aan business rules (detectieregels met scenario's en grenswaarden) om witwas- en terrorisme-financieringsrisico's te detecteren.

DNB verwacht dat uw bank beschikt over een transactiemonitoringssysteem dat passend is bij uw eigen risicoprofiel. Het transactiemonitoringssysteem is bij voorkeur een systeem waarin data vanuit meerdere bronnen geïmporteerd wordt, bijvoorbeeld open bronnen en bronnen van commerciële aanbieders.

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, moet iedere bank een afweging maken tussen kosten, risico's en de in te zetten methode. De manier van monitoren hangt zodoende sterk af van de aard en omvang van uw instelling, en van het aantal transacties dat dagelijks door uw instelling wordt uitgevoerd. Van belang is op te merken dat de wetgever niet eist dat transactiemonitoring geautomatiseerd moet gebeuren. De keuze voor handmatig of automatisch monitoren is dus aan uw bank, maar moet voldoende onderbouwd kunnen worden. Zo verwacht DNB dat een bank in staat is om uit te leggen waarom een handmatig transactiemonitoringssysteem volstaat indien de bank tienduizenden transacties op een dag verricht. Dat kan bijvoorbeeld als de bank kan aantonen dat zij beschikt over voldoende geschikte resources om handmatig te monitoren.

5.3.1 Gebruik van business rules

Zoals uiteengezet in paragraaf 4.1, 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 transactiemonitorings-systeem worden 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 transactiemonitorings-systeem opgenomen business rules risicogebaseerd zijn opgesteld en herleidbaar zijn tot de uitkomsten van de SIRA. Herleidbaar wil zeggen dat een verband bestaat tussen de business rules en de restrisico's die uit de SIRA volgen. De bank legt dit verband vast.

Bij het opstellen van deze business rules houdt de bank rekening met verschillende factoren, zoals:

- het soort cliënt, bijvoorbeeld particulier en zakelijk;
- het cliëntsegment, bijvoorbeeld onderscheid tussen private banking of retail; waarbinnen andere gesegmenteerde doelgroepen zijn te onderscheiden, zoals professionele sportbeoefenaars;
- het cliëntrisicoprofiel, zoals opgesteld bij cliëntacceptatie en mogelijk later aangepast;

- het land waar de transactie naartoe gaat of vandaan komt, bijvoorbeeld hoog-risicoland, EU- of non-EU land;
- het product, bijvoorbeeld sparen, vastgoed-financiering of handelsfinanciering;
- de distributiekanalen, bijvoorbeeld fysieke aanwezigheid van de klant of online;
- de aard en frequentie van de transacties, bijvoorbeeld giraal of contant;
- het risicoprofiel van de cliënt, bijvoorbeeld laag, midden of hoog;
- internationale transacties die vanuit off-shore landen via Nederland doorgeboekt worden naar andere off-shore landen.

De bank zorgt voor voldoende diversificatie in de business rules, zeker als sprake is van meerdere cliëntsegmenten, landen, producten, distributie-kanalen en soorten transacties.

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

Een ander voorbeeld is wanneer in geval van een slapende bankrekening de volgende business rules worden opgesteld:

- 'dormant' scenario (= slapende rekening) voor 6 maanden, waarna plotselinge activiteit;
- een groot verschil (door de bank zelf te definiëren) in de balans op de rekening ten opzichte van een gemiddelde van de laatste 3 maanden;
- transacties van of naar hoog-risicolanden/ financiële organisaties of naar landen waar voorheen nog geen geld vandaan kwam;
- scenario voor zogenoemde 'consultancy payments'.

Verder wordt bij het bepalen van de business rules ook gebruik gemaakt van vergelijkingen met andere transacties van de cliënt, of met informatie over transacties in eerdere perioden, hoe lang de klant al klant is bij uw bank of vergelijking met de leeftijdsgroep, de risicopostcode en/of risicoland.[20]

Good practice

Bij de uitvoering van de SIRA heeft een bank een inherent corruptierisico geïdentificeerd, dat volgt uit transacties van cliënten die geclassificeerd zijn als PEP. De bank bepaalde dat dit risico diende te worden gemitigeerd tot een acceptabel risico om de bankzaken van deze clientgroep te kunnen blijven faciliteren. De bank anticipeerde hierop door binnen haar transactiemonitoringsproces specifieke business rules te implementeren voor het transactiegedrag van PEP's.[21]

20 Een en ander uiteraard met inachtneming van de geldende privacy-bepalingen.

21 PEP staat voor Politically Exposed Persons: voor deze cliënten dient het verscherpt cliënentonderzoek te worden uitgevoerd.

Van belang is dat een bank documenteert op welke wijze zij tot een definitie van een business rule is gekomen, hoe ze doorlopend haar business rules onderhoudt en hoe ze de rules periodiek test, bijvoorbeeld door gebruik te maken van 'backtesting'. Met backtesting wordt bedoeld dat uw bank achteraf de effectiviteit van de toegepaste business rules toetst en waar nodig de business rules aanpast; voor een verdere toelichting wordt verwezen naar 5.3.3.

5.3.2 Business rules in relatie tot terrorismefinanciering

DNB verwacht dat banken specifieke indicatoren voor terrorismefinanciering vertaald hebben in business rules en die vervolgens in hun transactie-monitoringssystemen opgenomen hebben. Alleen transactielimieten volstaan niet, aangezien uitsluitend een laag transactiebedrag uiteraard niet duidt op terrorismefinanciering. Dus zouden banken business rules over transactielimieten moeten koppelen aan andere indicatoren van terrorismefinanciering, bijvoorbeeld lagere grensbedragen voor transacties met risicolanden of regio's in samenhang met bepaald soorten cliënten, zoals stichtingen.

Het detecteren van terrorismefinanciering is dan ook geen statisch proces, maar bij uitstek een gebied waarop uw bank de business rules voortdurend aanpast: de set aan business rules voor detectie van mogelijke terrorismefinanciering wijzigt continu mee met het dynamische karakter van de aan terrorismefinanciering gelieerde activiteit zelf.

Daarnaast kan op basis van het risicoprofiel van een cliënt een lagere limiet worden vastgesteld, voor een hoog-risicocliënt zult u bijvoorbeeld lagere limieten instellen in het transactiemonitoringssysteem.

Tijdens de onderzoeken is gebleken dat de selectie van risicolanden die banken in verband brengen met terrorismefinanciering beperkt of 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, hun risicolandenlijst hierop aanpassen en dit vervolgens vertalen naar hun transactiemonitoringssysteem.

5.3.3 Periodieke evaluatie van business rules: back testing

De business rules worden periodiek onderhouden en getest op effectiviteit.

DNB verwacht dat banken de effectiviteit van het transactiemonitoringssysteem op het gewenste niveau krijgen en houden. In dit verband verwacht DNB dat uw bank dit systeem periodiek evalueert om te beoordelen of gebruikte business rules effectief zijn of mogelijk ineffectief. Dat kan bijvoorbeeld wanneer uw business rules te grofmazig zijn of te hoge grenswaarden hebben, waardoor nauwelijks sprake is van alerts op een bepaalde business rule. Banken voeren daarom een periodieke beoordeling uit, om te beoordelen of bepaalde business rules ten onrechte geen alerts hebben gegenereerd en dat derhalve bijstelling van de bestaande rules mogelijk noodzakelijk is.

Evaluatie van de rules kan plaatsvinden door middel van het zogenoemde 'backtesting'. Op basis van de uitkomsten van uw backtest past u eventueel de business rules van uw transactiemonitorings-systeem aan.

Backtesting kan op verschillende manieren, zoals:

1. Een test waarbij achteraf een selectie van transacties wordt geanalyseerd die binnen de toenmalige configuratie van het systeem niet tot een alert hebben geleid. Het doel hiervan is vast te stellen of deze transacties terecht niet tot een alert hebben geleid, een 'true negative' of dat bepaalde transacties toch indicatief zijn voor mogelijke ongebruikelijk gedrag, een 'false negative'. Indien false negatives worden waargenomen, breidt u de business rules uit of verhoogt u de grensbedragen.
2. Een analyse van de transacties die als mogelijk ongebruikelijk zijn opgemerkt via een andere route dan post-transactiemonitoring. Het doel van deze vorm van backtesting is te analyseren in hoeverre uw transactiemonitoringssysteem in staat is deze ongebruikelijke transactiepatronen en transacties te detecteren.
3. Een test waarbij business rules met veel of alleen maar 'false positive' alerts worden geanalyseerd. Het doel van deze test is te onderzoeken hoe deze business rules, na aanpassing, verhoudingsgewijs meer 'true positives' kunnen genereren.
4. Een test waarbij achteraf de tijdigheid van meldingen van ongebruikelijke transacties wordt geanalyseerd met het doel om dit te verbeteren.

Het doel van deze tests is de business rules verder te optimaliseren en effectiever te maken, zodat deze meer true positive alerts kunnen generen. Gelijktijdig helpen dergelijke tests uw bank de transactiemonitoring zo efficiënt mogelijk uit te voeren.

Good practice

Een bank beschikt over een systeem dat periodiek de effectiviteit van alle business rules evalueert en uit een ruime set aan variabelen (100+) een overzicht creëert van de variabelen die de business rules potentieel verbeteren. In de periodieke controle is een business rule op internationale transacties omhoog gekomen met veel meer false positives op transacties binnen de Europese Unie (EU) dan op transacties buiten de EU. De bank heeft deze waarneming aangevuld met een data- en risicoanalyse, om te na te gaan of bij potentiële aanpassingen de business rule het beoogde risico nog voldoende afdekt. Vervolgens heeft de bank een aanpassing gedaan in de business rule door de grenswaarde voor transacties binnen de EU op te hogen ten opzichte van de grenswaarde voor transacties buiten de EU. De feedback-loop heeft zo geleid tot een business rule met een hogere effectiviteit.

5.3.4 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 om geavanceerde data-analyse en artificial intelligence in te zetten bij de uitvoering van haar transactiemonitoring. Geavanceerde technologie, zoals het gebruik van 'big data' en datamodeling-technieken, vergroot namelijk de mogelijkheden van een instelling om in de beschikbare data mogelijke ongebruikelijke transactiepatronen en afwijkend transactiegedrag op te sporen.

Door meer geavanceerde technologie te gebruiken, zal een bank het risico verminderen dat zij meewerkt aan het witwassen van geld of het financieren van terrorisme. De bank is immers effectiever in staat om mogelijk ongebruikelijk gedrag van een cliënt te detecteren en daarop te anticiperen.

Twee voorbeelden van specifieke technologie voor verschillende onderdelen van beschikbare data zijn:

- 'full-text search' en 'text-mining' op de beschikbare free-form[22] tekst en aan de transactie gerelateerde aanvullende ongestructureerde informatie zoals contracten of andere transactiedocumentatie. Dit kan variëren van het doorzoeken op kernwoorden tot het ontdekken van belangrijke woordpatronen of codewoorden in transactiegegevens; voor terrorismefinanciering kunnen dit bijvoorbeeld de termen "Family Support" of "Gift"[23] zijn;
- 'patroonanalyses en netwerkanalyses' om onderlinge verbanden tussen transacties te detecteren.

Bij de toepassing van geavanceerde technieken als full-tekst search, text-mining, machine learning en clustering, is het van belang de kwaliteit van de algoritmes te meten aan de hand van een referentie-set waarin handmatig verdachte patronen zijn geannoteerd. Dat wil zeggen dat u de patronen 'labelt', zodat bekend is welke patronen en waar in de geteste data de verborgen patronen zitten. Meting kan ook door handmatige analyse van uitgevoerde steekproeven. In dit verband merkt DNB op dat de vakgebieden 'Information Retrieval' en text-mining meetwaardes hanteren als 'precision' en 'recall'. De toepassing hiervan geeft een goede indicatie van de kwaliteit en betrouwbaarheid van de automatische data-analyses.

5.3.5 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 kunnen duiden op witwassen of terrorismefinanciering. 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 geautomatiseerd en standaard bredere transactiepatronen en -structuren en netwerken van transacties te detecteren.

5.3.6 Data-analyse in relatie tot terrorismefinanciering

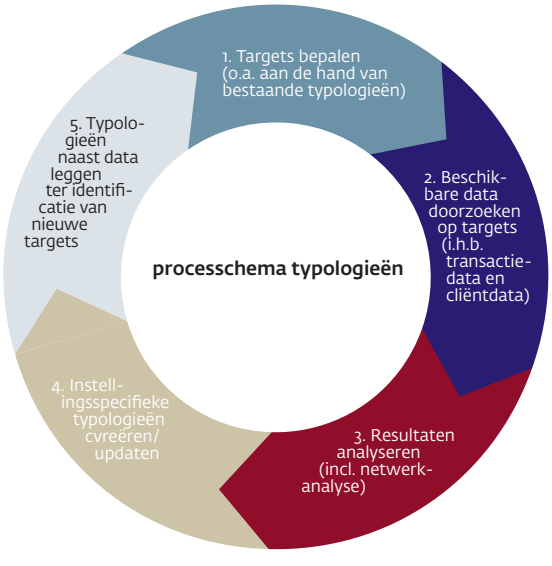
Data-analyse met behulp van targets en typologieën speelt een centrale rol bij het bestrijden van terrorismefinanciering. Banken beschikken over een grote hoeveelheid transactie- en cliëntdata. Van belang is om een proces in te richten waarbinnen deze data continu wordt geanalyseerd om te komen tot relaties met personen die mogelijk verband houden met terrorismefinanciering en nieuwe typologieën.

22 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.

23 Bron: The Egmont Group of Financial Intelligence Units, A global Financial Typology of Foreign Terrorist Fighters; November 2015.

Hieronder is een good practice weergegeven van een processchema[24] 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.

Figuur 3 Processchema typologieën



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.

24 Bron: Western Union.

5.3.7 IT-beheersingsmaatregelen om kwaliteit en volledigheid data te borgen

Banken borgen de kwaliteit en de volledigheid van de data die gebruikt wordt in het transactie-monitoringssysteem, bijvoorbeeld door technische functiescheiding en volledigheidscontroles.

DNB verwacht dat de kwaliteit en de volledigheid van de data bij het gebruik van een geautomatiseerde transactiemonitoringssysteem adequaat zijn geborgd. Belangrijke beheers-maatregelen hiervoor zijn (technische) functiescheiding en controles op de volledigheid van de data. Voor het borgen van de kwaliteit van data is (technische) functiescheiding een wezenlijk onderdeel van de beheersing van processen in betalingsverkeer, om te zorgen dat geen ongewenste en ongecontroleerde aanpassingen plaatsvinden. Functiescheiding kan op meerdere manieren plaatsvinden: functiescheiding tussen twee processen als invoeren en autorisatie, maar ook technische functiescheiding tussen de testomgeving en de productieomgeving.

Om de volledigheid te waarborgen is het van belang dat alle transacties met bijbehorende data vanuit de bronsystemen worden geladen in het transactiemonitoringsysteem. Het waarborgen van de volledigheid kan op verschillende manieren en is afhankelijk van het IT-landschap en de gebruikte bronsystemen. Welke transacties en bijbehorende data moeten worden gecontroleerd dient u vooraf te bepalen, waarna u controlemaatregelen moet vaststellen zowel bij de bronsystemen als bij het transactiemonitoringsysteem. Deze maatregelen hebben betrekking op de kwaliteit (inhoudelijk) van de data en de volledigheid (kwantitatief).

Onderliggend aan genoemde maatregelen is een goede beheersing van het IT-landschap voor het transactiemonitoringproces. DNB raadt daarom aan om periodiek te controleren of dit IT-landschap nog voldoet aan de gestelde eisen en of deze eisen nog overeenkomen aan de risico's:

- Voldoet het IT-deel van de risicoanalyse voor transactiemonitoringproces nog aan de steeds veranderende omstandigheden?
- Zijn de getroffen IT-beheersingsmaatregelen van alle bronsystemen tot het transactie-monitoringsysteem inclusief alle interfaces en tussenliggende platformen op basis van een risicoanalyse nog effectief?
- Bevat het proces geen single-point of failure en is kennis van het transactiemonitoringsysteem voldoende geborgd?
- Beschrijft de documentatie de werkelijke situatie, IT-technisch en niet-IT-technisch zoals business rules?
- Worden de general IT-controles voldoende beheerst?

Tijdens het onderzoek bleek dat de onderzochte banken nauwelijks beschikken 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 maar 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.

Tijdens het onderzoek heeft DNB bij enkele onderzochte 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 deze periodiek te controleren.

5.4 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 tijdig melden van ongebruikelijke transacties aan de FIU-NL is een van de belangrijkste onderdelen van het gehele proces ter bestrijding van witwassen en terrorismefinanciering. De FIU-NL onderzoekt alle gemelde transacties en meldt ze, indien dit onderzoek ertoe leidt dat de gemelde transactie verdacht verklaard wordt, aan de opsporingsinstanties. Zo kunnen uw meldingen van ongebruikelijke transacties leiden tot strafrechtelijk onderzoek. De meldingsplicht van een bank is daarmee essentieel voor opsporen van witwassen en financiering van terrorisme.

In onderstaande paragrafen leest u handvatten voor het alertafhandelings- en meldproces.

5.4.1 Alertafhandelingsproces

Banken beschikken over een adequaat alert-afhandelingsproces. In dit proces zijn per alert overwegingen en conclusies vastgelegd om te komen tot het sluiten dan wel escaleren van alerts.

Een bank beschikt over procedures en werk-processen om alerts te beoordelen en af te handelen. DNB verwacht dat een bank voldoende inzicht heeft in de audit trail en doorlooptijden van vervolgacties naar aanleiding van een alert. Deze procedures en werkprocessen moeten eraan bijdragen dat de doorlooptijden vanaf het genereren van de alert 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. Zoals eerder beschreven is hierbij van belang te documenteren of de betreffende transactie past in het transactiegedrag van cliënt, maar ook of een dergelijke transactie logisch en plausibel is voor het soort cliënt en de sector waarin de cliënt actief is, bijvoorbeeld vanwege het coupuregebruik bij contante transacties, wat in sommige sectoren gebruikelijk is.

DNB constateerde bij de onderzochte banken dat escalatie van alerts naar de 2e lijn veelal ontbrak in het alertafhandelingsproces. Het is daarom van belang dat banken duidelijke richtlijnen bieden voor de gevallen waarin escalatie vanuit de 1e lijn naar de 2e lijn (Compliance) moet plaatsvinden.

Wellicht ten overvloede: DNB verwacht ook dat de bank het adequaat kan onderbouwen als zij vanuit de risiscoafweging de conclusie trekt om juist niet over te gaan tot melding aan FIU-NL.

DNB trof de volgende voorbeelden aan van hoe 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 niet onderbouwd of het gebruikelijk is om auto's in deze prijsklasse contant af te rekenen. Uit een door DNB achteraf opgevraagd transactieoverzicht bleek dat in negen maanden tijd meer dan EUR 550.000 contant bij de bank is gestort. Naar de plausibiliteit van die contante storingen heeft de bank geen (zichtbaar) verder onderzoek gedaan.

Het sluiten van de alert alleen omdat contant geld past in het transactierisicoprofiel, 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 tenminste dat de bank een uitgebreidere analyse doet van 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 twintig 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, maar uit het alertdossier blijkt niet hoe die behandelaar tot deze conclusie is gekomen.

Good practice

Bij een bank wordt door het transactiemonitoring-systeem een alert gegenereerd naar aanleiding van substantiële contante stortingen op een zakelijke rekening. In respons op deze alert wordt in de eerste plaats een brede analyse gemaakt van het cliënt- en transactieprofiel. Hierbij wordt vastgesteld dat de gebruikte rekening op naam staat van een bekende horecagelegenheid aan de Nederlandse kust, en dat in het CDD-dossier geen bijzondere risico's zijn onderkend. Ook uit een additioneel onderzoek naar de achtergrond van de cliënt blijkt een transparante situatie en geen bijzonderheden uit het verleden.

Uit het transactieonderzoek blijkt dat contante stortingen op deze rekening geregeld voorkomen, waarbij het volume maandelijks fluctueert tussen de EUR 5.000 en EUR 15.000. In de zomerperiode is dit volume eenmalig toegenomen tot over de EUR 20.000. In die specifieke periode is het in het risicoprofiel van de cliënt vastgestelde verwachte volume aan contante storingen overschreden.
In het onderzoek wordt vastgesteld dat de contante stortingen ongeveer 19% van de totale inkomsten vormen. In lijn met de guidance kan de alert-behandelaar, na onderzoek, bevestigen dat dit percentage conform de verhoudingen in deze sector zijn. Ook in de zomerperiode blijft de verhouding tussen cash en girale inkomsten beneden de 20%. Dit is te verklaren binnen de reguliere bedrijfsactiviteiten van de cliënt, waarbij een seizoenspatroon en extra inkomsten in de zomerperiode gebruikelijk zijn. Daarnaast wordt vastgesteld dat de uitgaande transacties vooral betrekking hebben op het doen van betalingen aan salaris, inkoop bij horecagroothandels, belastingen en huur. Ook deze uitgaande betalingen passen binnen gebruikelijke activiteiten van een horeca-onderneming.

De alert-behandelaar concludeert op basis van de verrichte analyse dat de contante stortingen niet ongebruikelijk zijn gegeven het cliëntprofiel. Er wordt besloten om de transactie niet als ongebruikelijk door te melden.

5.4.2 Capaciteit en middelen om alerts te beoordelen

DNB verwacht dat banken voldoende capaciteit en (financiële) 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 bank. Om dit te bewerkstelligen kan de bank 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.

Van belang is tot slot ook dat de processen van de banken zodanig zijn ingericht dat risico op vertraging wordt geminimaliseerd.

Good practice

Uit het thema-onderzoek bleek dat één van de onderzochte banken in de praktijk bij de alertafhandeling het uitgangspunt hanteert "kwaliteit gaat voor snelheid".[25] 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.

Good practice

Banken hebben de mogelijkheid om een spoedmelding bij FIU-Nederland te doen. Een van de onderzochte banken maakte van deze mogelijkheid gebruik in een geval waarbij ze zagen dat de patronen op de rekening veel weg hadden van een zogenoemde "ponzi-fraude". Dankzij de spoedmelding van de bank kon de politie na het ontvangen van de door FIU-NL verdacht verklaarde transactie-informatie snel een onderzoek starten en beslag leggen op het door de fraudeurs buitgemaakte geld, voordat het weggesluisd kon worden .

25 Snelheid wil zeggen zo snel mogelijk afwerken van de alerts teneinde achterstanden te voorkomen.

Good practice

Een bank stelt zichzelf op de hoogte van de nieuwste ontwikkelingen op het gebied van witwassen en terrorismefinanciering en heeft daarbij ook oog voor betaalmethodes zoals bitcoins of andere virtuele betaalmiddelen.[26] Een van de onderzochte banken liep in de alertafhandeling aan tegen een klant die veel contante geldopnames deed nadat zijn bankrekening gevoed was met girale overboekingen afkomstig van bedrijven die bitcoins en andere cryptovaluta aan- en verkopen. De bank deed melding van de ongebruikelijke transacties.

Na onderzoek van FIU-Nelderland en de FIOD bleek dat de klant een zogenaamde "bitcoincasher" was. De bitcoincashers kopen bitcoins van handelaren die deze bitcoins vermoedelijk hebben verkregen door te handelen in illegale goederen op Dark Web waarbij bitcoins als betaalmiddel worden gebruikt. De bitcoincashers verkopen vervolgens op legale bitcoinplatforms deze bitcoins voor euro's aan zogenaamde exchange-kantoren. De opbrengsten van deze verkopen worden na ontvangst op de bankrekening contant opgenomen in euro's.

5.4.3 Alerts in relatie tot risico op terrorisme-financiering

DNB verwacht dat een bank voor het detecteren van terrorismefinanciering beschikt over een lijst met red flags en mogelijke business rules die kunnen duiden op terrorismefinanciering. Deze lijst dient te zijn toegespitst op het risicoprofiel van de bank en – indien mogelijk – te worden vertaald naar business rules om risico's op terrorismefinanciering te detecteren. Tevens verwacht DNB dat een bank daarbij gebruik maakt van actuele guidance en nieuwsbrieven van DNB en FIU-NL, alsmede internationale publicaties, waaronder FATF.

Good practice

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.

26 DNB heeft in juli 2014 de sector banken in het kader van het thema onderzoek "Nieuwe betaalmethoden" gewezen op het hoge risicoprofiel van deze betaalmiddelen.

Good practice

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

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 alle transacties, zowel de pin-transactie als de beide aangevraagde leningen. 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.

5.4.4 Meldproces

Banken beschikken over een adequaat meldproces. Banken zorgen ervoor dat voorgenomen en uitgevoerde ongebruikelijke transacties onverwijld en volledig aan de FIU-NL worden gemeld.

Volgens de wet moeten instellingen onverwijld melden, zodra het ongebruikelijke karakter van een transactie bekend is geworden. Naast een melding aan FIU-NL is het mogelijk 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. Wellicht ten overvloede moet ook, mocht sprake zijn van een incident, gemeld worden bij DNB.[27]

Het spreekt voor zich dat u als bank ongebruikelijke voorgenomen en uitgevoerde transacties onverwijld en volledig aan de FIU-NL meldt. Daarbij is belangrijk dat uw bank beschikt over een procedure hoe het meldproces er intern uit ziet en waaruit blijkt hoe in voorkomende gevallen gehandeld dient te worden. Belangrijk 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 worden heroverwogen.

De bank draagt zorg voor adequate (beschreven) processen om transacties, waarbij aanleiding is om te veronderstellen dat deze verband kunnen houden met witwassen of financieren van terrorisme, onverwijld 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 de 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 ongebruikelijke transacties, beveiliging van informatiestromen en dat hierover guidance en training wordt verstrekt aan betrokken medewerkers. Deze guidance en training zijn vooral van belang voor eerstelijnmedewerkers die contact hebben met cliënten. Voor deze medewerkers is het essentieel om te weten wanneer mogelijk sprake is van ongebruikelijke transacties, welke vragen dan aan een cliënt gesteld moeten worden en welke informatie onder geen beding aan de cliënt 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 uitkomsten van een onderzoek weegt de bank mee in de bestaande risicobeoordeling van de cliënt.

27 Zie ook artikel 12, Bpr.

De bank meldt onverwijld aan FIU-NL

In de in 5.4.3 beschreven casus vonden transacties plaats met een land met een hoger TF-risico, waarbij de bank vanuit berichtgeving in de media een relatie van een cliënt met een uitreiziger had opgemerkt. Deze informatie werd 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 met een kortere doorlooptijd 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 langere doorlooptijd de gewenste zorgvuldigheid in de behandeling van de alert en het feit 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 over de melding noch over de manier waarop 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.

5.4.5 Heroverwegen risicoclassificatie cliënt

Indien de onderzoeksresultaten van de alert daar aanleiding toe geven, verwacht DNB dat de instelling het bestaande risicoprofiel van de cliënt opnieuw bekijkt om te bepalen of redenen bestaan om dit profiel aan te passen. Dit kan bijvoorbeeld door middel van een zogenoemd 'event driven review'. Op deze wijze borgt de instelling dat het risicoprofiel van de cliënt en daarmee diens risicoclassificatie 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 indien van toepassing terugmeldingen ontvangen) mogelijkheden hebben om zelf het risicoprofiel van de cliënt te herbeoordelen. Ook verwacht DNB dat deze analisten aan de medewerkers die verantwoordelijk zijn voor de cliëntbeoordeling aan kunnen geven dat herbeoordeling noodzakelijk is. DNB verwacht in dit verband ook dat banken door middel van het quality assurance-proces monitoren of dergelijke herbeoordelingen adequaat worden uitgevoerd. Het alertafhandelingsproces kan daarnaast ook inzichten bieden in de effectiviteit van de ingestelde business rules. De eerstelijnsmedewerker kan hier een belangrijke rol spelen en input leveren voor het periodiek evalueren van de business rules.

Good practice

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 cliënt op onacceptabel geplaatst.

5.4.6 Objectieve indicatoren voor automatisch melden

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.

5.5 Governance

Banken hebben hun governance ten aanzien van transactiemonitoring zodanig ingericht dat sprake is van een duidelijke functiescheiding, bijvoorbeeld via de three lines of defense model.

Bij de beoordeling van dit onderdeel van het volwassenheidsmodel, is als uitgangspunt genomen het zogenoemde 'three lines of defence model'. Hiervoor is gekozen omdat de huidige praktijk leert dat banken veelal dit model toepassen in hun governance. Dit wil echter niet zeggen dat andere assurance-modellen niet zouden kunnen volstaan. Van belang is echter dat in het model te allen tijde het element van onafhankelijke controletechnische functiescheiding voldoende is geborgd. Het spreekt daarbij voor zich dat banken dienen te beschikken over een onafhankelijke compliancefunctie[28] en een onafhankelijke interne-controlefunctie, veelal de internal audit-functie.

Good practice

Alle onderzochte banken beschikken over een onafhankelijke interne-controlefunctie, vaak de derdelijnsfunctie, ofwel de interne accountants-functie. Deze onafhankelijke controlefunctie vormt door middel van audits periodiek een oordeel over de opzet, het bestaan en de werking van het transactie-monitoringssysteem en -proces. Deze audits waren over het algemeen van goede kwaliteit en bevindingen werden adequaat opgevolgd. Een bank monitorde daarnaast maandelijks de voortgang van de actiepunten die door de business waren opgesteld naar aanleiding van de auditrapportage. Daarbij paste de interne accountantsfunctie een integrale benadering (ketenbenadering) toe.

28 Bpr artikel 21.

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.[29]

De bank geeft aan wat de adviserende taak van compliance in relatie tot transactiemonitoring inhoudt, bijvoorbeeld hoe dient te worden omgegaan met het advies van compliance ten aanzien van hoog–risico-gevallen. 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 tweedelijnsorganisatie-onderdeel 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 interne controlefunctie, met voldoende frequentie het functioneren van de eerste en tweede lijn controleert. Daarbij zorgt de organisatie ervoor dat zij voldoende capaciteit – zowel kwantitatief als kwalitatief - 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 uw bank beschikt over adequate en periodieke managementinformatie die inzicht geeft in deze signalen en uitkomsten, opdat u daarop tijdig kan sturen. Zodoende vervult Compliance naast haar adviserende en controlerende rol, tevens een rapporterende rol ten aanzien van transactiemonitoring. Deze rol bestaat reeds bij het merendeel van de onderzochte banken. DNB verwacht in de periodieke verantwoordingsrapportage van Compliance expliciete managementinformatie over de belangrijkste uitkomsten van haar transactiemonitoring.

29 In dit verband merkt DNB op dat mogelijk in de nog te herziene Wwft (op grond van de huidige teksten van de Vierde Anti-Witwasrichtlijn) over de compliancefunctie het volgende zal worden opgenomen: "de compliancefunctie is gericht op het controleren van de naleving van wettelijke regels en interne regels die de instelling zelf heeft opgesteld en heeft onder meer als taak het verstrekken van de gegevens, bedoeld in artikel 16 Wwft, aan de FIU-NL".

5.6 Training en awareness

Banken beschikken over een toegesneden trainingsprogramma voor hun medewerkers. De medewerkers zijn zich bewust van witwas- en terrorismefinancieringsrisico's.

DNB constateert dat banken trainingen over de Wwft hebben opgenomen in een (jaarlijks gewijzigd) trainingsprogramma. DNB verwacht dat hierbij de inhoud van dit programma is afgestemd op de medewerkers, bijvoorbeeld door een juiste adressering per doelgroep: van bestuur en senior management tot junior medewerker. Daarnaast verwacht DNB dat de training is aangepast op het niveau van de medewerkers, rekening houdend met competenties en ervaring, alsmede dat gebruik wordt gemaakt van casuïstiek vanuit het eigen transactiemonitoringsproces. Bij het opstellen van de inhoud van het trainingsprogramma kan gebruik worden gemaakt van de casuïstiek van de FIU-NL: iedere twee weken publiceert de FIU-NL nieuwe casussen.

Good practice

Een van de onderzochte banken beschikt 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 waren.

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 het voorkomen van terrorismefinanciering.

Begrippenlijst

Alert
Een signaal dat duidt op een mogelijk ongebruikelijke transactie.

Alert afhandelaar
De medewerker die de alert analyseert, onderzoekt en vastlegt.

Backtesting
Het testen en optimaliseren van een bepaalde aanpak op basis van gegevens uit het verleden.

Business rules
De set aan detectieregels die in het transactiemonitoringssysteem wordt toegepast, die bestaan uit de toegepaste scenario's en bepaalde grenswaarden.

Cliënt
Natuurlijke persoon of rechtspersoon met wie een zakelijke relatie wordt aangegaan of die een transactie laat uitvoeren.

Cliëntenonderzoek
Het onderzoek zoals bedoeld in artikel 3 van de Wwft.

Cliëntrisicoprofiel
Beschrijving van een cliënt in risicocategorieën; zie ook DNB Leidraad Wwft/SW, pagina 11 en 12.

Event-driven review
Op grond van gebeurtenis of incident verricht de bank een cliënten onderzoek.

Financieel Economische Criminaliteit
Witwassen, corruptie (omkoping), financiering van terrorisme, handel met voorwetenschap, niet naleven van sancties en ander crimineel gedrag (bijvoorbeeld verduistering, oplichting en valsheid in geschrifte).

Indicatoren
Aanwijzing en/of signaal, waarbij mogelijk sprake is van witwassen of financiering van terrorisme.

Meldproces
Het proces van melden bij de FIU-NL; een melding als bedoeld in artikel 16, eerste lid van de Wwft.

Peergrouping
Het definiëren van cliëntgroepen met soortgelijke kenmerken.

SIRA
Systematische integriteitsrisico analyse, zoals bedoeld in artikel 10 Bpr.

Targets
Targets zijn subjecten die in verband worden gebracht met (de financiering van) terrorisme.

Transactie
Handeling of samenstel van handelingen van of ten behoeve van een cliënt waarvan de instelling ten behoeve van haar dienstverlening aan die cliënt heeft kennisgenomen.

Transactiedata
Alle gegevens die betrekking hebben op de transactie.

Transactieprofiel
Het bepalen van het profiel op basis van de verwachte transacties of het verwachte gebruik van de rekening van een cliënt.

Typologie
(groepen van) Kenmerken die duiden op het financieren van terrorisme.

Verwacht transactiegedrag
Het verwachte gedrag van de transacties van de cliënt.

Voortdurende controle
Continue bewaking, permanente controle.

Disclaimer

In deze guidance 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 toezichthouder-regelingen 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.

De Nederlandsche Bank N.V.
Postbus 98, 1000 AB Amsterdam
020 524 91 11
dnb.nl