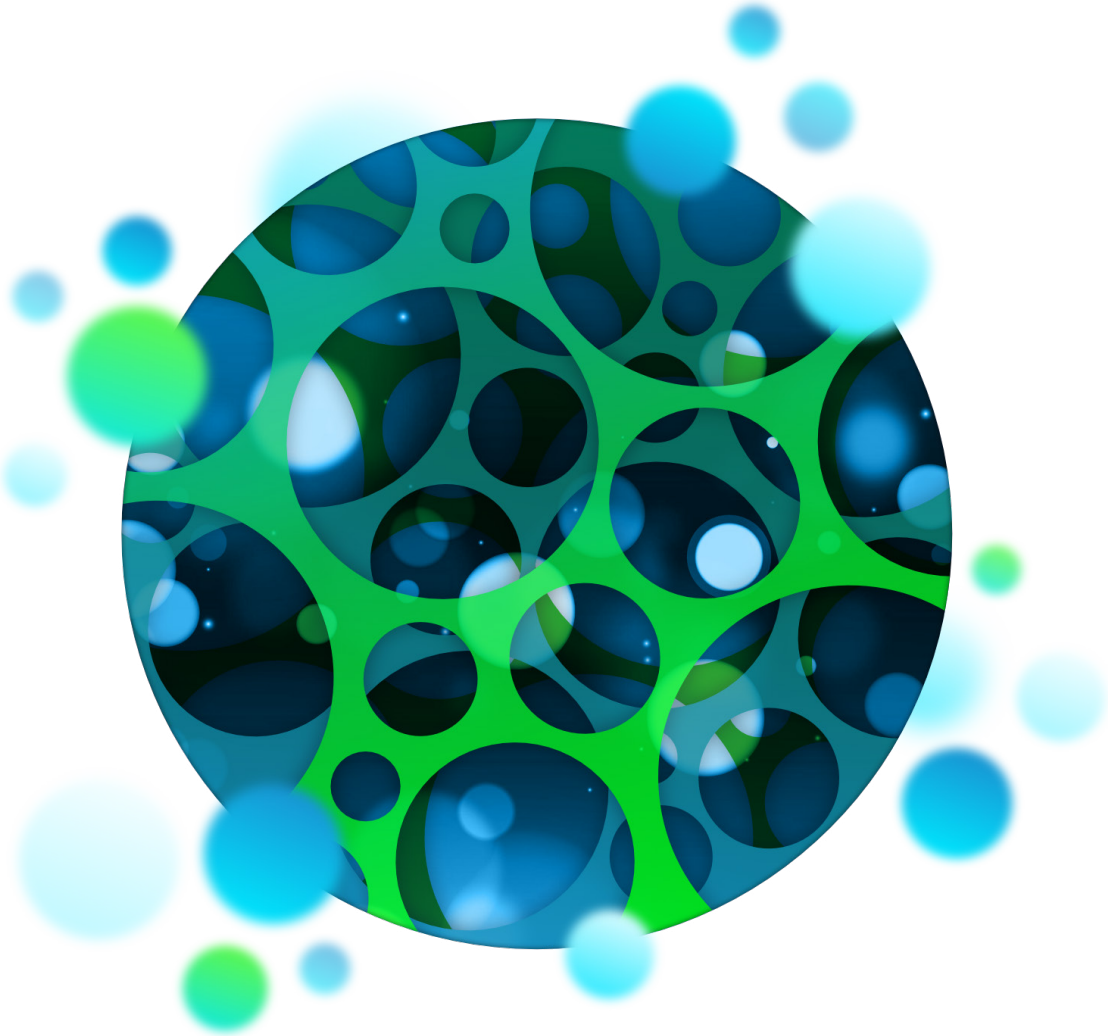
Deloitte.



NextGen AML : A point of view

Ideas on transforming the Dutch anti money laundering effort

MAKING AN IMPACT THAT MATTERS since 1845

Deloitte Netherlands
Forensic & Financial Crime

Contents

1. Introduction

Amid growing regulatory and public scrutiny, financial institutions are mounting massive efforts to fight money laundering through their systems — but the actual effect on financial crime is as yet disappointing (see Figure 1). We believe it's high time for a radically new approach: NextGen AML. What that means? First, going back to the legal basis of current anti-money laundering practices. Then, focusing on deep impact and clear outcomes.

When financial institutions (FIs) appear in the media these days in connection with financial crime, the spotlight is on fines and sanctions, or on the huge army of staff involved in detecting money laundering. Only incidentally do these reports highlight the actual outcomes of the collective AML efforts. This illustrates the case for change we see for AML. A better AML approach, we believe, would be driven by impact, become smarter and digitalised, turn wasted efforts into a connected defence, and prepare an adequate response to emerging crime schemes.

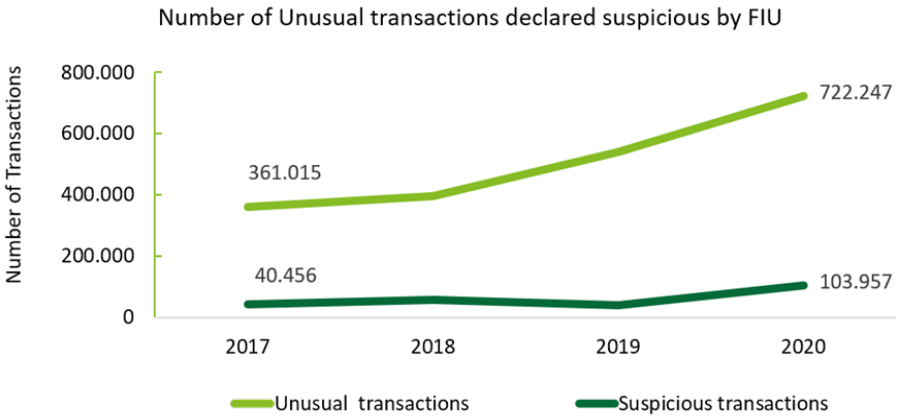


Figure 1 *(Sources: Annual reports FIU)*

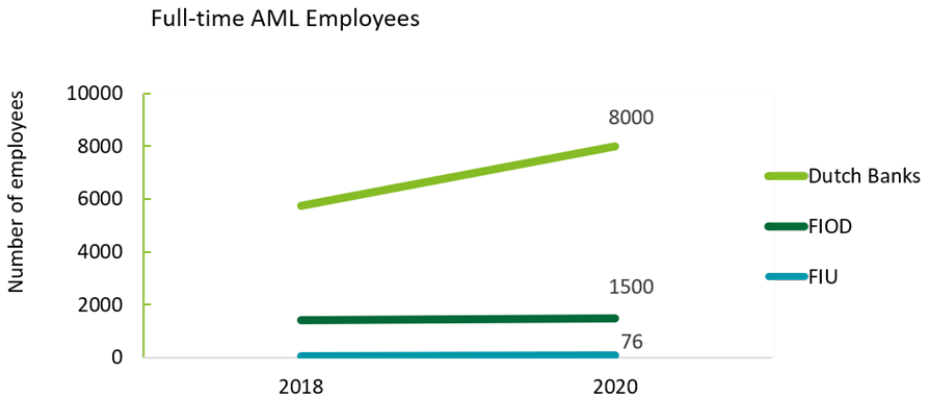


Figure 2 *(Sources: Annual reports FIU, Jaarplan Belastingdienst 2021, NVB)*

Mounting pressure on FIs

In April 2021, the Dutch financial sector was once more shaken-up by the second major settlement[1] for violation of anti-money laundering and counter-terrorism financing regulations. Moreover, the Dutch regulator has just confirmed that yet another financial institution is under criminal investigation, proving that the regulatory pressure on our financial institutions is not going to ease up any time soon. A trend that is also seen globally.

Too many people, too little impact

So what is the financial sector's response to this growing regulatory scrutiny? Snowballing more and more resources into remediation and enhancement programmes. The most noticeable symptom being the exponential rise in the number of employees active in an AML/KYC role (see Figure 2). Financial institutions are paying thousands of people to perform compliance checks. But the

[1] Netherlands Public Prosecution Service, news item 19 April 2021, https://www.prosecutionservice.nl/latest/news/2021/04/19/abn-amro-pays-eur-480-million-on-account-of-serious-shortcomings-in-money-laundering-prevention

impact of these ever-increasing efforts is questionable: will they produce a more vigilant financial system, and in the end make the world a safer place?

Box-ticking

Consensus is growing that the current AML framework, while costing billions of euros annually, is not as effective as it should be. And more fines will not necessarily lead to better outcomes. Why is this? Firstly, within operations, there is a strong short-term focus on 'technical compliance', which comes down to mere box-ticking. Additionally, the total system is by its very nature painfully slow. In many cases it takes years before a criminal transaction is even identified as suspicious, let alone before the originator gets prosecuted. By contrast, financial criminals are extremely quick to adapt to changes in the financial landscape.

Reinventing AML

So just doing more of the same will not stop the problem. The sheer complexity of financial crime and its far-reaching social consequences calls for broader solutions involving partnerships and ecosystems. This was also underlined in the presentation of the Nationaal Plan Witwassen in 2019.[2] We believe that current implementations of the AML framework have reached end of life and are ready for reform. Especially considering the challenges yet to come. To upgrade the AML approach, parties must:

1. Increase impact — Transform to more effective efforts, and give a strong push on actual crime reduction.

2. Be smarter — Digitalise the fight against financial crime with more and better data and the latest technology.

3. Reduce waste — Stop unnecessary efforts and align cooperation in the entire chain of actors against financial crime, creating a connected defence.

4. Be prepared — Anticipate and adjust to new modus operandi of financial criminals, in existing infrastructure as well as future platforms.

NEW PERSPECTIVE

What's needed is a new perspective about how financial crime should be combatted in a joint effort spanning the whole chain. Still based on the legally bound roles of actors, but with enhanced and better aligned strategies. This is what we call NextGen AML. In this paper, we'll be revealing our view on the drivers that will help to achieve this required change in the whole industry.

[2] Dutch government website, 1 July 2019. https://www.rijksoverheid.nl/actueel/nieuws/2019/07/01/minister-hoekstra-en-grapperhaus-presenteren-nationale-aanpak-witwassen

2. A case for change

Are the outcomes of current Anti-Money Laundering implementations worth the vast efforts that players in the field put into it? To increase impact, reduce unnecessary efforts and keep up with criminal inventiveness, a new approach is needed. But how do we get there? Creating NextGen AML calls for change in five driving areas.

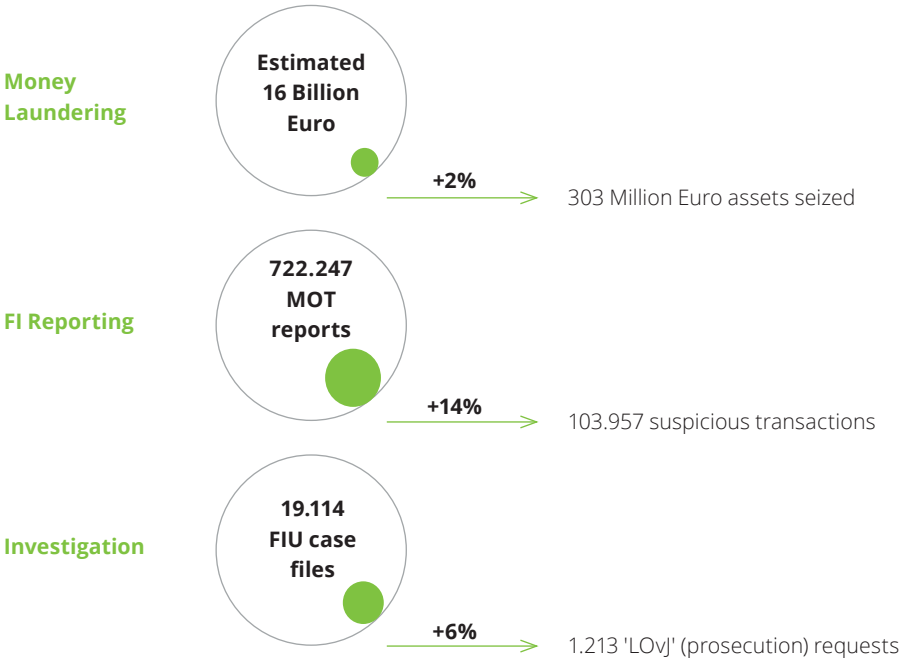


Figure 1: Overview money laundering KPI's
(sources: Universiteit Utrecht, OM Report 2020, FIU Annual Report 2020)

To spot the shortcomings in the current AML approach, it's good to zoom out and look at the entire AML chain (see Figure 1). It starts with money laundering itself. Crime doesn't really pay until criminal money finds its way into the financial system, and can be used to buy for instance houses, cars, luxury goods, financial assets, and political influence. Money laundering is what makes crime worth trying, and why crime is a disruptive force in the financial system and in society.

Legislators, who observe the cost to society of money laundering, draft their law with the goal of fighting financial crime. The law appoints financial institutions as gatekeepers and obligates them to (1) perform reviews and monitoring on clients and transactions and (2) report unusual transactions to the Financial Intelligence Unit.

Losing sight of the goal

But somewhere along the line, the original goal of the law has drifted away. The law and directives, and the regulating financial industry obligations that may be seen as following from this law, became an end in themselves. Financial institutions, fearful of fines, have become heavily focused on their own regulatory safety. In response to the increasing public and regulatory expectations, they perform more checks. More and more checks. With more and more people.

This has resulted in a significant increase in the number of clients and transactions reported to the Financial Intelligence Unit (FIU) as 'unusual' in recent years. The additional checks and reports arguably have resulted in fewer potential forms of money laundering going unnoticed. Meanwhile, however, the FIU and other public parties have been struggling with limited budgets. So

just a fraction of these reports from the FIs actually got followed up by law enforcement. This means that, apart from the potential remedial and preventive effects that arise from efforts by financial institutions, the output of these well-intended but uncoordinated efforts has been inevitably modest. Financial crime continues – maybe less unnoticed but still far from eliminated.

Change in five driving areas

This, admittedly simplified, story reveals an AML framework at end of life, suffering from a variety of shortcomings. Initiatives are underway to tackle some of them, but accelerated and more ground-breaking change will be required to really fix the AML framework. In our analysis, we've identified five kinds of change that need to be accelerated:

Together, the measures proposed here will result in a smarter, more digitalised AML approach with far more impact. One that turns isolated efforts into a connected defence and prepares an adequate response to emerging crime schemes.

1. Ecosystem drive: AML is not the sole responsibility of the 'gatekeepers'. Let's make effective cooperation between public and private parties, now emerging in many places (and perhaps too many different places), the default. Let's get parties sharing information and aligning their core strategies and intended outcomes.

2. Intelligence drive: Intelligence, feeding both rapid response and careful thinking, is key. Let's replace the current reactive, static, rules-led processes with proactive and agile ones that go deep and fast on detecting real criminal networks.

3. Output drive: Let's remember what these processes are supposed to deliver: less money laundering, more justice. Let's rethink wat 'risk-based approach' really means: not screening everything so as not to miss a single risk, but directing efforts where risk is highest.

4. Data drive: Data is a plentiful and rich resource, but to make AML more effective, it needs to be properly organised and cleaned. And it needs to be shared among ecosystem partners without compromising cyber security and privacy.

5. Technology drive: The days of 'compliance by workforce' are over. To make sense of the mountains of data, while reducing human effort, let's make radical choices and rack up investment in (AI) technology. And let's do it together, financial institutions and the public sector, as that's the only way to keep innovation on track.

BUILDING NEXTGEN AML

We see first steps being taken in all five areas. However, change is not fast, coordinated and foundational enough. Real progress is a matter of scaling up and accelerating the many promising initiatives, while creating maximum space for cooperation and innovation. The following chapters discuss each of these themes, analysing the current situation and proposing what we think it will take to achieve NextGen AML.

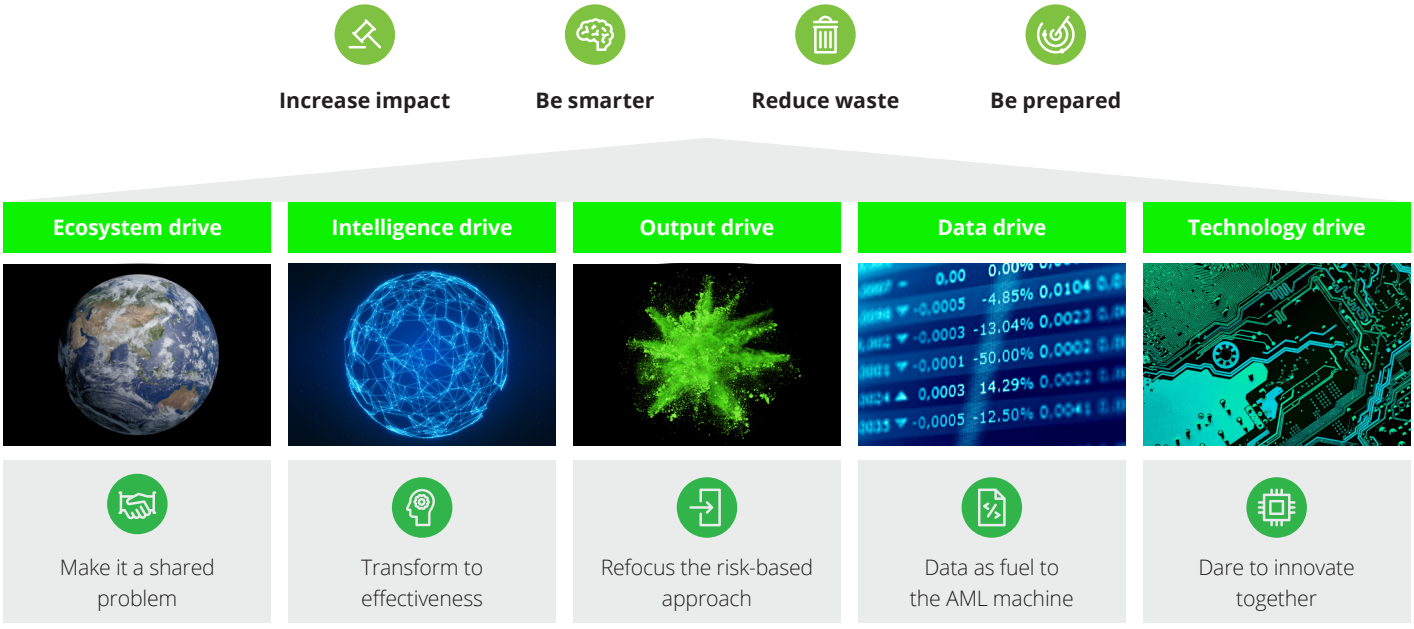


Figure 2: NextGen AML framework

3. Ecosystem-driven change

A big step towards more effective AML efforts would be to improve the organisation of processes within the ecosystem of financial institutions, regulators and law enforcement.

Collectively, FIs are the gatekeepers of the financial system, responsible for keeping criminal money out. However, their efforts are at the moment largely executed in isolation and hence disconnected. FIs each have their own AML approach implemented by their own compliance teams. FIs do realise, though, that more coordination is needed, and they are working hard to achieve this. A good example is the launch of Transactie Monitoring Nederland (TMNL): a joint transaction monitoring utility set up by five major Dutch banks, in which they monitor a subset of their transaction data in encrypted form on multibank networks.

Public-private partnerships

In the broader financial ecosystem, however, there are also public sector organisations with a crucial role to play in improving AML practice, such as legislators, supervisors, FIUs and law enforcement agencies. They need to work effectively with FIs to make the overall AML effort worthwhile. There is no lack of good intentions in the field, witness the numerous small-scale initiatives. One such initiative is the Serious Crime Task Force (SCTF), in which tactical information is shared between Dutch law enforcement agencies and FIs in order to close the feedback loop and speed up response times. The leads produced by SCTF are for the most part actionable for law enforcement, and are much more effective than the avalanche of unusual transaction reports coming from FIs. However, to deliver its full potential, public private cooperation should be more than a flurry of isolated initiatives, with signals of overlap and duplication. Parties should place such cooperation at the heart of their strategy, where operating in ecosystems is the default rather than an add-on to regular AML activities. And they should do so because they genuinely believe that it's the right way to go.

Believers

So where should that that belief in public-private cooperation be grown? The first step is to enhance the mutual trust between the parties. The success of the current small-scale initiatives has already sown valuable seeds of trust throughout the ecosystem, and these need to be cultivated. Public sector parties should cultivate the seedlings by incentivising cooperation and removing barriers. If and when they do so, FIs can afford to invest more in impactful AML actions and feel less scrutiny. The common purpose that all ecosystem parties should be working towards is to make money laundering as difficult as possible, and to make the financial benefits of criminal activities much less appealing. Public and private sector parties should feel that they are part of the same team – each with their own roles and responsibilities – and should have similar incentives and targets to act on their common purpose.

Central coordination

Above all, a national AML coordinator is needed to steer the many existing initiatives and ensure that public private cooperation gains momentum. The person appointed should be a real connector, not a micromanager of tactical and operational issues and procedures. Their first task is to align public and private parties on strategy, priorities and the efficient use of the available resources, and their second task is to monitor execution. The AML coordinator could be a public sector role, similar to the National Counter-Terrorism Coordinator, complemented with appointees from the financial sector. Cooperating within an effective and efficient governance model, they should jointly set the course for the entire ecosystem of public and private parties and provide a frictionless framework for operational cooperation. Such coordination will merge the individual initiatives into a connected, strong and effective defence system. And needless to say, sufficient funding is essential to achieve strong central coordination.

Secure information highways

Another important task for the coordinator is to enable more and faster information exchange in the financial ecosystem. It's time to open up secure and selective information highways across private-private, public-private and international borders. Currently, FIs are afraid to open up to their competitors or supervisors. Parties fear overstepping perceived restrictions following legislation and EU directives. In fact, however, AML and privacy legislation offers more wiggling room than parties are using right now. FIs and public sector parties should establish together how far they are willing and able to go and how this can be explained and accounted for towards all relevant stakeholders in society. By conducting a transparent and due process, enabled by technological advancements, a careful balance can be found between fighting crime by sharing information and protecting basic and important rights of individuals.

Common plan of attack

To ensure that all ecosystem partners realise the full potential of a common public-private agenda against financial crime, a common plan of attack is needed. The National Risk Assessment (NRA) against money laundering could serve as such a strategic management document — if it were to describe joint strategic goals and priorities, if it were to be more frequently updated, if it were to receive broader attention and support, and if it were to be operationalised on a deeper level to make it actionable in practice. Such as common plan of attack would also enable public and private parties to focus and maybe even pool their resources in order to develop and implement AML innovations responsibly and more cost-efficiently. Let's not forget the financial benefits that this would bring.

PUBLIC-PRIVATE COOPERATION ON STEROIDS

Public-private cooperation in the financial ecosystem at its current level is promising, with plenty of good intentions and smaller scale developments. However, in order to reach the desired NextGen AML state, this cooperation needs to be gathered up, coordinated and put on steroids. Not just because it's a recipe for higher-quality AML reporting by FIs and for faster feedback and action on these reports. But also because participation and active collaboration in the ecosystem should be seen as a key metric of maturity of the AML framework. Moreover, this ecosystem-driven change is essential to enable the next kind of change we'll be discussing: intelligence-driven change.

4. Intelligence-driven change

Anti-money laundering processes are often 'one size fits all'. All clients and transactions receive similar treatment within large scale factories. This is causing loads of red tape for ordinary citizens and businesses, while criminals may still manage to escape notice. It's time for a smarter approach, one that some FIs are already pioneering. As true front runners of NextGen AML, they adjust their focus based on the latest intelligence from across the AML ecosystem.

In the current state of affairs, FIs feel forced to funnel all their payment traffic through vast, FTE-heavy AML processes. Traditionally, these static, rule-led processes produce lots of individual signals, of which many are unlikely to be crime related. In the absence of deeper understanding of the key money laundering schemes and risks, FIs sustain these approaches, afraid to miss cases and anxious to prove their 'technical compliance'.

Sharing more intelligence

Meanwhile, other parties in the ecosystem have potentially useful intelligence. Intelligence following from criminal investigations, for example. FIs can use this information to find and report money laundering transactions — and terminate or limit the criminals' access to the financial system.

This is already taking place on a modest scale in the Netherlands. For example in the country's Financial Expertise Centre (FEC), in which regulators, ministries and law enforcement are represented and strategies are aligned. And in the Fintell Alliance, where specially screened employees from several banks work side by side with the experts of the Financial Intelligence Unit (FIU). FIs outside such initiatives, however, only receive ad-hoc requests in connection with incidents and cases.

In the NextGen AML framework we envisage, the pool of intelligence to be shared will be far richer. All parties will continuously share intelligence on a structured basis, preferably coordinated centrally (see previous chapter). This intelligence can be multifold: detailed modus operandi, actionable typologies, tactical information related to specific networks and schemes, and general intelligence on money laundering patterns. In other words: exchanges that are now happening ad hoc or on a limited scale will become the default and large scale. This also means that more legislative room must be made for public-private and private-private information sharing.

Slow and careful thinking

When this flow of intelligence starts picking up, all parties involved need to be ready for it. In the current set-up, there is not always sufficient capability and capacity to handle new intelligence. Both on the public and private side, staffing is focused on sustaining the usual level of 'technical compliance', leaving limited time and capacity for more intelligent scenarios and searches. Intelligence can then end up on the shelf. The danger is that if the parties providing the information see no results, they will sense a pushback, become demotivated and give up. Utilising intelligence calls for orchestration of the AML ecosystem.

FIs would therefore do well to anticipate this increased flow of intelligence by setting up a sound process ('intelligence pipeline') for receiving and assessing it. One that checks the reliability of the source. One that weighs the feasibility of acting on the intelligence against what the organisation itself has to gain or lose from doing so. One that, once the intelligence has been found worthy for follow-up, specifies precisely how to do so. This 'slow and careful thinking' will enhance

the compliance risk management cycles (in the Netherlands: SIRA) that most FIs already have in place.

More intelligence and better processes for using it will ultimately enable FIs to do less. Intelligence is about focusing efforts where it matters. This means that, if there are no intel signals about a specific area, FIs can decide that it is not really worth investigating, and stop efforts in this area. Existing controls (such as transaction monitoring) can be sharpened, resulting in fewer clients being signalled and requiring review. And some of the current controls — ones that lack precision and proven effectiveness based on true intelligence from the field — can be stopped.

Rapid response and fast thinking

Eventually, this process could become more agile and integrated, and be linked to the upgraded version of the National Risk Assessment (NRA) we proposed in the previous chapter. The advantage of having a sound process is that when the FI decides to act, a protocol of appropriate actions will already be in place. And since the routine compliance workforce is already overwhelmed, this needs to be tackled by a dedicated team, who will take the intelligence and run with it: rapid response. As said, a few pioneer FIs already have such teams. By performing high-speed checks and analyses, and connecting with like-minded experts elsewhere in the ecosystem, they can quickly find relevant transactions and clients based on intelligence and ensure quick follow-up, both internally and by public parties. The result is a cycle that is much faster then the traditional cycle of FATF recommendations, EU directives and local legislation and guidance. A cycle that stops criminals and money laundering risks sooner.

Of course, technology is key in making the analyses faster and more effective. Typologies can be encoded, for example, and artificial intelligence can help the experts discover patterns and networks. In the ultimate NextGen AML situation we envisage, the entire ecosystem will be working with these technologies and will collaborate to innovate these.

This does mean that an FI's team must include both money laundering experts and data science specialists, or, even better, that rare breed who really understand both: 'purple people'. People like this will be needed across the ecosystem, to help make the most of technology — and, importantly, to ensure this technology is applied responsibly, taking proper account of security, privacy, and ethics.

Ultimately, this will lead to a more intelligent system, in which the static and simple controls of the 'technical compliance' version of the AML framework are replaced by more proactive, agile and well informed measures. Rather then doing simple things on a bulk of signals, FIs will gradually shift towards deep-diving into (combinations of) patterns and networks with the biggest financial crime impact.

NO SITTING BACK

For now, the flow of intelligence from the ecosystem has to gain further momentum, but FIs don't need to sit back and wait for that to happen. By beefing up their own parallel, intelligence driven compliance processes, FIs can get better results from the information they already have, and detect AML more quickly and effectively. Plus, they can instantly benefit as soon as information sharing in the ecosystem really takes off. This will enable FIs to generate more relevant outcomes, with less direct human effort, where it adds most value. A benefit that will also serve as the cornerstone for output driven change in AML, the subject of the following chapter.

5. Output-driven change

If the combined AML efforts of FIs, regulators and enforcers are to really reduce financial crime, they need to be focused where they will have most impact. That means first reaching agreement among themselves what the output of these efforts should be to make an impact. And then, importantly, making choices which new and existing AML processes they need — or don't need — to achieve it.

FIs are steadily ramping up their AML efforts. And indeed, the output of their 'AML factories', i.e. the number of transactions that are deemed useful to investigate according to the participating banks, has risen significantly in recent years. An encouraging, measurable output, but are these red flags really the output we're seeking from our overall AML efforts? Are FIs that report many potential unusual transactions 'AML champions'?

Measuring success

We could also define output as the number of criminal investigations resulting from current AML efforts. This output (partly because law enforcement can only investigate a fraction of the FIs' unusual transaction reports) is as yet fairly low. But how interesting is that as a measure of success? The first responsibility of FIs, as gatekeepers of the financial system, is to perform strong Client Due Diligence, and thereby keep money launderers from accessing the system in the first place. So the question is: do more unusual transaction reports and investigations, however welcome, really signal a better-working AML framework?

Taking AML to the next level, we believe, means looking beyond such quantitative output and focusing more on quality. Our collective goal should be to make money laundering harder, riskier and less rewarding for criminals. This is also the basis for the risk-based approach that various AML directives and policies are imposing. The question is, how do we make the AML approach more risk-based?

Joint strategy and tactics

As described in the previous chapters on ecosystem- and intelligence- driven change, we advocate stronger, broader, more structural alignment between parties in the AML chain. Especially when it comes to priorities, strategies and tactical information. In the ideal situation, with a strategic agenda agreed, financial institutions will pledge to reserve and deploy part of their precious human resources specifically for the chosen high-risk, high-priority themes. These teams will have the freedom to conduct their own investigations based on internal or external intelligence. On a tactical level, when they receive details from task forces on targets under investigation, they will also have capacity for a quick deep-dive, producing relevant information that gets immediate follow-up by law enforcement.

Rethinking instruction and supervision of FIs

However, freeing up enough capacity for this targeted approach will only happen if FIs can afford to reduce the amount of staff working on low-risk, low-priority checks. State-of-the-art technology may help to smooth the way for this paradigm shift, but in the meantime, what FIs need is the assurance that, if their overall AML approach meets requirements, the regulator can grant them at least a little room for error. In the US, a setup in which FinCEN (the equivalent of our FIU) determines priorities that FIs should and could follow in their AML programmes has been enthusiastically received in the sector (AML Act 2020)[3]. It is seen as the first step towards shifting the focus of the regulatory framework from 'technical compliance' to outcome effectiveness. As our colleagues in the US have described, this opens up possibilities for FIs, but also comes with a series of

questions and challenges to consider. In the Netherlands, it would be interesting to explore these possibilities, too.

AML programme effectiveness

The ideal regulatory approach for assessing FIs' AML performance, in our view, is one that takes more account of what an FI is doing right. Rather than a primary focus on what has gone unnoticed, the regulator reviews an FI's AML programme in its entirety. And to evaluate whether the programme is effective both the FIs and the regulators alike should then have agreed-upon norms. Norms that are based on actual outcomes and output, rather than on paperwork conditions that do not directly create an impact against financial crime in the real world. Norms that incentivise innovations and new initiatives to meet the prioritised AML goals. FIs should not feel limited by scrutiny (such as lookback obligations) to do a better job on the AML priorities.

Focused control and resource allocation

As stated above, more clarity and regulatory certainty about AML priorities within the field will enable FIs to allocate their focus and resources to generate output that makes an impact. As such, they are not only adequately performing their general gatekeeper role. They are also providing reports that contain more actionable information for law enforcement, because the information is aligned with the public priorities that have been set. As with a better use of intelligence, explained in the previous chapter, this should also enable FIs to stop efforts that do not contribute to effective outcomes. For instance, periodic client due diligence reviews on low-risk clients without any deviating profile or behaviour can be replaced by more automated procedures, screening the client data for 'triggers' that have been proven to be indicative of financial crime risks. This will enable FIs to scope their reviews on clients with actual risks, rather then performing pointless technical compliance checks for all clients.

MAXIMISE VALUE ADDED

By making the AML effort output-driven, we can maximise the value added by FIs as gatekeepers. The current practice of blanket AML screening needs to gradually give way to a deeper and well-established risk-based approach, aimed at making impact where it matters. The already existing initiatives are only the beginning, and it's a matter of putting more push behind them. However, for the output driven AML framework to be successful, there is another firm requirement, and that's high quality data. More about that in the next chapter.

[3] Anti-money laundering (AML) program effectiveness, Deloitte. https://www2.deloitte.com/us/en/pages/regulatory/articles/aml-program-reform.html

6. Data-driven change

Any AML approach, and certainly a next-generation one, is fuelled by digital data. Fortunately, in our digital era there is no lack of available data to analyse. Indeed, FIs and other parties in the financial ecosystem are already struggling to handle the sheer mass of data generated by financial transactions and KYC processes. To leverage this valuable resource for AML, FIs must climb the data maturity ladder.

The current fight against money laundering involves a huge amount of data crunching. FIs in the Netherlands have plenty of data to work with, but many still lack the foundations to benefit from data. Due to IT migrations over the years (with scant attention to data management) and variations in tooling across groups, data is often scattered across a multitude of IT systems and in some cases even hard-copy files. This is perhaps worst for the older banks, which have foreign branches and a long history of mergers and acquisitions.

Data remediation

To make AML processes more effective (producing more valuable insights for the investigation of financial crime) and more efficient (fewer false positives), FIs are going through a data maturity journey. The first step is focused on data remediation: improving the quality of the data. Each FI is faced with the Herculean task of standardising its data and transferring it to its own centralised data lake or data mart. FIs are already tackling this inescapable task, but with traditional resources and approaches it's slow and painstaking work. However, standardising and centralising the data is not enough. Sometimes, data that is meant to fuel the AML machine proves to be sand in the gears. This happens when the data that is centralised is incorrect. To make it suitable for automated processes, the bank needs to review its client information, repairing errors and supplying missing data. At most Dutch financial institutions in the Netherlands this review cycle is well under way as part of the mandatory Know-Your-Customer procedures. All the while, though, new data is generated and old data becomes obsolete due to mutations. Getting a grip on this constantly changing mass of data, and keeping sand out of the gears, will get easier over time, though. How? Thanks to more awareness, growing expertise and better technology.

Data optimisation

The next stage is about automating and optimising data management, and strengthening AML with good data. This step is made easier by technical innovations like chatbots and image processing. They lead to better and smoother online client processes, which in their turn ensure that correct and consistent data, including good-quality images, is provided by clients directly in digital form. Besides this, a more structured approach[4] to managing digital data also includes active data quality monitoring. Clients are thus regularly reminded – and incentivised! - to update their details themselves. Data details such as name changes after marriage, new beneficial owners with legal persons, address changes or an expansion of the client's product portfolio need be taken into account when optimising the client data. As data is collected, the system can also enrich it with contextual data, enabling a wider and deeper understanding of client structures and behaviour. An FI with its own data lake full of such optimised data is halfway up the data maturity ladder. It is ready to start developing more advanced analytical models (described in the next chapter) and can achieve vastly better AML outcomes.

Data sharing

But just imagine how much more insight could be gained from combining and relating data within and across institutions in a safe

[4] The Foundation for Quality Data Management, Deloitte. https://www2.deloitte.com/nl/nl/pages/financial-services/articles/the-foundation-for-a-strong-data-quality-management-practice.html

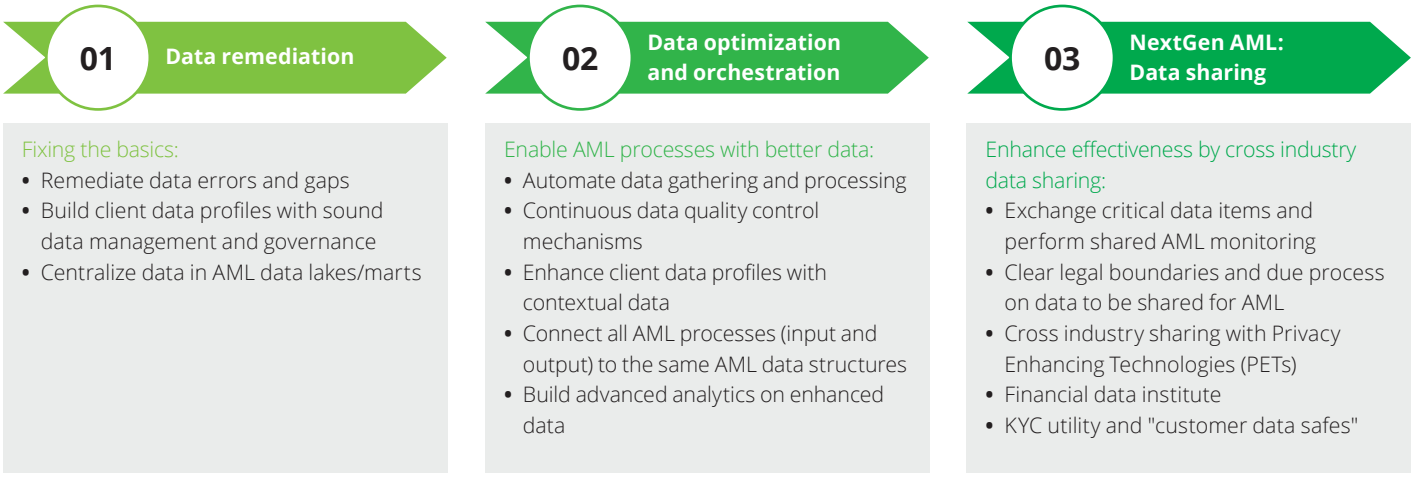


Figure 1: AML data maturity

manner. Pooling data is the final step that will bring FIs to the top of the data maturity ladder. Within the AML domain, it is widely recognised that data sharing across institutions and maybe even countries is required to fight crime. The Netherlands is a front runner in this space, for example with the pioneering initiative Transaction Monitoring Nederland (TMNL).The Financial Action Task Force (FATF) recently published its *Stocktake on Data Pooling, Collaborative Analytics and Data Protection*.[5] This publication, based on discussions with a range of experts worldwide, makes the case for data sharing and collaborative analytics. Given that FATF's standards and recommendations will find their way into US and European legislation, this can be seen as an important step towards more sharing. A series of approaches to share data have been trialled and described, but we will need to reach conclusions about the legal conditions and processes within which such sharing can be done responsibly.

What about privacy?

FATF does cite data privacy as a challenge in the context of data pooling. Indeed, data pooling may seem at odds with privacy regulations and interests. But the EU's GDPR is in fact not a set of prohibitions per se. It also defines guidelines and processes for using data responsibly: for a specific, legitimate purpose, in a way that is proportional to that purpose and explainable to stakeholders. Fighting financial crime is without doubt such a legitimate purpose, given its large societal impact. This doesn't justify all kinds of data sharing, though. It just implies that stakeholders and actors should follow a due process in deciding which data can be shared for which purpose, and under which conditions. Additional guidance from regulators and/or more precise AML legislation would be invaluable in going through this process. Moreover, apart from the due process and legal boundaries, there is also technical innovation. Privacy enhancing technologies (like the one being described in the FFIS project)[6] can open up new methods for sharing, while at the same time protecting the interests of ordinary, law-abiding consumers and businesses. This technology is still in the early stage of its maturity curve, but it may provide strong tactical solutions to reach the goal of responsible data sharing.

Financial data institute

At the top of the data maturity ladder, there would ideally be a non-profit organisation with a dual purpose. The first purpose would be to uphold standardisation and quality of data in the entire financial sector, a service that would be offered in the private and possibly also public domain. This organisation could produce common data dictionaries (the granular definitions of 'passport', 'first name', etc.). Secondly, this same organisation could centralise the process of data collection, validation and storage by clients of FIs. What if each client (natural person or business entity) had their own 'virtual data safe' where they store all the documentation required to be onboarded by FIs? With the client (as owner of the safe) deciding to whom, for what purpose and under which conditions the documentation is provided? Such a set-up would greatly enhance client data collection by FIs as well as the customer experience, while at the same time securing the data and providing transparency. This could form the basis of an industry-wide KYC utility, which we see being trialled at various locations around the globe.

ADDED VALUE FOR AML

The journey up the data maturity ladder is tough and laboursome, but essential. Without it, there can be no NextGen AML. But however mature our data is, it all still needs to be analysed, and traditional tools, even if they could handle the sheer mass of data available, cannot extract real intelligence from it. Fortunately, new technology, based on artificial intelligence, is emerging that can turn all this data into relevant information, and make AML a lot smarter. We'll be discussing the latest and greatest in the next chapter.

[5] Stocktake on Data Pooling, Collaborative Analytics and Data Protection, FATF. https://www2.deloitte.com/us/en/pages/regulatory/articles/aml-program-reform.html
[6] The Future of Financial Intelligence Sharing. https://www.future-fis.com/the-pet-project.html

7. Technology-driven change

Technology offers financial institutions a world of opportunities to make data-heavy anti-money-laundering processes faster and smarter. Artificial intelligence in particular promises to revolutionise the AML effort. FIs are scrambling to hop aboard this train, but to truly benefit from today's technology, they have work to do. First, revisit yesterday's legacy, and then develop a comprehensive tech strategy for the next decade. Meanwhile, regulators are challenged to keep abreast of these new technologies and create a safe space where they can flourish.

Endless possibilities

The Regtech market is awash with new applications that can make an FI's AML processes more efficient and effective. As discussed in the previous chapter, technology is vastly improving data collection, processing and validation. But where technology really makes a difference is in data analytics. Artificial Intelligence (AI)-based solutions can analyse data and detect irregularities much faster and more precisely than humans,. What's more, the self-learning models can increasingly recognise and ignore false positives, leaving AML staff more time to focus on the true hits.

These are some of the hottest technologies that have already delivered meaningful results and are promising more in the future:

1. Advanced entity resolution enables fully holistic client views and provides context to individual client attributes and transactions

2. Machine learning predicts risk scores on alerts and sorts them by priority (supervised machine learning) or detects unknown risk signals and finds new patterns (unsupervised machine learning/anomaly detection)

3. Network analytics make it possible to follow unusual money flows end-to-end and analyse complete networks and communities on unusual patterns

4. Recognition systems (e.g. facial recognition) can verify identity in a smooth client process with much better certainty than traditional human judgment

5. Orchestration engines combine a range of risk signals (fraud, AML, extraction requests, sanctions, etc.), making CDD processes faster and more effective

The benefits of technology like this are spectacular, but not necessarily futuristic: in many areas (also beyond AML), FIs are already applying these methods with the utmost caution and with great success. However, there is no single technology providing a solution for all AML business problems. The AML tech stack of the future will therefore contain a combination of various technologies and models (including traditional business rules). Rather than each FI choosing its own favourites, it would be good for them to compare notes, pool talent and develop collective solutions, also involving the public sector parties. For example, it would be great to maintain an 'AML github', secured but open to all ecosystem partners and including pieces of code that operationalise the newest typologies and models. TMNL, which monitors the transactions of five Dutch banks, is in that context a best practice worth copying in other areas.

Legacy woes

To make the most of these advanced technologies, FIs first have a big hurdle to overcome: IT legacy. When computers made their entrance in the world of business, FIs were among the early adopters, building big mainframes to handle their administrative processes. Over the decades – as FIs went through mergers and acquisitions, as new technologies emerged, as regulations changed and quick fixes were applied – their IT infrastructures grew organically into a 'spaghetti' of older and newer software applications. Looking specifically at AML,

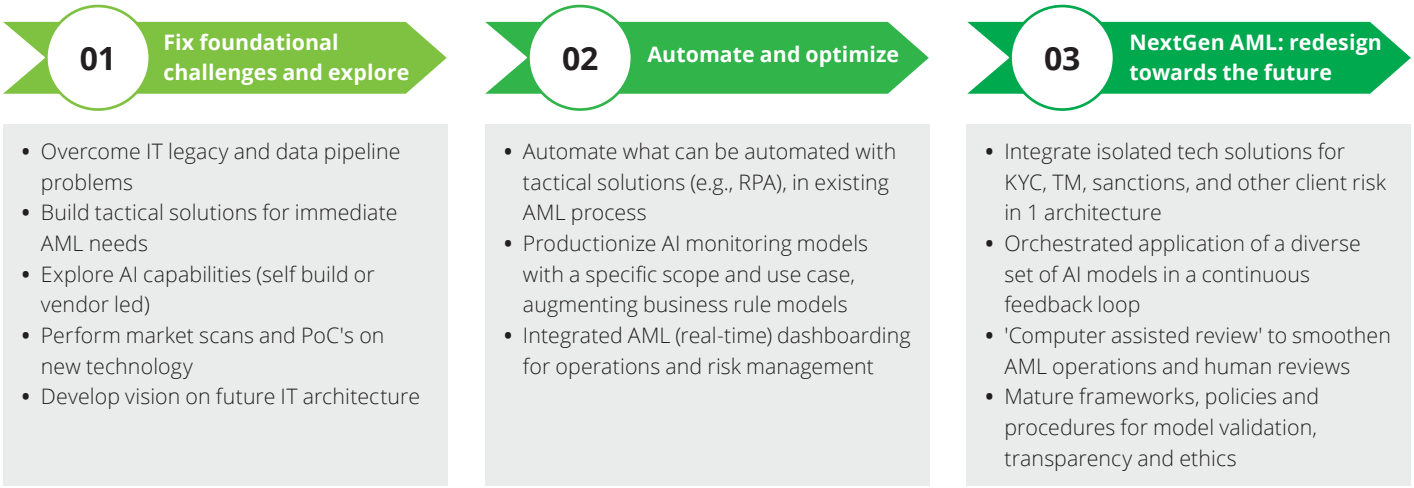


Figure 1: AML technology maturity

FIs have collected a basketful of separate applications for things like sanction list checks, KYC, transaction monitoring and FATCA compliance. Some bought new in the Regtech market, some just an existing program more or less successfully repurposed. Each add-on poses more risk to the stability and security of the legacy infrastructure, certainly given the vast amounts of data to be stored and processed. Moreover, as discussed in the previous chapter, all those promising new technologies cannot work effectively with non-standardised, poor quality data scattered across such a system.

Long-term tech strategy

When faced with technology choices under increasing regulatory and public scrutiny, the temptation for FIs is to do what they have always done: step into a dozen different ad-hoc solutions for a dozen individual problems, based on department-level decisions. FIs would do better, however, to step back from day-to-day pressures and think at strategic level about how they want to be dealing with AML a decade from now. With a long-term vision in place they can develop an integrated strategy to reach that destination: NextGen AML.

Specifically, this means rethinking the IT architecture behind the AML solutions. Instead of a duck-taped landscape full of unexplainable dependencies, it needs to become a modular platform that can readily accommodate further innovations as they emerge. A platform that can continuously inherit, test and productionise these innovations. And it also means ditching ad hoc solutions in favour of a holistic approach, encompassing all AML needs (KYC, TM, sanctions) and possibly more (other client risk and business domains).

Given the need for flexibility, NextGen AML is almost certainly going to happen in the cloud. The transition to cloud that is ongoing in the financial sector will unlock new tech enablers for FIs and give a boost to innovation. With data and key AML processes on multi-modal cloud platforms, there's no end to the incremental steps FIs can take to advance AI models and other functionalities. The AML cloud platform will be a key accelerator for tech innovation towards NextGen AML.

Regulator's role

For all the exciting possibilities that new technologies offer to really benefit the sector, however, the regulator must also keep up with them and create regulatory scope for their application. Current supervision is focused on individual human-based processes, like periodic client reviews and transaction monitoring. If these processes become machine-based, the focus of supervision will have to shift to a higher and deeper level: model validation. To assess models, the regulators will need in-house AI expertise. And they will have to use this new expertise to set new standards and frameworks that will reduce regulatory uncertainty and thereby support and embrace innovation. It is an encouraging sign that the Dutch regulator is taking meaningful steps in this direction.

With this shift in focus, regulators will have to assess FIs' performance differently: based on the effectiveness of the entire effort (for example model and data governance or orchestration of their signals) rather than on individual missed signals. For example, there is often discussion to what extent any new technology deployed must also be applied to historical data (lookbacks). Because the enhanced detection is bound to reveal irregularities that slipped through the net before, FIs, rather than being incentivised to innovate, are in fear of being penalised. In the US, proposals for a more balanced approach to innovation in AML, where FIs that innovate are given some room for error, have been received with great enthusiasm. Such an approach deserves consideration in our country as well.

Trust

The final question, then, is: how do all ecosystem players learn to trust these new technologies? Trust is an issue we cannot afford to ignore. Any application of AI that undermines trust will attract massive media attention and set back public acceptance of AI by years. An old-fashioned rules-based tool, despite its limitations, is perceived to

[7] Deloitte, 2021, Trustworthy AI and effective financial crime detection: not a zero-sum game https://www2.deloitte.com/nl/nl/pages/risk/articles/trustworthy-ai-and-effective-financial-crime-detection.html

be relatively transparent and explainable to both regulators and stakeholders. Unlike AI-based tools, which, if they are not adequately managed, documented and explained, can to non-experts be a black box. The challenge is to fanatically document the models and the underlying considerations, ensuring a clear audit trail that makes their operations explainable. The proposed EU legislation on Trustworthy AI[7] offers detailed guidelines to avoid ethical pitfalls. As this field matures further, it will provide further foundation and trust for innovation.

IN THE DRIVER'S SEAT

New technology is a must-have to lift AML to NextGen status. It has powerful potential to transform AML and change the way we do it, think about it, and look at the outcomes. There are risks, but with proper awareness and a concerted approach they can be managed within maturing frameworks. Fears of computers taking control are unfounded. Technology, even smart technology, supports rather than replaces human decision making, and humans will always remain in the driver's seat. New AML technology is a car built for speed and performance. To perform to the max, all it needs is a brave and responsible driver, guided by clear 'rules of the road' and inspired by a culture and system of open innovation.

8. Getting there together

In the previous chapters, we have identified issues with the current AML framework. We have discussed changes in five driving areas that can make AML efforts smarter, increase their impact and reduce operational waste. This chapter sums up the work needed to achieve NextGen AML. The challenge now: the entire financial ecosystem, from regulators and enforcers to FIs, must start taking action on all these good ideas at once and orchestrate them into solid momentum.

Our NextGen AML perspective is holistic, involving quite a lot of changes in the five areas highlighted above. Changes, moreover, that are interdependent. As such, it will require many conversations, loads of complex process redesign, shifts in relationships and a range of transformation efforts to come to a future AML framework.

Current efforts by FIs to fight money laundering through their systems are costly, without as yet achieving the desired effect on financial crime. The complexity and consequences of financial crime call for broader solutions. A better AML approach would be driven by impact, become smarter and digitalised, turn wasted efforts into a connected defence, and prepare an adequate response to emerging crime schemes. What's needed is a new perspective about how financial crime should be combatted in a joint effort spanning the whole chain. Still based on the legally bound roles of actors, but with enhanced and better aligned strategies. This is what we call NextGen AML. Getting there requires five change in five driving areas.

Activating the ecosystem

AML is the shared responsibility of all the public and private parties in the financial ecosystem. This includes FIs, legislators, supervisors, FIUs and law enforcement agencies. Better cooperation within the ecosystem will make the overall AML effort more efficient and effective. Existing public-private initiatives need to be incentivised, intensified and coordinated. Obstacles to such cooperation must be removed. Parties must draft a common 'plan of attack', based on an upgraded NRA. To do so, they need safe 'highways' for sharing information. Above all, a national AML coordinator is needed to steer the many existing initiatives and ensure that public private cooperation gains momentum.

Leveraging Intelligence

AML teams should be enabled to respond to the latest intelligence from across the ecosystem, for example data from criminal investigations, detailed modus operandi, actionable typologies, tactical information related to specific networks and schemes, and general intelligence on money laundering patterns. Sharing of such information should become the default and large scale, and legislative room must be made for it. This intelligence can be codified into technical procedures, by a team of 'purple people' (technical specialists and financial crime specialists in one). More intelligence and better processes for using it ultimately creates scope for FIs to give up current FTE-heavy blanket screening.

A keen eye on output

The ultimate aim of AML efforts is less money laundering, more justice, so parties need to look beyond output like unusual transaction reports and focus more on quality. The AML approach must become more risk-based: not screening everything so as not to miss a single risk, but directing efforts where risk is highest. This means regulators must grant FIs more room for error, and look more at what they're doing right. Basing their assessment on norms agreed with ecosystem partners. These norms should incentivise innovation. FIs should not feel limited by scrutiny (such as lookback obligations) to do a better job on the AML priorities.

Better and shared data
To make the most of data in AML processes, FIs must climb the data maturity ladder. This starts with data remediation: improving the quality of the data by removing inaccuracies, standardising formats and moving all data to a centralised (cloud) location. Next is data optimisation: keeping the 'clean' data up to date, automating data management processes and enriching data with contextual info. The final, crucial step is data sharing among ecosystem partners. A national data institute could be established to uphold data standardisation and quality and to offer FIs' clients a 'safe' where they can safely store their data and manage who accesses it. This could form the basis of an industry-wide KYC utility.

Smart use of smart technology
Advances in technology, and especially AI-based analytics tools, can revolutionise AML, promising faster and better analysis and fewer false positives. But to truly benefit, FIs must transform their legacy IT into a modular cloud platform that can accommodate further innovations as they emerge. Also, they must develop a comprehensive and integrated tech strategy — preferably together — for dealing with AML in the next decade. Regulators must keep abreast of new technologies and create a safe space where they can flourish.

Tactical and foundational change
Some change is and will be stepwise and tactical. For example when it comes to achieving more cooperation in the financial crime ecosystem, incorporating more intelligence into AML monitoring, and moving up the data maturity curve. Other essential change will be very foundational and will break through barriers. Examples are creating clear legal grounds for data and information sharing, developing mature regulatory perspectives on outcome effectiveness, and taking the step towards AML cloud platforms.

Debating roles
This kind of foundational change will have to be driven by a debate on the roles and incentives of each of the players in the AML chain. The gatekeeper role of financial institutions is one role that certainly needs further debate and clarification. What do we really expect from FIs in the fight against financial crime? But beyond that, other questions are waiting for well-considered answers. For instance, which party will be mandated to actively orchestrate actions and alignment in the full AML chain?

Focus on the future
The transition to NextGen AML calls for foundational and strategic thinking. It is that type of thinking and alignment that we would like to spark and facilitate. Because we believe that the current focus on fixing yesterday's compliance issues should be recalibrated to the future. Some of the change and debate is already ongoing, but we need to go faster and deeper.

This paper is primarily written from the perspective of today. Likewise, discussions in the field are often focused on being more effective in the current framework and state of the business. The future of financial crime will, however, be even more complicated and challenging. Criminals will continue to find new methods to hide and exploit their funds of illicit origin. Amid the fast-paced changes in banking and payments that are ongoing and coming up, with supervision often lagging behind, there will be plenty of opportunity for criminals to innovate their money laundering schemes as well. Traditional 'technical compliance' is only part of the answer, and by nature it is almost always too little, too late.

THE WAY FORWARD
In our opinion, the level of AML enforcement that we can achieve within the current AML framework is unsatisfactory. Even if it does result in compliance with current regulations. Society deserves better. All parties in the field should therefore support each other in finding new approaches to fight financial crime, with an open mindset on innovation.

Because the ultimate goal is not to prove 100% compliance to a law and avoid public and political scrutiny. The responsibility for all involved in the AML chain, either directly and indirectly, is to think and act beyond mere compliance. To create an environment that keeps up with the criminals, or preferably, stays one step ahead of them. The next horizon for AML is to do everything we can to maintain a financial system that is safe, trustworthy and accessible. For this generation and the next. We are ready to deliver for this future. Are you in?

NextGen AML: a Point of View

AML Glossary

AML	Anti Money Laundering
AI	Artificial Intelligence
AMLD	Anti Money Laundering Directive (EU)
ANPRM	Advance notice of proposed rule making
AVG	Algemene Verordening Gegevensbescherming (=GDPR)
BSAAG	Bank Secrecy Act Advisory Group
CDD	Client Due Diligence
FATF	Financial Action Task Force (36 landen)
FEC	Financial Expertise Centre
FI	Financial Institution
FinCEN	Financial Crimes Enforcement Network (US financial inelligence unit)
FIU	Financial Intelligence Unit
GDPR	General Data Protection Regulation
ILFC	Intelligence Led Financial Crime
KYC	Know your customer
LOvJ	Landelijk Officier van Justitie (National Prosecutor)
Nextgen	Next Generation
NRA	National Risk Assessment
PoC	Proof of Concept
PoV	Point of View
PPP	Public private partnership(s)
SAR	Suspicious activity reporting
SIRA	Systematic integrity risk analysis
TF	Trade Finance
TMNL	Transaction Monitoring Netherlands

Contacts

Hilko van Rooijen
hvanrooijen@deloitte.nl
+31882887771

Mark Hoekstra
mahoekstra@deloitte.nl
+31882885377

Robby Philips
rphilips@deloitte.nl
+31882887902

Deloitte.

Designed by CoRe Creative Services. RITM0846400