Financial Action Task Force: Mogelijkheden en uitdagingen voor nieuwe AML-/CFT-technologie

Michelle Fisser (VCO), Eddy van Rooijen (VCO), Jean Jacques Bisterveld (NBA)

Introductie

Met de toepassing van technologie in de strijd tegen witwassen (AML) en terrorismefinanciering (CTF) is het lange tijd ondenkbare ineens werkelijkheid geworden. Het kan sneller, goedkoper en effectiever. Inmiddels richten alle ogen zich op nieuwe vormen van technologie en gerelateerde businessmodellen. Om wat voor nieuwe technologieën en businessmodellen gaat het precies? Wat zijn de randvoorwaarden? En hoe zou dit moeten werken in de praktijk?

Dit is een selectie van vragen die leven bij onder andere de compliance professionals en (IT-)auditors die zich richten op de strijd tegen witwassen. Het 'digitale goud' is qua technologie aanwezig, maar de exacte toepassing hiervan is voor velen nog onbekend terrein. Wij willen in dit artikel samen met de lezer dit terrein verkennen en baseren ons daarbij op de grondige ontginning van de Financial Action Task Force (hierna FATF[1]. De FATF heeft in 2021 een specifieke studie uitgevoerd om antwoord te kunnen geven op bovenstaande vragen. De verkregen inzichten zijn gepubliceerd om financiële instellingen te helpen keuzes te maken over deze nieuwe technologieën in de strijd tegen witwassen. Hiermee is een nuttige handreiking ontstaan om te voldoen aan de FATF-standaarden, zonder dat nadelige effecten ontstaan, zoals uitsluiting van financiële diensten.

Achtergrond in de strijd tegen witwassen

Criminelen hebben er veel geld voor over om onzichtbaar te blijven. Klanten voelen zich soms de dupe van digitalisering, want hoewel voor de digitaal vaardige consument veel zaken gemakkelijker gaan, worden zij ook weer gemakkelijker bestolen. Van hun identiteit, privacy, hun geld of van alle drie deze zaken. Ook ervaren klanten soms de negatieve (bij)effecten in de strijd tegen witwassen door banken. In een enkele situatie voelt een klant zich zelfs als crimineel behandeld door een financiële instelling die beweert slechts de wetgeving strikt na te leven[2]. De hard tegen criminelen optredende wetgever lijkt daarmee soms wetgeving te maken die op gespannen voet staat met andere basisbeginselen. Een zeer recent voorbeeld waarover een dergelijke discussie loopt is het wetsvoorstel 'Plan van Aanpak witwassen' dat in oktober naar de kamer is gestuurd ter accordering[3].

In Nederland is de toepassing van AML/CTF en sanctiewetgeving een combinatie van *risk based* en *rule based*. Dat biedt dus ruimte voor interpretatie van deze wetgeving door de financiële instellingen. Tegelijkertijd zijn er regelmatig (internationale) berichten over financiële instellingen die een boete krijgen van een of meer toezichthouders. De invulling van de regelgeving en/of de uitvoering door de financiële instelling blijkt niet voldoende te zijn.

De FATF wil voorop blijven lopen in de race tegen witwassen met slimme guidance, met evenwicht tussen uitdagingen en risicobeheersing. Zij richt zich daarbij zowel op *regtech* als op *suptech*: *Regtech* is de term die wordt gebruikt voor technologische ontwikkelingen bij het voldoen aan wet- en regelgeving. *Suptech* gaat over technologieën en modellen voor toezichthouders. In de complexe materie van witwassen is innovatie een speerpunt geworden voor de effectiviteit en efficiency van instellingen.

Wij zijn van mening dat deze innovatie vraagt om een veilige leeromgeving, de mogelijkheid om fouten te maken en daarna uiteraard snel weer te herstellen. Als deze niet geboden wordt zullen instellingen weinig innovatie tonen en leidt dit tot het strikt kijken naar de uitleg en mogelijkheden die een toezichthouder voorschrijft in richtlijnen en andere uitingen. Samenwerking, kennisdeling en het doorgronden van nieuwe technologieën helpen op verantwoorde wijze tot invoering van die nieuwe technologieën en businessmodellen voor financiële instellingen te komen. Waarbij in voldoende mate rekening wordt gehouden met anti-witwas wetgeving.

We bespreken enkele vormen van technologie die FATF beschrijft in haar paper uit juli 2021. We schetsen scenario's waar deze technologieën praktisch wordt toegepast. We beginnen met de door FATF genoemde randvoorwaarden uit haar studie als het gaat om de inzet van de deels nieuwe technologieën.

De randvoorwaarden volgens FATF: wat is nodig voor effectieve implementatie?

De FATF wijst op twee hindernissen bij technologische middelen die de effectiviteit van de strijd tegen witwassen beogen te vergroten:

1. Het beter begrijpen van de echte AML/CTF-bedreigingen en risico's om tot een echte *risk based approach* te komen;
2. Het voorkomen van (onterechte) uitsluiting van groepen tot het financiële stelsel, ook wel 'financiële inclusie genoemd'.

Ad 1

Met betrekking tot de *risk based approach* signaleert FATF dat veel financiële (Wwft-)instellingen een risicoanalyse als grondslag hebben ingevoerd. En daarbij automatisering hebben toegepast. De basis voor een gedegen *risk based approach* is daarmee nog niet op orde gebleken. Veelal

[1] FATF: De Financial Action Task Force (FATF), opgericht in 1989, is een intergouvernementele task force die zich bezighoudt met de bestrijding van witwassen en de financiering van terrorisme.

[2] https://www.volkskrant.nl/nieuws-achtergrond/banken-behandelen-clienten-als-halve-criminelen~bb40f5b4/

[3] https://www.rijksoverheid.nl/documenten/kamerstukken/2022/10/21/wetsvoorstel-plan-van-aanpak-witwassen

richten de risicoanalyse en het risicomanagement voor AML zich op een statische analyse met een vooraf bepaalde set aan risicofactoren, zoals 'autohandelaar' of 'actief in vastgoed'. Deze compliance gedreven *tick-the-box*-applicaties lijken ingericht om te laten zien dat hard gewerkt wordt en veel geld wordt uitgegeven. Bestaande systemen worden daarna voorzien van nieuwe algoritmen om de gegevens hier enigszins bij aan te laten sluiten, maar de dynamiek en het inzicht en het echte risico ontbreekt.

In de praktijk vertaalt dit zich ook naar het werk van IT-auditors. Bijvoorbeeld het toetsen van ineffectieve implementaties tegen reeds achterhaalde beleidskaders en inzichten. En veel bedrijven achten de auditor niet de persoon die moet kijken naar de *state-of-the-art* uitleg die de toezichthouder aan de regels geeft, waardoor ook de auditor de kans loopt niet voorbij het eigen bedrijfsbeleid te kijken als de vigerende 'norm'. Daar staat tegenover dat de compliance professional soms tekortschiet op (inzicht in) het gebied van de technologische mogelijkheden. Financiële instellingen zien zich vervolgens gedwongen handmatig veel herstelacties uit te voeren met grote aantallen analisten en vaak onder hoge tijdsdruk. Dat blijkt bovendien kostbaar en tijdsintensief, bovendien blijken het langjarige trajecten.

Ad 2

Financiële instellingen richten zich in compliance gedreven programma's regelmatig op het uitsluiten van risicovolle groepen. En door de verhoogde risico classificaties wordt er soms veel informatie gevraagd aan klanten. Deze ontwikkeling staat soms op gespannen voet met de privacyregels omdat de anti-witwas wetgeving in veel gevallen niet exact voorschrijft wat benodigd is. Regelmatig kiezen instellingen er dan ook voor om de naar hun indruk 'hoog risico' en kwetsbare groepen, met veelal de minste middelen en mogelijkheden, uit te sluiten voor dienstverlening[4]. Bijvoorbeeld klanten uit specifieke landen, kleine garagebedrijven of indirect aan de bouwsector te relateren beroepen: het is voor de instellingen te kostbaar en te tijdsintensief om zich met deze klantgroepen op rendabele manier bezig te (kunnen) houden.

Om van technologische kansen gebruik te maken zullen instellingen waarborgen moeten treffen voor deze twee genoemde randvoorwaarden. Anders heeft de inzet van méér vormen van technologie uiteindelijk niet het gewenste effect en worden bepaalde groepen nog steeds ten onrechte uitgesloten

Technologische kansen voor een effectievere AML-management

Om een beeld te krijgen bij de diverse vormen van technologie die in steeds grotere mate worden toegepast hebben we deze onderstaand uiteengezet

- Toepassing van artificial Intelligence;
- Natural Language Processing (NLP) en 'soft computing'-technieken;
- Distributed Ledger Technologie (DLT);
- Digitale oplossingen voor due diligence voor klanten;
- Application Programming Interfaces (API's).

Artificial Intelligence (AI)

AI, of kunstmatige intelligentie, heeft betrekking op systemen of machines die onze eigen intelligentie kunnen nabootsen om taken uit te voeren[5]. Tegelijkertijd kan deze intelligentie zichzelf tijdens dat proces verbeteren op basis van de vergaarde informatie. AI kan verschillende vormen aannemen en is een overkoepelende term waar meerdere begrippen onder vallen. Denk hierbij bijvoorbeeld aan *machine learning* (ML) en *deep learning*.

We raakten het onderwerp AI al in ons artikel uit 2021 met een praktijkvoorbeeld uit Japan die in voorgaande Tech Paper van FATF is benoemd. AI en ML vormen voor FATF beiden hoopvolle technologieën voor de toekomst om in de enorme hoeveelheid data rond financiële transacties of een effectieve wijze verdachte transacties te gaan signaleren.

Natural Language Processing (NLP) en 'soft computing'-technieken'

FATF ziet in NLP een vorm van AI die computers in staat stelt om taal te interpreteren en verwerken. Een vorm van 'soft computing'-technieken is bijvoorbeeld *Fuzzy logic*. *Fuzzy logic* is een stroming binnen de logica waarin met waarschijnlijkheden wordt gerekend in plaats van alleen met de mogelijkheden 'waar' en 'onwaar'. Je ziet in de praktijk dat die techniek bij sanctie-screening wordt toegepast bijvoorbeeld om namen en naamcombinaties die op elkaar lijken te relateren en zo toch personen te signaleren die mogelijk de gesanctioneerde zijn. Denk bijvoorbeeld aan het relateren van een Russische naamformulering relateren aan Engelse verwoording.

Daarnaast ziet FATF NLP-techniek en *fuzzy logic matching tooling* als mogelijkheden om binnen bovenstaand domein de enorme berg aan *false positives* en *false negatives* te reduceren. En ook de uitdagingen in het domein datakwaliteit te overwinnen doordat men elementen van informatie beter aan elkaar kan koppelen. Bijvoorbeeld het automatisch koppelen van PEP-lijsten met zoekmachineresultaten, het signaleren van namen op sanctielijsten et cetera.

Distributed Ledger Technologie (DLT)

DLT is een vorm van een gedistribueerde database of grootboek of databases die op verschillende plekken opgeslagen en gesynchroniseerd worden zodat wijzigen van de informatie moeilijker wordt. In de praktijk is het bekendste voorbeeld van de toepassing van deze technologie die van de *crypto currencies*. FATF heeft hoop dat de toepassing van DLT de volgbaarheid van transacties op internationale of mondiale schaal kan verbeteren. Maar FATF ziet veel beren op de weg voor de doorbraak van deze technologie in de (nabije) toekomst.

Digitale oplossingen voor due diligence voor klanten

Digital solutions for customer due diligence is een verzamelterm voor technische oplossingen die klanten op een laagdrempelige wijze toegang geven tot de verstrekte diensten waarbij gelijktijdig de noodzakelijke CDD-activiteiten worden uitgevoerd. Denk hierbij aan toepassingen rond een digitale ID, zoals eIDAS, en diverse onboarding tools die snel en effectief checken op fraudesignalen (EVA, VIS), kredietwaardigheid (BKR) en logische variabelen als geolocatie van de klant.

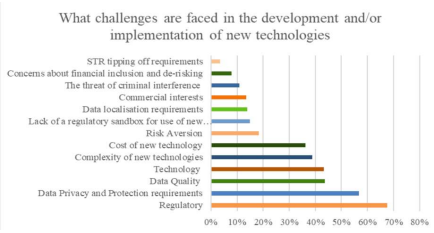
De klant identificatie en verificatie is een essentiële hoeksteen in een effectieve AML-strategie, maar vormt vaak ook een flinke hindernis voor klanten. De huidige systemen en oplossingen zijn voor klanten veelal nog gebruiksonvriendelijk. De FATF signaleert dat Digitale ID's voor de financiële echte drivers zijn om zowel de dienstverlening als de AML-inspanningen effectiever te maken.

Application Programming Interfaces (API's)

Een API is een software-interface welke wordt gebruikt om op een geformaliseerde manier gegevens uit te wisselen tussen apps, programma's, systemen en/of platformen. Een voorbeeld in Nederland van een 'externe' API is de VIS API van Stichting BKR. FATF stelt dat via moderne API's het mogelijk moet worden om data buiten bestaande en nieuwe bronapplicaties, via koppeling en samenvoeging, te verrijken en (real time) te delen tussen stakeholders. Ook ziet FATF hier mogelijkheden om de toezichthouders meer real time de datastromen van de onder toezicht staande organisaties te laten monitoren om de kwaliteit van de AML/CTF-inspanningen te bewaken. Dat laatste is natuurlijk ook weer een spanningsveld met de belangen van financiële instellingen.

De uitdagingen van het adopteren van bovenstaande technologieën

De FATF heeft, om inzicht te krijgen in de drempels voor de toepasbaarheid van bovengenoemde technologieën, marktpartijen bevraagd over wat zij ervaren als de grootste uitdagingen om tot adoptie en implementatie over te gaan. In onderstaande histogram staan de uitkomsten van dit onderzoek weergegeven.



Bron: FATF, 2021.

Met stip bovenaan staan volgens de marktpartijen andere wet- en regelgeving, zoals privacywetgeving en de huidige richtlijnen, kaders en instructies van de toezichthouders. Dat de inhoud van de FATF uitgave ook in 2022 nog actueel is blijkt wel uit de recent uitgegeven studie 'Van herstel naar balans' van DNB[6]. DNB heeft met deze uitgave de grootste uitdaging in bovengenoemd schema willen adresseren met een schets voor de toekomstvisie die zij als leidende toezichthouder heeft: het wettelijk kader. Een aantal van de technologieën die FATF in 2021 heeft beschreven, worden specifiek door DNB geadresseerd. Maar ook de AVG[7] blijft dus een spanningsveld en de Autoriteit Persoonsgegevens en een belangenorganisatie als Privacy First hebben aangegeven dat goed rekening dient te worden gehouden met de privacybelangen van de consument[8].

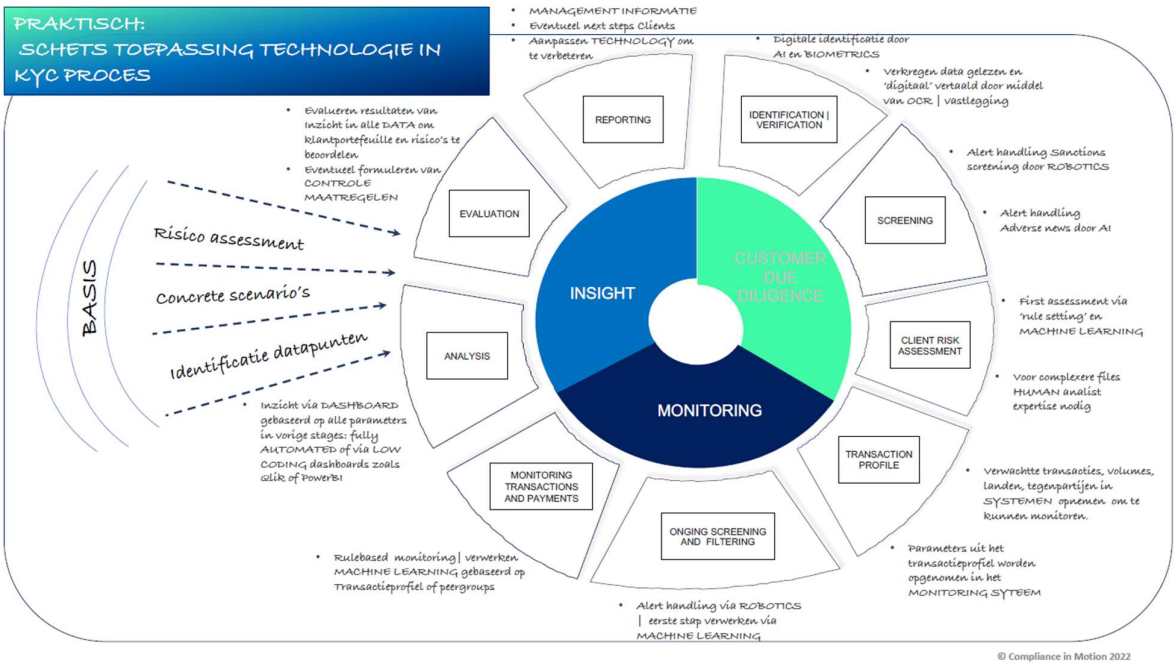
Technologie in het KYC-proces: een praktische toepassing

Het 'Ken uw Klant'-principe (KYC), waarbij in de *client life cycle* diverse fases op het gebied van compliance kunnen worden geïdentificeerd, is een speeltuin voor IT-leveranciers. Op dit moment is er (nog) geen *one size fits all*-platform in de markt om het hele KYC-proces op de gehele *cliënt life cycle* toe te passen. Er worden dus nog veel platformen met elkaar verbonden door deze leveranciers. Dit is niet alleen relevant binnen de financiële sector maar zeker ook daarbuiten. Naast bestaande antiwitwaswetgeving kan de nieuwe Corporate Sustainability Due Diligence Directive[4], waarin due diligence op meer plaatsen in de *supply chain* terugkomt, ook zomaar van toepassing zijn op instellingen van buiten de financiële sector. Kennis van het KYC-principe en de impact op de *supply chain* is essentieel om de technologische keten effectief in te richten.

De achtergrond van de FATF-aanbevelingen is duidelijk: het gebruik van deze technologie moet leiden tot een effectievere aanpak van witwassen en terrorismefinanciering. En bij gebruik zelfs meerdere integriteitsrisico's of misstanden optimaal identificeren via een beperkt aantal geautomatiseerde handelingen. Maar hoe is dit in de praktijk toe te passen? En is het mogelijk om met enkele simpele oplossingen toch efficiënter en effectiever te zijn?

In de volgende figuur schetsen we een praktijkvoorbeeld van het KYC-proces in de *cliënt life cycle*, die doorlopend aangepast en verbeterd dient te worden:

[4] Corporate Sustainability Due Diligence Directive: https://ec.europa.eu/info/business-economy-euro/doing-business-eu/corporate-sustainability-due-diligence_en#documents



Bron: Compliance in motion, 2023

Zoals in de figuur weergeven, en eerder al bij de randvoorwaarden benoemd, is bij het inrichten van een compliance-organisatie het uitvoeren van een risico-assessment fundamenteel. Bij voorkeur doet men dit zoveel mogelijk op basis van data en wordt het doorlopend bijgesteld afhankelijk van omgevingsfactoren. Het vaststellen van de risico's en de bijbehorende beheersmaatregelen wordt vervolgens systematisch geplot binnen de getoonde fasen in de *life cycle*. Dit is ook wat de FATF onderstreept in haar studie.

Waar dit proces in de huidige praktijk echter scheef gaat lopen is dat de gegevensstroom beperkt blijft tot een 'papieren exercitie', suboptimaal ondersteund door spreadsheetachtige oplossingen. Men mist inzicht in de echte risico's en aan gedegen *red flag*-scenario's gerelateerde datapunten. Deze datapunten zijn nodig om in de berg data in systemen concreet en eenduidig de echte risico's te signaleren. En zonder gedegen data leidt het inrichten van compliance-processen binnen de instelling daarom al gauw tot ruis, subjectieve veronderstellingen en eigen interpretatie door verschillende teams en professionals.

Naast een goed fundament voor de transitie naar technologische ondersteuning van het compliance-raamwerk zijn er nog een aantal praktische suggesties waar een compliance officer of IT-auditor rekening mee kan houden in zijn of haar advies:

- Het zorg dragen voor een brede groep aan deelnemers bij het uitvoeren van een risico-assessment, inclusief IT-stakeholder.

  Datapunten, systemen (en het ontsluiten van de data), koppelingen, dat is de expertise die je ook nodig hebt voor het inregelen van effectieve geprogrammeerde beheersmaatregelen;
- Vragen om een complete *IT Landscape mapping* en een visie op het toekomstige landschap in relatie tot het onderwerp van AML/CFT-technologie;
- Het goed inrichten van *data governance* (met onder andere duidelijke definities), want: *garbage in is garbage out*;
- Continue monitoring en opschoning van de data wat noodzakelijk is voor de datakwaliteit;
- Output moet terug te herleiden zijn naar de risicobeoordeling (de zogenaamde *data lineage*);
- Het klein beginnen, omdat organisaties vaak vele legacy-systemen hebben die niet makkelijk even te ontsluiten zijn.

Tot slot: voor de echte complexere situaties en de besluitvorming (denk hierbij ook aan de AVG!) blijft de menselijke factor noodzakelijk. De systemen moeten de compliance-processen gaan ondersteunen en repetitieve taken zoveel mogelijk automatiseren. Kennis van de business, samen leren en samenwerking tussen disciplines blijft echter cruciaal bij het toepassen van de technologie.

Dit artikel is een publicatie van de Vereniging van Compliance Professionals; sinds 2001 dé beroepsvereniging voor professionals op het gebied van Ethiek, Compliance en Integriteit.