nederlandse vereniging van banken

NVB Risicogebaseerde Standaard

Ongoing Due Diligence (ODD)

sterke banken
sterke samenleving

Context

Inleiding

De Nederlandse bankensector heeft behoefte aan een meer risicogebaseerde benadering om financiële criminaliteit effectief te bestrijden. De sector is daarom aan de slag gegaan met het in de praktijk brengen van de risicogebaseerde aanpak om te voldoen aan de wettelijke eisen [1] van de 'Wet ter voorkoming van witwassen en financieren van terrorisme' (hierna: Wwft). Deze praktische implementatie van de risicogebaseerde aanpak wordt ondersteund en aanbevolen door de Nederlandse AML toezichthouder, De Nederlandsche Bank (hierna: DNB). In 2022 heeft DNB het rapport 'Van herstel naar balans' gepubliceerd [2]. Hieruit volgde een reeks van risicogebaseerde rondetafelgesprekken met de Nederlandse bankensector. Het doel van deze gesprekken is om effectieve beheerskaders voor financiële criminaliteit op te stellen en de relevante risico's op witwassen (hierna ML) en financieren van terrorisme (TF) adequaat te kunnen beoordelen. Met een risicogebaseerde aanpak kunnen capaciteit en middelen proportioneel worden ingezet op hogere risico's. Deze aanpak heeft invloed op het Ongoing Due Diligence (hierna: ODD) framework van banken [3], dat gericht is op continue controle van de ML/TF risico's.

Deze NVB Risicogebaseerde Standaard richt zich op:

- de transitie naar een situatie waarin banken vertrouwen op een (geautomatiseerd) ODD framework op basis van risicotriggers en relevante Event Driven Reviews (hierna: EDRs), waardoor
- risicogedifferentieerde reviews kunnen worden uitgevoerd.

Dit document bevat dan ook geen volledig overzicht van alle componenten van het ODD framework. Dit document richt zich op het toepassen van de risicogebaseerde aanpak en de voorwaarden om relevante EDRs uit te voeren in plaats van standaard periodieke reviews (hierna: PRs) op basis van het verstrijken van een vaste periode. Vanuit risicoperspectief kan de relevantie van een PR beperkt zijn, hoewel ze in sommige gevallen onderdeel kunnen zijn van de beheersmaatregelen voor financiële criminaliteit.

Met de hierboven genoemde praktische implementatie van de risicogebaseerde aanpak hebben banken een effectievere en geautomatiseerde aanpak ter beschikking om de ML/TF risico's te detecteren, namelijk door het klantgedrag continu te monitoren, de zogeheten klantmonitoring. Klantmonitoring maakt gebruik van risicotriggers op basis van zowel statische gegevens als het klantgedrag. In het algemeen neemt hierdoor de kwaliteit van de gegenereerde alerts en events en de effectiviteit van de (geautomatiseerde) detectie van risico's toe. Dit komt onder andere door de automatisering van de actualisatie van klantgegevens en betere, geavanceerdere risicodetectiemechanismen. Door het toevoegen van klantmonitoring aan de detectiemechanismen voor ML/TF risico's neemt de toegevoegde waarde van de tijd en de inspanningen die worden besteed aan periodieke reviews af. Hierdoor kan een stapsgewijze en zorgvuldige implementatie plaatsvinden van de transitie naar het uitvoeren van relevante EDRs.

1 Het overkoepelende doel van banken is om misbruik van het financiële systeem voor witwassen en het financieren van terrorisme te voorkomen.
2 Van herstel naar balans; Een vooruitblik naar een meer risico-gebaseerde aanpak van het voorkomen en bestrijden van witwassen en terrorismefinanciering (DNB, 2022).
3 Hierbij merken we op dat andere processen (zoals de screening van transacties) ook worden gebruikt om te voldoen aan (onderdelen van) de sanctiewetgeving en als doel hebben om bepaalde sanctierisico's te beperken.

In deze NVB Standaard komen de volgende belangrijke uitgangspunten aan bod:

- Banken kunnen ODD uitvoeren op een risicogebaseerde manier (dus op basis van relevante EDRs in plaats van PRs als standaard CDD-methode).
- Banken bepalen zelf welke CDD-methoden zij toepassen om te voldoen aan de Wwft.
- De voorwaarden in deze NVB Risicogebaseerde Standaard moeten door banken gelezen worden als overwegingen om rekening mee te houden bij het toepassen van de risicogebaseerde aanpak. Het zijn geen minimumeisen waaraan banken eerst moeten voldoen voordat zij kunnen vertrouwen op hun (geautomatiseerde) ODD framework op basis van risicotriggers. Banken bepalen naar eigen inzicht of het door hen geïmplementeerde framework voldoende effectief is om (deels) niet meer te hoeven terugvallen op PRs.
- De risicogebaseerde processen van banken en de volwassenheid van deze processen zullen in de loop van de tijd verder ontwikkelen en verbeteren, naarmate de banken meer inzichten vergaren over de uitvoering van zo'n framework.

Het ODD framework bestaat uit drie kernelementen:

- **Klantgegevens**, dit heeft betrekking op het proces om de relevante gegevens structureel actueel te houden. Veel banken verschuiven van het periodiek versturen van informatieverzoeken aan de klant naar een meer op risicogebaseerde en geautomatiseerde manier om de klantgegevens te updaten, bijvoorbeeld door koppelingen met externe bronnen (zie NVB Standaard 'Actualisatie van klantgegevens', april 2023).
- **Het genereren van alerts en events,** dit is het toepassen van risicodetectiemechanismen om klanten continu te screenen en hun gedrag te monitoren. Hierbij nemen banken risicoanalyses in overweging, zoals de National Risk Assessment (NRA) en Systematische Integriteitsrisicoanalyse (SIRA) [4] [5]. Deze kunnen worden aangevuld met andere interne informatie (zoals inzichten en lessons learned vanuit de uitkomsten van alert en event handling en externe bronnen, bijvoorbeeld internationale rapporten, publicaties, datalekken enz.). Veel banken verbeteren hun processen om alerts en events te genereren continu, door klantgegevens effectiever en efficiënter te analyseren om ML/TF risico's te detecteren op een risicogebaseerde manier (zie ook de NVB Standaarden 'Modellen voor het genereren van alerts en events' van juli 2023 en 'Verwacht transactieprofiel' van april 2023).
- **De handling van alerts en events,** dit is de risicogebaseerde aanpak om alerts en events die zijn gegenereerd te behandelen (indien van toepassing), evenals meldingen van klanten waarbij potentiële risico's zijn vastgesteld (zie paragraaf 1.3).

4 Ook bekend onder de naam Enterprise-wide Risk Assessment (EWRA) of Firm-wide Risk Assessment (FWRA)

5 Banken kunnen ook de EBA Guidelines inzake CDD in overweging nemen, zie het persbericht van de Europese Bankautoriteit (EBA) van 1 maart 2021.

De positionering binnen het Financial Crime Framework

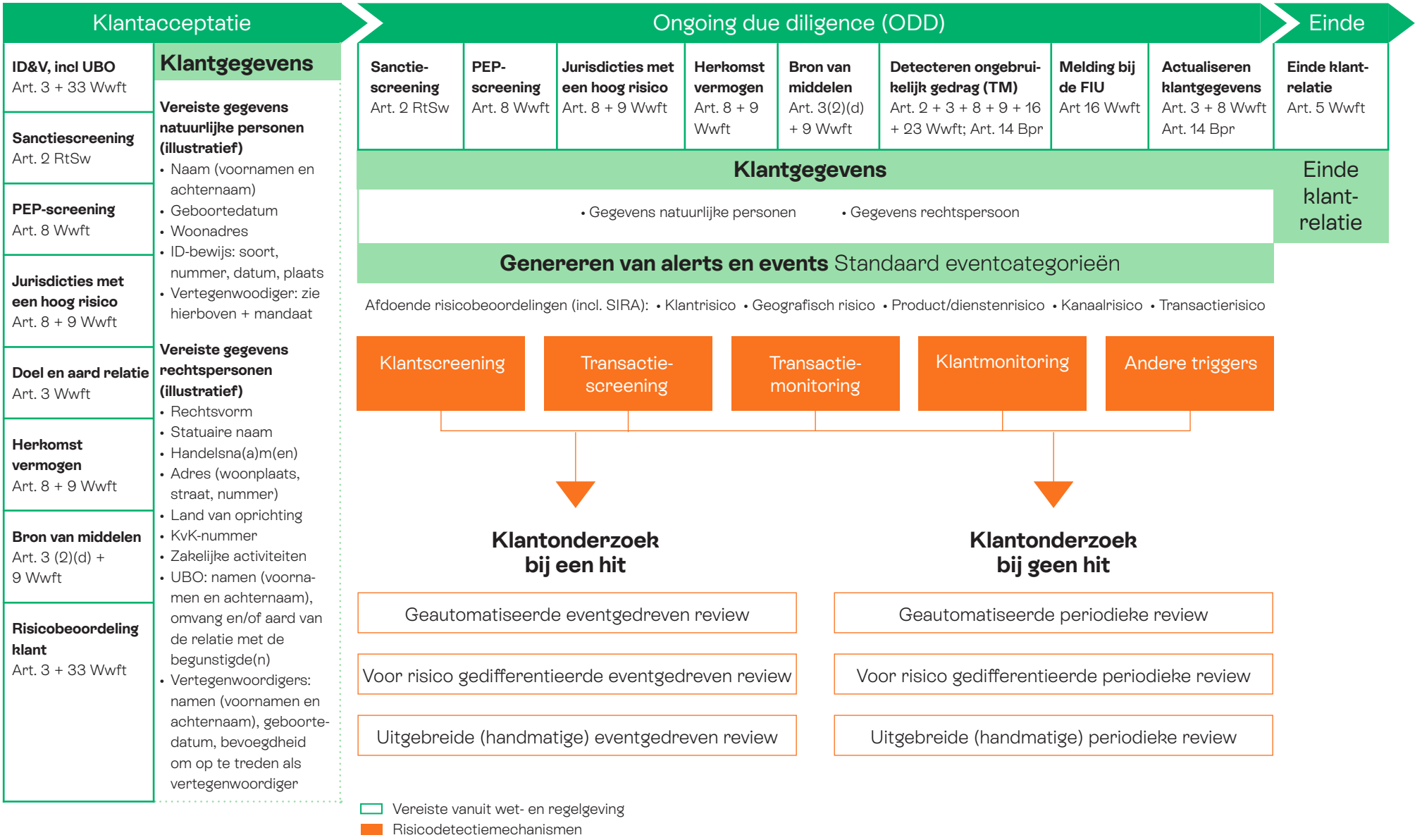
Het ODD framework bestaat uit fundamentele componenten die verplicht zijn voor effectieve ODD. Dit framework bevat een aantal processen en maatregelen voor continue screening en monitoring door banken nadat zij een klant hebben geaccepteerd.

Financial Crime Framework – traditioneel en risicogebaseerd

- Op pagina 4 staat het traditionele Financial Crime Framework, waarin PRs een aanzienlijk onderdeel zijn van de ODD beheersmaatregelen. Om een meer risicogebaseerde aanpak toe te passen, zijn de eerste banken al begonnen met het toepassen van klantmonitoring en minder met het standaard uitvoeren van PRs.
- Op pagina 5 staat het risicogebaseerde Financial Crime Framework, waarbij standaard triage voor de handling van het alert/event plaatsvindt bij alerts en events die door risicotriggers zijn gegenereerd. In dit framework vertrouwen banken onder andere op klantmonitoring binnen hun risicodetectiemechanismen voor ML/TF risico's. Hierdoor kan er een stapsgewijze en gecontroleerde transformatie plaatsvinden naar een situatie waarbij banken kunnen vertrouwen op effectieve EDRs.

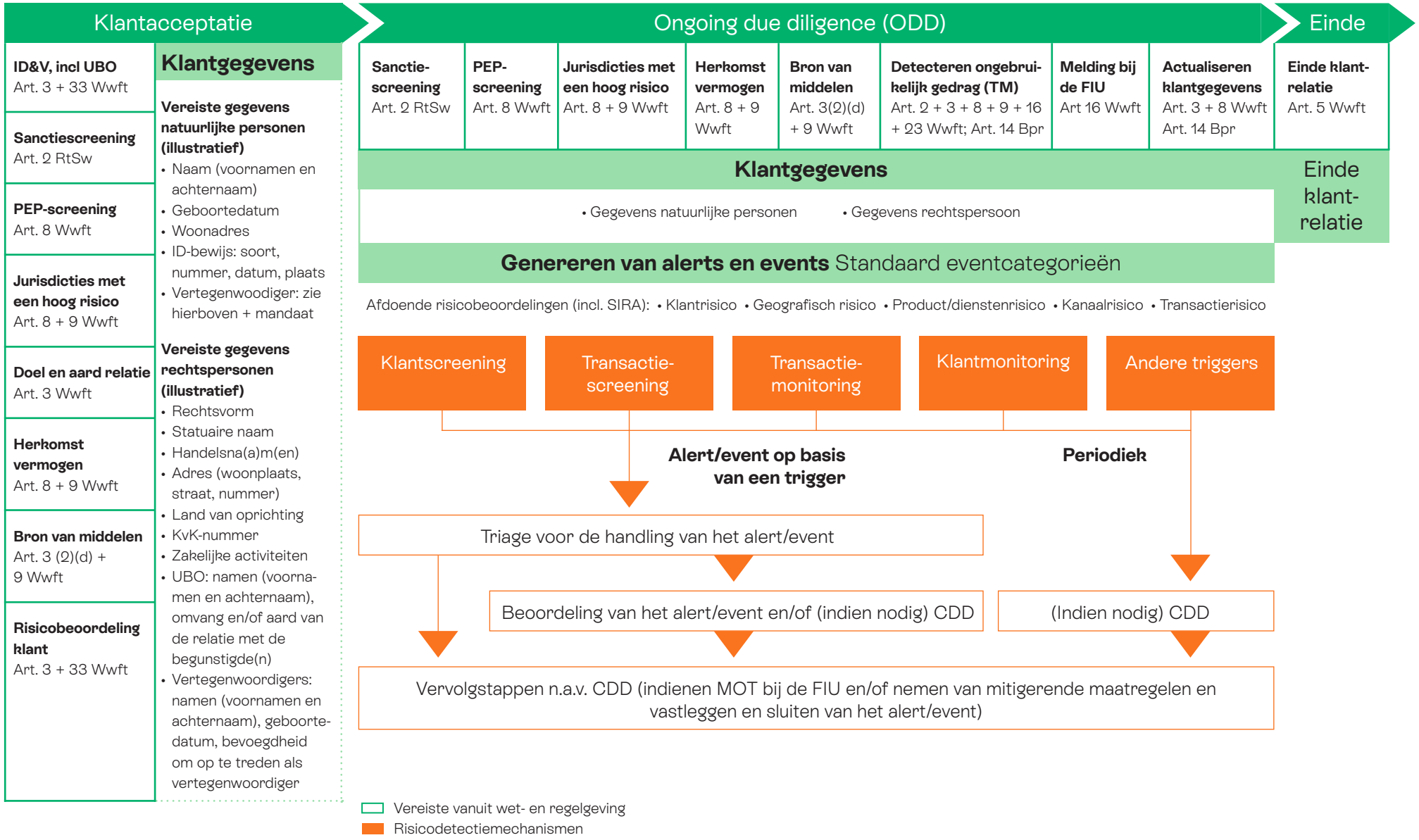
Financial Crime Framework

Traditioneel



Financial Crime Framework

Risicogebaseerd



NVB Risicogebaseerde Standaard

1 NVB Standaard

Deze NVB Standaard beschrijft de praktische implementatie van de risicogebaseerde uitvoering van het ODD framework in de Nederlandse bankensector. Banken moeten hun ODD framework continu bijwerken om de ML/TF risico's op de meest effectieve en proportionele manier te beheersen en te beperken. Deze risico's en de mitigerende maatregelen kunnen bijvoorbeeld worden afgeleid uit de risicoanalyses van de bank (bijvoorbeeld SIRAs), gebaseerd worden op een gedegen inzicht in de klantenportefeuille en de producten die de bank aanbiedt, en afgestemd worden op de risicobereidheid van de bank. Deze inzichten in de risico 's kunnen worden aangevuld met de National Risk Assesment (NRA), supranationale risicoanalyses en andere bronnen.

Voor het operationaliseren van een goed ontwikkeld (geautomatiseerd) ODD framework op basis van triggers, moeten banken beschikken over proces- en beheerskaders die aan interne audits kunnen worden onderworpen. De processen en de volwassenheid daarvan zullen daarbij in de loop van de tijd verder ontwikkelen en verbeteren, naarmate de banken meer inzichten vergaren over de implementatie van zo'n framework.

1.1 De voorwaarden voor het operationaliseren van een (geautomatiseerd) [6] ODD framework op basis van triggers

Het ODD framework stelt banken in staat klanten, inclusief hun transacties en gedrag, continu te screenen en te monitoren, met als doel het detecteren van ongebruikelijke transacties, te zorgen dat de risicoclassificatie van de klant actueel blijft en vast te stellen welke acties nodig zijn naar aanleiding van de risico's van de klant. Banken mogen met dit kader afstappen van PRs voor hun gehele klantpopulatie en vertrouwen op de actualisatie van klantgegevens en (gedeeltelijk) geautomatiseerde riscoanalyses.

Om een (geautomatiseerd) ODD framework op basis van triggers te operationaliseren, moeten banken de volgende voorwaarden in overweging nemen.

- Door middel van continue verbeterprocessen voor datakwaliteit streven banken ernaar dat relevante klantgegevens compleet en juist zijn. De kwaliteit van de relevante klantgegevens moet binnen de risicobereidheid van de bank vallen en onderhevig zijn aan regelmatige monitorings- en feedback loops. De bank actualiseert de gegevens op basis van op regels en/of modellen gebaseerde alerts en events of op basis van gegevens die zijn verkregen uit externe bronnen, interne analyse of informatieverzoeken aan de klant (zie de NVB Standaard 'Actualisatie van klantgegevens' april 2023).
- De bank beschikt over geautomatiseerde risicodetectiemechanismen en alerts en events worden eveneens automatisch gegenereerd (op basis van transactiepatronen, klantgedrag en wijzigingen in de klant- of transactiegegevens) en deze zijn bewezen effectief. Er moet passend beheer zijn op deze mechanismen, bijvoorbeeld in het geval van modellen in overeenstemming met het model risk management framework van de bank.
- De risicotriggers moeten effectief de mogelijke risico's binnen de klantportefeuille en de risicoanalyses van de bank afdekken (zie paragraaf 1.2). Banken moeten aantonen dat hun detectiewerkzaamheden adequaat zijn (op basis van monitorings-, audit- en continue verbeterprocessen). Als er sprake is van tekortkomingen, moet de bank mitigerende maatregelen nemen om het probleem op te lossen. Dit zou bijvoorbeeld het reviewen van een specifieke klantgroep kunnen zijn.

6 Niet ieder risico kan worden vastgesteld door geautomatiseerde risicotriggers. Dit gaat dan bijvoorbeeld over situaties waarvan banken kennis nemen via thematische onderzoeken, portefeuille-analyses of medewerkers.

- Banken borgen naleving van wet- en regelgeving (zodat de risicogebaseerde aanpak in lijn is met de wettelijke vereisten die van toepassing zijn). Banken reageren op veranderingen in de eigen risicopositie en op veranderingen in de wet- en regelgeving.
- Banken zorgen voor een adequate opzet en implementatie van EDR processen en een adequate operationele effectiviteit van deze processen, in lijn met de interne beleidsmaatregelen en procedures waarin de methodologie en de reikwijdte van deze aanpak staan beschreven, evenals de functies en verantwoordelijkheden [7]. Daarnaast moeten de opzet en implementatie voldoen aan alle interne beleidsmaatregelen van de bank, waaronder bijvoorbeeld het privacybeleid.
- Banken zorgen voor adequaat toezicht op effectieve EDR processen (bijvoorbeeld op de doorlooptijden, operationele inzichten, prioriteiten en de effectiviteit) op basis van adequate managementinformatie.
- Alerts en events worden binnen de relevante doorlooptijd verwerkt, in overeenstemming met de risicobereidheid van de bank.

1.2 Voorwaarden voor geautomatiseerde risicodetectiemechanismen

Banken die gebruikmaken van geautomatiseerde risicodetectiemechanismen (zoals transactiescreening, klantscreening, transactiemonitoring en klantmonitoring) zorgen dat zij voldoende vertrouwen hebben (op basis van de monitorings-, audit- en continue verbeterprocessen) dat deze processen adequaat voorzien in de wettelijke verplichtingen en dat zij de geïdentificeerde potentiële risico's beperken, waaronder de inherente risico's die zijn vastgesteld in de risicoanalyses (waaronder SIRA).

Banken kunnen het gebruik van geautomatiseerde risicodetectiemechanismen voldoende onderbouwen zonder nog PRs te gebruiken, door aan de volgende voorwaarden te voldoen.

- Banken streven continu naar volledigheid van de risicotriggers om de potentiële risico's van de klantportefeuille en van de risicoanalyses van de bank effectief te beheersen, en van de mitigerende maatregelen die zijn opgenomen in de risicoanalyses van de bank (waaronder SIRA). De kwaliteit van de risicotriggers ligt binnen de risicobereidheid van de bank en wordt regelmatig gemonitord en verbeterd op basis van feedback loops. Hierbij merken we op dat een een 100% dekking van van de risico's niet haalbaar is.
- Banken handhaven een adequaat niveau van risicobeperking en zorgen voor continue verbetercycli van de risicodetectiemechanismen (bijvoorbeeld door feedback loops) en dat deze operationeel effectief zijn.
- Banken beschikken over relevante managementinformatie (waaronder informatie over de effectiviteit) waaruit blijkt dat de resultaten van de geautomatiseerde risicodetectiemechanismen in lijn zijn met de daadwerkelijke risico's binnen de klantportefeuille.

1.3 Handlingmethoden

Als klantmonitoring een integraal onderdeel is van ODD processen, kunnen banken relevante veranderingen in de klantsituatie vaststellen. Soms veroorzaakt een verandering in de klantsituatie een trigger om het vastgestelde risico te beoordelen door het alert of event te behandelen.

Banken passen een risicogebaseerde aanpak toe bij het opstellen van de handlingmethoden voor alerts en events. Het doel van alert- en eventhandling is om het alert of het event adequaat op te volgen door het risicoprofiel van de klant te bevestigen of aan te passen, mitigerende maatregelen te nemen (indien nodig) en/of een MOT in te dienen bij de FIU.

7 Art.10 Bpr verplicht instellingen om hun eigen beleidsmaatregelen en procedures na te leven.

* Dit diagram is een vereenvoudigde weergave en is bedoeld als illustratie. Let op, voor verschillende risicodetectieprocessen (transac tiescreening,transactiemonitoring, klantscreening, klantmonitoring) zijn verschillende en specifiekere processen van toepassing.

Risicodetectiemechanisme Risicogebaseerde handlingmethode

Banken richten hun handlingprocessen in en leggen deze vast in lijn met hun interne processen en toepasselijke methoden voor de handling van alerts en events, en houden hierbij rekening met wettelijke verplichtingen, specifieke risico's, de klantportefeuille, de producten die worden aangeboden en de risicobereidheid van de bank.

Banken zijn niet verplicht om standaard voor iedere klant periodiek uitgebreide (handmatige) reviews uit te voeren (zoals de traditionele PRs) wanneer er een goed onderbouwd en effectief ODD framework op basis van triggers is opgesteld. Banken kunnen tegelijkertijd geautomatiseerde, risicogedifferentieerde en uitgebreide methoden uitvoeren voor verschillende delen van hun klant-portefeuille om te zorgen dat middelen op een risicorelevante en proportionele manier worden ingezet.

De risicogebaseerde aanpak voor handling van alerts en events kan als volgt worden gevisualiseerd. Om te zorgen dat de middelen van de bank zo effectief mogelijk worden ingezet, gebruiken banken een risicogebaseerde aanpak. Hierin vinden de volgende activiteiten plaats:

- triage voor de handling van het alert/event (waarbij de handlingmethode wordt vast-gesteld);
- geautomatiseerde handling en het geautomati-seerd sluiten van alerts en events;
- handling van een alert of een event door een analist door middel van:

  - een risicogedifferentieerde review (waarbij alleen het vastgestelde risico wordt beoordeeld), en/of
  - een uitgebreide review (waarbij de klant als geheel wordt beoordeeld).

Bij het bepalen welke handlingmethode de bank moet toepassen, moet de bank rekening houden met de volgende overwegingen.

- De volwassenheid van de identificatie en de coverage van de ML/TF risico's door de risicodetectieprocessen van de bank. Banken moeten voldoende vertrouwen hebben in hun ODD processen om te kiezen voor een risicogedifferentieerde EDR (zie de voorwaarden onder 'Handling m.b.v. een risicogedifferentieerde review'). Het vertrouwen dat de bank hierin heeft, wordt gebaseerd op onder andere het testen van het proces en de resultaten vanuit monitoring en audits.
- De risico's van de bank zoals vastgesteld in de risicoanalyses van de bank. De handlingmethoden moeten in lijn zijn met de SIRA-resultaten en de risicobereidheid van de bank. Meer specifiek moeten deze in lijn zijn met de risico's die volgen uit de klantportefeuille en het productenaanbod van de bank (zo kan de handlingmethode per klant of klantgroep verschillen) en in lijn zijn met de risico's gerelateerd aan de alerts en de events die zijn gegenereerd. Ook de complexiteit van de klant of het risicoprofiel van de klant kan hierbij relevant zijn; zeer complexe klanten vereisen mogelijk meer kennis bij werknemers en een intensievere afhandeling. Voorbeelden van complexe klanten zijn per bank verschillend. Minder complexe klanten komen eerder in aanmerking voor risicogedifferentieerde reviews of voor het automatisch sluiten van alerts en events.
- Banken streven naar volledige en juiste relevante klantgegevens door de kwaliteit van die gegevens continu te verbeteren, waarbij de kwaliteit van de relevante klantgegevens binnen de risicobereidheid van banken valt en onderhevig is aan regelmatige monitorings- en feedback loops. Banken actualiseren de gegevens op basis van op regels en/of modellen gebaseerde alerts en events of op basis van gegevens die zijn verkregen uit externe bronnen, interne analyse of informatieverzoeken aan de klant (zie de NVB Standaard 'Actualisatie van klantgegevens' april 2023).

Triage voor de handling van alerts en events

De detectiemechanismen van banken genereren alerts en events. Triage van alerts en events betekent dat de diepgang, methode en prioriteit van de vervolgacties worden bepaald (dit kan ook 'hibernation' betekenen, waarbij een alert of event alleen relevant wordt in combinatie met ander klantgedrag dat een trigger oplevert en zal worden afgehandeld binnen de context van dat klantgedrag, maar niet op zichzelf). Banken moeten beoordelen of het alert of het event dat is gegenereerd, betrekking heeft op een daadwerkelijk ML/TF risico dat moet worden behandeld door een analist.

Banken bepalen zelf waar het inzetten van medewerkers de grootste toegevoegde waarde heeft. Mogelijke handlingmethoden zijn:

- Geautomatiseerde handling en sluiten van alerts en events die binnen de risicobereidheid vallen. De handling van het alert of het event is afgerond wanneer de bank tot de conclusie komt dat er geen risico is vastgesteld en dat handmatige handling niet nodig is.
- Handling m.b.v. een risicogedifferentieerde review. Als een risico is geïdentificeerd en vervolgstappen zijn nodig, is de volgende stap het opstarten van een risicogedifferentieerde review.
- Handling m.b.v. een uitgebreide review. De uitkomst van de triage kan zijn dat er direct een uitgebreide review van het alert of het event wordt opgestart.

Automatisering van het handlingproces

Alerts en events kunnen automatisch worden afgehandeld op basis van een vooraf vastgestelde reactie op een bepaald risico. De automatisering van het handlingproces vindt plaats binnen het Financial Crime Framework van de bank. Dit kan bijvoorbeeld gaan om het (rule-based) automatisch afhandelen en sluiten van alerts en events. Zo kan het besluit om niet te reageren op specifieke risicotriggers worden gezien als een risicogebaseerde beslissing. Dit betekent dat de geautomatiseerde afhandeling en sluiting van alerts of events kan worden gezien als een respons/reactie op het risico. Deze reactie valt binnen de risicobereidheid van de bank en de bank

leeft hiermee de wettelijke verplichtingen die de Wwft oplegt na. Banken moeten hierbij het volgende vastleggen:

- de overwegingen;
- een onderbouwing van de mogelijke impact van het sluiten van het alert of event op de geïdentificeerde risico's;
- de expliciete relatie met de integriteitsrisicobereidheid van de bank;
- de dossiers die binnen de reikwijdte van het besluit vallen.

Het automatisch sluiten van alerts en events zou moeten leiden tot een verfijning van de regels voor het genereren van alert en events en is geen structurele langetermijnoplossing.

Een bulksluiting van alerts en events betekent dat een groot aantal alerts of events tegelijkertijd wordt gesloten. Dit kan bijvoorbeeld plaatsvinden wanneer de bank besluit (na uitvoerig testen) om specifieke risicotriggers (stapsgewijs) af te schaffen. Dit kan een gevolg zijn van een verandering van de risicobereidheid van de bank, of wanneer alerts of events onterecht worden gegenereerd. In dit geval beoordeelt de bank het geïdentificeerde risico en legt met een onderbouwing vast waarom dit besluit past binnen de risicobereidheid van de bank. Zo'n bulksluiting van een alert of event kan worden gezien als een respons/reactie op het risico. In de risicogebaseerde aanpak geldt dat hoe groter het aantal bulksluitingen, hoe diepgaander de onderbouwing moet zijn om de impact van deze bulksluiting op de relevante risico's, de risicobereidheid en de wettelijke verplichtingen aan te tonen.

Voorwaarden voor het toepassen van een vooraf vastgestelde reactie van de bank op risico's.

- *Klantgegevens*
  De bank streeft ernaar de relevante klantgegevens die nodig zijn voor een risicobeoordeling beschikbaar en toegankelijk te hebben op een gestructureerde en makkelijk op te vragen manier zodat deze gegevens te gebruiken zijn voor een geautomatiseerde verwerking. Daarnaast implementeert de bank kwaliteitscontroles om de juistheid, volledigheid en integriteit van de relevante klantgegevens op een risicogebaseerde manier te kunnen monitoren en aan te kunnen tonen.
- *Documentatie over het testen van de effectiviteit*
  De bank beschikt over documentatie over de interne testen van de opzet, het bestaan en de operationele effectiviteit van de belangrijkste controles.

Handling d.m.v. een risicogedifferentieerde review

Handling door middel van een risicogedifferentieerde review is gericht op de ML/TF risico's die betrekking hebben op het alert of het event. De analist beoordeelt het alert of het event in de context van de specifieke klantsituatie. Bij de afronding van de handling wordt de conclusie vastgelegd, inclusief een onderbouwing van de toegepaste wijze waarop het alert of het event is afgehandeld en de impact van het alert of het event op de benodigde mitigerende maatregelen (inclusief een bevestiging of aanpassing van de risicoclassificatie van de klant). Als de analist van mening is dat de risicogedifferentieerde review niet voldoende is als gepaste reactie op het risico, start de analist een volledige review en geeft feedback op de geautomatiseerde risicodetectiemechanismen.

Voorwaarden voor de handling met behulp van een risicogedifferentieerde review.

- De bank moet onderbouwen onder welke voorwaarden de bank risicogedifferentieerde reviews wil toepassen (bijvoorbeeld het aantal risicotriggers dat van toepassing is op de klant, specifieke risico's die zijn vastgesteld tijdens de risicobeoordeling van de klant, specifieke klantgroepen).
- De bank voert periodiek ex-post controles uit en legt deze vast om te beoordelen of in de praktijk aan alle voorwaarden is voldaan. Analisten worden getraind om zich te richten op de relevante risico's bij een bepaald alert of event van een risicotrigger in de context van de klantsituatie, en weten wanneer zij de handling kunnen afronden (dus waar ze kunnen stoppen) [8]. Daarnaast worden analisten getraind om situaties te herkennen waarin een uitgebreide review nodig is [9].

8 De Wwft vereist van banken dat zij alle werknemers die betrokken zijn bij het AML/CFT-domein opleiden en trainen om te borgen dat zij over de vaardigheden en kennis beschikken om hun baan uit te voeren.

9 Dit is in aanvulling op de training om uitgebreide reviews uit te voeren.

- Banken hebben procedures en werkinstructies vastgelegd voor risicogedifferentieerde reviews van alerts en events. Het uitvoeren van processen op een risicogebaseerde manier houdt ook in dat er een balans wordt gevonden in de tijd en de diepgang van beoordelingen en reviews. Los van de controles en maatregelen die banken hanteren tijdens hun ODD, moeten werknemers hun AML/CFT-controles altijd uitvoeren met een risico management mindset.
- De effectiviteit van de toegepaste aanpak wordt geverifieerd door interne (bijvoorbeeld eerste-, tweede- en derdelijns) en externe partijen, zij tonen de effectiviteit aan met bewijs (bijvoorbeeld door kwaliteitsbewaking, steekproefcontroles, back-testing en portefeuille-analyses).
- Doelstelling van banken is dat relevante klantgegevens volledig en juist zijn. Daarnaast is er sprake van een risicogebaseerd proces om relevante gegevens te actualiseren. De kwaliteit van de gegevens ligt binnen de risicobereidheid van banken en er vinden regelmatig monitorings- en feedback loops plaats. Banken actualiseren de gegevens op basis van op regels en/of modellen gebaseerde alerts en events of op basis van gegevens die zijn verkregen uit externe bronnen, interne analyse of informatieverzoeken aan de klant. De effectiviteit van de toegepaste aanpak wordt geverifieerd door interne (bijvoorbeeld eerste-, tweede- en derdelijns) en externe partijen, zij tonen de effectiviteit aan met bewijs.

Handling via een uitgebreide review

Bij de handling via een uitgebreide review beoordeelt de analist de volledige klantsituatie handmatig en uitgebreid. Dit kan een EDR of PR zijn. Bij deze review worden relevante nieuwe risico's beoordeeld om te bepalen of de risicoclassificatie en de potentiële relevante mitigerende maatregelen nog steeds passend zijn bij het klantprofiel. Daarnaast kan deze review goede inzichten geven ten aanzien van de effectiviteit van de risicodetectiemechanismen; worden alle relevante risico's door het systeem gedetecteerd?

In de volgende situaties vindt er een uitgebreide review plaats.

- Als de geautomatiseerde risicodetectiemechanismen de risico's die zijn vastgesteld tijdens de risicoanalyse van de bank (waaronder SIRA) voor specifieke klanten of gebeurtenissen onvoldoende afdekken; of
- Als er nieuwe risico's worden gevonden tijdens de risicogedifferentieerde review, of risico's blijken te complex voor een risicogedifferentieerde review, waardoor een uitgebreide review wordt getriggerd; of
- Als banken van mening zijn dat de klant en/of de transactie te complex is voor een geautomatiseerde of risicogedifferentieerde review; of
- Wanneer wet- en regelgeving een uitgebreide review voorschrijft.

1.4 Risicorelevantie

Het ODD framework dat in deze NVB Standaard wordt beschreven, draagt bij aan het operationaliseren van een risicogebaseerde aanpak én het naleven van de Wwft-verplichtingen. Hierbij krijgen klanten, hun transacties en gedrag waarvan uit de risicodetectiemechanismen van de bank blijkt dat er sprake is van een hoger risico, een hogere prioriteit voor het beperken van deze risico's.

Het operationaliseren van het ODD framework op basis van triggers verhoogt de relevantie van het handlingproces, doordat middelen proportioneel worden toegewezen aan hogere risico's en prioriteiten die zijn geïdentificeerd met de risicodetectiemechanismen. Dit betekent dat banken stappen moeten nemen om passende beheersmaatregelen te bepalen (zoals risicotriggers, drempelwaarden, enz.) om de Wwft na te leven en voor het beheersen van hun exposure aan ML/TF risico's en hun risicobereidheid.

Hierbij merken we op dat bij iedere risicogebaseerde aanpak ook risico's over het hoofd zullen worden gezien. Geen enkel framework is foutloos, en de risicogebaseerde aanpak is geen 'zero failure'-aanpak, net zoals handmatige handling en PRs dat niet zijn. Banken moeten beschikken over feedback loops, procesmonitoring, (interne) testen van beheersmaatregelen en audits om te zorgen voor continue verbeteringen en om het framework te versterken indien nodig. Los van de beheersmaatregelen die banken hanteren tijdens hun

ODD, moeten werknemers hun AML/CFT-beheersmaatregelen altijd uitvoeren met een risicomanagement mindset.

1.5 Klantgroepen

Banken kunnen de risicogebaseerde aanpak toepassen op alle klanten en op alle klantgroepen. Afhankelijk van de risicobereidheid van de bank kan de bank wel differentiëren wat betreft de handlingmethode voor verschillende klantgroepen, bijvoorbeeld op basis van de omvang, complexiteit, specifieke risico's, de klantenportefeuille en de producten die worden aangeboden.

1.6 Criteria voor het aantonen van een effectieve implementatie

Hoewel de opzet en de implementatie van een ODD framework per bank kan verschillen, moeten banken er altijd voor zorgen dat zij hun framework blijven verbeteren, om zo de effectiviteit te verhogen en om in te spelen op de risico's die zij onderweg tegenkomen. Deze continue verbetercyclus is belangrijk om te zorgen voor een adequate en tijdige reactie op nieuwe risico's. Bovendien is het continu monitoren van de bestaande processen en het toetsen van de resultaten belangrijk voor een effectieve implementatie. De bank moet de effectieve implementatie van het (geautomatiseerde) ODD framework op basis van triggers en van de handlingmethoden kunnen aantonen.

Het aantonen van een effectief (geautomatiseerd) ODD framework

De bank toont de effectieve implementatie van de voorwaarden aan waaraan de bank moet voldoen om een ODD framework op basis van triggers te operationaliseren, door te onderbouwen op welke manier de bank een proportionele risicogebaseerde set van beheersmaatregelen heeft opgesteld en onderhoudt om de ML/TF risico's te beperken. Ook de relatie met andere bestaande processen of beheersmaatregelen moet worden vastgelegd (zoals de actualisatie van gegevens, het bepalen van drempelwaarden, de reactie op risico's, enz.). Dit is een bankspecifieke aangelegenheid, aangezien de opzet en de implementatie van het ODD framework worden gebaseerd en afgestemd op de risicobereidheid van de bank en het bijbehorende AML/CFT-beleid. Ook zal de volwassenheid van dit framework in de loop van de tijd verder ontwikkelen, dankzij de inzichten die zijn opgedaan tijdens het implementeren van een geautomatiseerd ODD framework op basis van triggers.

Banken moeten binnen hun eigen ODD processen over de volgende documentatie beschikken om een effectieve implementatie van de risicogebaseerde aanpak te kunnen aantonen in de verschillende ODD processen.

I Risico- en controledocumentatie

- Vastlegging van de belangrijkste risico's en beheersmaatregelen om helder aan te tonen wat de relatie is tussen de ML/TF risico's van de bank (zoals bijvoorbeeld blijkt uit de risicoanalyses van de bank, inclusief SIRA), de risicodetectiemechanismen van de bank en de processen van de bank om de risico's te beperken.
- Risico- en controledocumentatie waarmee de bank de kwaliteit aantoont van de risicodetectiemechanismen ten opzichte van de risico's die door de bank zijn vastgesteld tijdens de risicoanalyses en in de portfolio management resultaten.
- Managementinformatie en verslagen waaruit de effectieve implementatie van de risicodetectiemechanismen van de bank blijkt.
- De bank beschikt over processen om aan te tonen dat de risicodetectiemechanismen continu worden verbeterd (door feedback loops) die:
  - zorgen voor het beter vaststellen van bekende risico's, bijvoorbeeld door opvolging te geven aan de resultaten van het testen van de beheersmaatregelen;
  - zorgen voor het beter identificeren van nieuwe risico's, bijvoorbeeld door middel van back-testing of externe situaties waardoor de bank is blootgesteld aan nieuwe risico's.
- De instellingen van de risicodetectiemechanismen, bijvoorbeeld het vaststellen van de drempelwaarden op basis van data-analyse (inclusief vastlegging van de onderbouwing). Deze instellingen moeten voldoende onderbouwd zijn en een overzicht geven van de huidige instellingen, de betrokken risico's met een duidelijke link met de risicobereidheid van de bank.

II Documentatie van het testen van de effectiviteit

De effectiviteit is sterk gerelateerd aan de mate waarin banken beschikken over interne controle-testen om de opzet en de operationele effectiviteit van de belangrijkste beheersmaatregelen te toetsen. Banken moeten hierbij besluiten hoe en in welke mate en frequentie zij de effectiviteit van de beheersmaatregelen gaan testen. De effectiviteit wordt beoordeeld op basis van het beoogde doel of de gewenste resultaten van een specifieke mitigerende maatregel.

- Documentatie waaruit een testplan blijkt waarin het doel, de reikwijdte en de methodologieën zijn opgenomen voor het testen van de effectiviteit. Dit plan moet ook testscripts bevatten die gedetailleerde instructies en stappen bevatten voor de manier waarop het systeem zal worden getest. Hierin worden de acties gespecificeerd die de bank zal ondernemen, de input die nodig is, en de verwachte output of resultaten.
- Documentatie waaruit de (operationele) effectiviteit blijkt van de output van de risico-detectiemechanismen met betrekking tot de (belangrijkste) ML/TF risico's die zijn vastgesteld (bijvoorbeeld door back-testing, op basis van de relevante managementinformatie). Hieruit moet blijken hoe en in welke mate de risicodetectiemechanismen van de bank in staat zijn om de risico's te detecteren.
- Daarnaast moeten banken opvolging geven aan deze resultaten, bijvoorbeeld door de acties die worden ondernomen te verfijnen en vast te leggen. Als een beheersmaatregel aanzienlijk meer tijd en/of middelen vereist voor een minimale beperking van het risico, kunnen banken overwegen de beheersmaatregel aan te passen of te schrappen en de vrijgekomen middelen toe te wijzen aan beheersmaatregelen met effectievere resultaten. Door deze handelswijze regelmatig toe te passen, kunnen banken ineffectieve en inefficiënte beheersmaatregelen afschaffen. De opportuniteitskosten van het niet aanpassen of niet afschaffen van een ineffectieve of inefficiënte beheersmaatregel zouden onderdeel moeten zijn van de totale beoordeling van de eigen risicogebaseerde beheersmaatregelen die de bank uitvoert.

III Documentatie van de validatie van processen

- De resultaten van de eerste-, tweede- en derdelijns (of externe) testen van (externe) quality assurance.
- Documentatie van de vervolgstappen naar aanleiding van deze resultaten, die bijvoorbeeld laten zien wat de aanpassingen en/of verbeteringen zijn die worden doorgevoerd in de ODD processen.

IV Documentatie van de relevante besluitvorming

- De gedocumenteerde motivering en onderbouwing voor besluiten ten aanzien van bijvoorbeeld de prioritering van verbeteringen en het bepalen van drempelwaarden (op het niveau van regels, modellen, transacties, events), bulksluitingen en automatische sluitingen, ook in relatie tot de risicobereidheid van de bank.
- De gedocumenteerde en heldere governance van de bank op basis waarvan de bank besluiten stuurt en neemt die onder andere impact hebben op de uitvoering van de processen van het ODD framework.

V Documentatie van klantgegevens

- De vereiste documentatie met betrekking tot financiële criminaliteit gegevens, inclusief de governance die van toepassing is op de gegevens.
- Een omschrijving van de datakwaliteits-processen en -procedures (bijvoorbeeld ten aanzien van de actualisatie van de gegevens).
- Voldoende onderbouwing van de relevante datakwaliteit (bijvoorbeeld dataintegriteit).

Het aantonen van een effectieve implementatie van de handlingmethoden voor alerts en events

- De bank beschikt over heldere governance op basis waarvan de bank besluiten stuurt en neemt die onder andere impact hebben op welke handlingmethoden worden toegepast in specifieke situaties.
- De bank onderbouwt welke handlingmethode wordt gebruikt in een specifieke situatie (inclusief de criteria, besluiten en analyses, bijvoorbeeld met betrekking tot het type klant, de risico's en de effectiviteit van de risico-detectiemechanismen). De bank houdt hierbij een audittrail bij van de in de loop van de tijd toegepaste handlingmethoden.
- De bank legt in het klantdossier de handling van alle alerts of events die zijn gegenereerd voor

een specifieke klant vast (bijvoorbeeld welk proces is toegepast en tot welke conclusie dit heeft geleid, inclusief de impact op de risicoclassificatie) op een dusdanige manier dat deze terug te vinden is.
- De bank voert periodieke effectiviteitstesten uit van de handlingmethoden en onderneemt actie als de resultaten daarom vragen.
- De bank beschikt over processen om de kwaliteit van de handlingmethoden voor alerts en events te monitoren en te verbeteren.
- De bank beschikt over voldoende managementinformatie om de effectieve implementatie door de bank van geautomatiseerde of handmatige handling van alerts of events aan te tonen.

In de praktijk zal een risicogebaseerde implementatie van handlingmethoden van een bank gericht zijn op de grootste risico's, en zullen op deze handlingmethoden de meest intensieve kwaliteitsprocessen van toepassing zijn.

2 Impact

Deze NVB Standaard biedt uitgangspunten aan de Nederlandse bankensector voor de transitie van het standaard uitvoeren van PRs naar een situatie waarin de bank kan vertrouwen op een (geautomatiseerd) ODD framework op basis van triggers en het uitvoeren van EDRs.

De operarionalisatie van continue screening en monitoring is belangrijk om een risicogebaseerde aanpak mogelijk te maken en tijdrovende PRs te voorkomen. Het ODD framework draagt bij aan de risicogebaseerde aanpak door een methode te bieden voor het beoordelen van alerts en events op basis van triggers, waardoor banken hun middelen effectief en op een risicorelevante manier kunnen inzetten. Met deze risicogebaseerde aanpak van het ODD kunnen banken hun AML/CFT-beheersmaatregelen effectiever uitvoeren, doordat zij zich beter kunnen richten op grotere risico's, en mitigerende maatregelen kunnen nemen waar deze het meeste effect hebben. Dit is essentieel om overcompliance te voorkomen, bijvoorbeeld wanneer een PR ten opzichte van potentieel effectievere mitigerende maatregelen een beperkte toegevoegde waarde heeft om de ML/TF risico's te beperken. Als het ODD niet op een risicorelevante manier wordt toegepast, kan dit bovendien leiden tot onnodige verzoeken en disproportionele maatregelen voor klanten.

De manier waarop banken ODD uitvoeren, heeft impact op de interne monitorings- en auditprocessen van de bank. Daarnaast heeft dit impact op de gesprekken over de kwaliteit van de interne controleprocessen van de bank binnen de eerste en tweede lijn en met de interne (raad van commissarissen) en externe toezichthouders. De maatschappij als geheel profiteert dankzij effectievere en efficiëntere AML/CFT-beheersmaatregelen van een veilig en betrouwbaar financieel systeem, waarbij tegelijkertijd een onnodige belasting van goedwillende burgers wordt beperkt.

3 Use cases

Het ODD framework: geen risico-trigger

Voorbeeld

Een klant laat een regelmatig patroon aan inkomende en uitgaande transacties zien, dat in lijn is met zijn of haar verwacht transactieprofiel (hierna: ETP). De klant neem geen complexe producten af. De klant woont al meer dan 10 jaar op hetzelfde adres in Nederland.

NVB Standaard

- De bank beperkt het risico van deze klant door klantmonitoring, transactiemonitoring en -processen en beheersmaatregelen uit te voeren.
- Er wordt geen alert voor deze klant gegenereerd, aangezien de statische gegevens en gedrag van deze klant geen indicatie geven voor een verandering van de risicoclassificatie van de klant.
- Zolang de klantsituatie niet verandert, dus de transacties binnen het ETP blijven, en er geen veranderingen plaatsvinden in het gedrag of de statische gegevens van de klant die mogelijk impact kunnen hebben op de risicoclassificatie van de klant, is het niet nodig een review van deze klant uit te voeren.
- Bovenstaande is gebaseerd op een situatie waarin het ETP, de klantmonitoring en de transactiemonitoring allemaal effectief zijn, de SIRA-risico's worden afgedekt en er geen grote hiaten worden geconstateerd.

Het ODD framework: een risico-trigger

Voorbeeld

Een klant laat een regelmatig patroon aan inkomende en uitgaande transacties zien en handelt in lijn met zijn of haar ETP. De klant neemt geen complexe producten af. De klant woont al meer dan 10 jaar op hetzelfde adres in Nederland. Uit de transactiegegevens blijkt dat het vestigingsland mogelijk is gewijzigd, doordat er meerdere opeenvolgende maanden sprake is van inkomende en uitgaande transacties van en naar Spanje. Er wordt een event 'potentiële verandering van vestigingsland' getriggerd. Uit interne analyse blijkt dat de klantgegevens mogelijk moeten worden geactualiseerd.

NVB Standaard

Uit de transactiegegevens blijkt dat het vestigingsland mogelijk is gewijzigd. Omdat de klantsituatie kan zijn veranderd (zie NVB Standaard 'Actualisatie van klantgegevens') is er reden om een beoordeling van een alert of event uit te voeren. Dit kan geautomatiseerd plaatsvinden wanneer de bijbehorende risico's binnen de risicobereidheid van de bank vallen.

Handlingmethode: risico-gedifferentieerde EDR

Voorbeeld

Klant

De klant is een rechtspersoon en is gevestigd in Nederland. De moedermaatschappij is geregistreerd in een jurisdictie met een hoger risico, waardoor verscherpte monitoring is vereist omdat er volgens de FATF sprake is van strategische tekortkomingen in de AML-wetgeving van het land. De kernactiviteit van de klant is het importeren van traditionele voedingsmiddelen vanuit de jurisdictie met een hoger risico om in Nederland te verkopen. Dit wordt gezien als een activiteit waarin veel contant geld omgaat, en daardoor als een activiteit met een hoger risico.

Bank

De geautomatiseerde risicodetectiemechanismen van de bank beheersen de relevante ML/TF risico's van de bank (op basis van SIRA) voldoende.

Risicotrigger

Uit de transactiegegevens van de klant blijkt dat de zakelijke activiteiten naast Nederland ook plaatsvinden in België (een neutraal land wat betreft ML/TF risico's). Verder worden er door de risicodetectiemechanismen geen andere veranderingen van de klantsituatie vastgesteld.

NVB Standaard

Omdat de risico's die volgen uit de locatie en het contante geld al eerder zijn beoordeeld, moet de analist zich richten op de beoordeling van de risico's met betrekking tot de zakelijke activiteiten in België, waarbij hij of zij ook de andere risico-triggers (import uit een jurisdictie met een hoog risico, een sector waarin veel contant geld omgaat) in overweging moet nemen. De analist komt tot de conclusie dat de verandering in de klantsituatie past bij het profiel van de klant en stelt geen risico's vast. Het is niet nodig om over te gaan op een uitgebreide handling [10].

Opmerkingen

1 In dit voorbeeld kan de verandering wel leiden tot de actualisatie van bepaalde klantgegevens om te voldoen aan de verslagleggingseisen die van toepassing zijn op de bank (zoals CRS).
2 Deze beoordeling kan ook automatisch worden uitgevoerd door middel van een vooraf vastgestelde reactie van de bank op dit risico.

10 Als de analist tot de conclusie komt dat de verandering in de klantsituatie niet past bij het klantprofiel of als er nieuwe risico's zijn geïdentificeerd kan de analist een uitgebreide review opstarten.

Handlingmethode: een uitgebreide PR

Voorbeeld

Klant

De klant is een rechtspersoon en is gevestigd in Nederland. Er is sprake van een complexe eigendomsstructuur (meerdere lagen tussen de klant en de UBOs) en uit de adverse media screening zijn in het verleden negatieve media-berichten over de moedermaatschappij van de klant naar voren gekomen. De klant heeft recent zijn activiteiten uitgebreid van een kleding-detailhandel waarbij alleen betalingen met een betaalpas werden geaccepteerd, naar horeca-activiteiten. Dit laatste wordt gezien als een sector waarin veel contant geld in omloop is en daarmee als een activiteit met een hoger risico.

Bank

De risicodetectiemechanismen van de bank beheersen de relevante ML/TF risico's van de bank (op basis van SIRA) voldoende.

Risicotrigger

Een detectiemechanisme op basis van regels constateert een verandering in de bedrijfs-activiteiten. Er wordt een alert gegenereerd.

NVB Standaard

De analist voert handmatig een uitgebreide risico-review uit vanwege de complexe risicosituatie (complexe eigendomsstructuur) en de verandering in de bedrijfsactiviteiten die is geconstateerd.

Context

Het regelgevend kader

De regelgevende context die van toepassing is op dit onderwerp is te vinden in de relevante delen van de toepasselijke wetten, regelgeving en richtlijnen van verschillende autoriteiten. Wetgeving waarin relevante wettelijke bepalingen te vinden zijn, zijn de Wwft, het Besluit prudentiële regels Wet financieel toezicht (hierna: Bpr Wft) en de Regeling toezicht Sanctiewet 1977 (hierna: RtSw).

Banken zijn niet verplicht PRs uit te voeren van individuele klanten. De Wwft schrijft niet voor wanneer of hoe vaak klantonderzoek moet worden gedaan. De Wwft specificeert wel dat de intensiteit van het klantonderzoek moet worden afgestemd op de risicogevoeligheid van de klant. Ook stelt de Wwft dat de klant van de bank en de zakelijke relatie continu moeten worden gemonitord.

Er zijn geen specifieke wettelijke eisen ten aanzien van de handlingmethoden voor alerts en events. Banken moeten wel verplicht een MOT indienen bij de Financial Intelligence Unit (hierna: FIU) zodra de ongebruikelijke aard van de transactie of de voorgenomen transactie duidelijk wordt.

- **Artikel 2a lid 1 Wwft**
  "Ter voorkoming van witwassen en financieren van terrorisme verricht een instelling cliëntenonderzoek en meldt zij verrichte of voorgenomen ongebruikelijke transacties overeenkomstig de bij of krachtens de hoofdstukken 2 en 3 gestelde regels. Daarbij besteedt een instelling bijzondere aandacht aan ongebruikelijke transactiepatronen en aan transacties die naar hun aard een hoger risico op witwassen of financieren van terrorisme met zich brengen."
- **Artikel 3 lid 2 sub d Wwft**
  "Het cliëntenonderzoek stelt de instelling in staat om (...):
  een voortdurende controle op de zakelijke relatie en de tijdens de duur van deze relatie verrichte transacties uit te oefenen, teneinde te verzekeren dat deze overeenkomen met de kennis die de instelling 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."
- **Artikel 3 lid 8 Wwft**
  "Een instelling stemt het cliëntenonderzoek aantoonbaar af op de risicogevoeligheid voor witwassen of financiering van terrorisme van het type cliënt, zakelijke relatie, product of transactie."
- **Artikel 3 lid 9 Wwft**
  "Een instelling houdt bij het bepalen van de risicogevoeligheid, bedoeld in het achtste lid, tenminste rekening met de in bijlage I bij de vierde anti-witwasrichtlijn genoemde risicovariabelen."
- **Artikel 3 lid 11 Wwft**
  "Een instelling neemt redelijke maatregelen om ervoor te zorgen dat de gegevens die ingevolge het tweede tot en met vierde lid zijn verzameld over daarin bedoelde personen, actueel gehouden worden."
- **Artikel 16 lid 1 Wwft**
  "Een instelling meldt een verrichte of voorgenomen ongebruikelijke transactie onverwijld nadat het ongebruikelijke karakter van de transactie bekend is geworden, aan de Financiële inlichtingen eenheid."
- **Artikel 14 lid 4 Bpr Wft**
  "De financiële onderneming, bedoeld in het tweede lid, onderscheidenlijk het bijkantoor, beschikt over procedures en maatregelen met betrekking tot de analyse van gegevens van cliënten, mede in relatie tot de door de cliënt afgenomen producten of diensten, en terzake van de detectie van afwijkende transactiepatronen. Aan de hand van voornoemde procedures en maatregelen bepaalt de financiële onderneming tevens de risico's van bepaalde cliënten, producten of diensten voor de integere uitoefening van haar bedrijf."

- **Artikel 2 RtSw**
  "1. De instelling waarborgt dat zij op het gebied van de administratieve organisatie en interne controle maatregelen heeft getroffen ter naleving van de Sanctieregelgeving.
  2. De maatregelen als bedoeld in het eerste lid voorzien tenminste in een adequate controle van de administratie van de instelling op het overeenkomen van de identiteit van een relatie met een (rechts)persoon of entiteit, als bedoeld in de Sanctieregelgeving, met het oog op het bevriezen van de financiële middelen van die relatie of het voorkomen van het ter beschikking stellen van financiële middelen of diensten aan die relatie."
- **Artikel 3 RtSw**
  "Indien de instelling constateert dat de identiteit van een relatie overeenkomt met een (rechts) persoon of entiteit, als bedoeld in de Sanctie-regelgeving, meldt de instelling dit onverwijld aan de toezichthouder. Bij de melding legt de instelling tevens de gegevens over van de identiteit van die relatie aan de toezichthouder."

Afstemming tussen de 'DNB Good Practices' en de 'NVB Standaard'

DNB heeft als doel organisaties waarop de bank toezicht houdt inzicht te geven in haar beleids-praktijk door bijvoorbeeld een interpretatie van wettelijke vereisten te geven (Q&A), evenals voorbeelden van manieren waarop aan de wettelijke vereisten kan worden voldaan (Good Practices). Het is hierbij belangrijk op te merken dat noch de Q&A's, noch de Good Practices van DNB juridisch bindend zijn.

De NVB Standaard beschrijft de toepassing en uitvoering van het ODD framework in meer detail, evenals de manier waarop dit bijdraagt aan een meer risicogebaseerde aanpak.

Nederlandse Vereniging van Banken
Gustav Mahlerplein 29-35
1082 MS Amsterdam
www.nvb.nl