IBM × ITERA

# FIGHTING FINANCIAL CRIME WITH AI

How Nordic financial institutions can leverage technology, such as artificial intelligence, to prevent anti-money laundering.

ITERA REPORT 2021

# How Nordic financial institutions best can leverage technology to prevent anti-money laundering and fraud

**For the last decades, financial institutions, particularly banks, have been making strenuous efforts to prevent criminals introducing the proceeds of their crimes into the banking system. By interdicting attempts to infiltrate the money transmission networks in this way it is hoped to prevent criminals laundering their profits and subsequently using them in the legal economy. Currently financial institutions rely heavily on human involvement in labor-intensive, manual compliance processes. However, this is about to change.**

Effective anti-money laundering holds out the hope of reducing the activities of organized criminal gangs, interdicting human trafficking and drug trafficking networks, and intercepting terrorist funding. Anti-money laundering legislation has been introduced across all major jurisdictions and there is significant political consensus across the globe about the need to prevent this type of activity. It is not unusual for large global banks to have more than 5000 people working across the different aspects of Financial Crime Compliance and to spend more than $150m in acquiring Anti Financial Crime technology.

Yet, despite all these efforts, we are no closer to our goal after twenty years.  There are many reasons for our inability to interrupt criminals' efforts to launder their ill-gotten gains. These range from a lack of political will in certain jurisdictions to political corruption to significant problems with the technology and the approach utilized in detecting the flow of suspicious funds through networks of banks.

Artificial intelligence and cloud technology are increasingly being utilised to alleviate some of these issues when combating money laundering. The emergence of digital capabilities in the cloud has accelerated financial institutions' access to and analysis of information – at a massive scale.

We applaud innovative organizations that use data in smart ways and embrace the opportunities offered by cloud services. With this report we aim to shed light on how Nordic financial institutions can best leverage large amounts of data and modern technology to prevent financial crime. As technology companies, Itera and IBM are passionate about artificial intelligence and using advanced technologies in new scalable ways in the cloud. We are teaming up by combining local and global capabilities, industry experience, proven software, and a data-driven approach with use of advanced cognitive solutions and artificial intelligence to take the next step in preventing and uncovering financial crime. Itera and IBM are combining local and global capabilities, industry experience, proven software, and a data-driven approach with use of advanced cognitive solutions and AI.

**We hope you enjoy the read!**

**/ Stefan Astroza**
Head of Financial Services, Itera
stefan.astroza@itera.com

**/ Paul Clandillon**
Practice leader financial crime, IBM
paul.clandillon@ie.ibm.com

**/ Arne Mjøs**
Group CEO and founder, Itera
arne.mjos@itera.com

IBM × ITERA

> "As technology companies, Itera and IBM are passionate about artificial intelligence and using advanced technologies in new scalable ways in the cloud."

## Content

### Dictionary

| | |
|---|---|
| **AI** | Artificial Intelligence |
| **AML** | Anti-Money Laundering |
| **AML TM** | Anti-Money Laundering Transaction Monitoring |
| **ARS** | Automated Review System |
| **CAM** | Client Activity Monitoring |
| **CDD** | Customer Due Diligence |
| **CFT** | Combating Financing of Terrorism |
| **CLM** | Customer Lifecycle Management |
| **CRR** | Customer Risk Rating |
| **EBA** | European Banking Authority |
| **DRR** | Dynamic Risk Rating |
| **EEA** | European Economic Area |
| **EDD** | Enhanced Due Diligence |
| **EU** | European Union |
| **FP** | False Positives |
| **FSA** | Financial Supervisory Authority |
| **FTAF** | Financial Action Task Force |
| **KYC** | Know Your Customer |
| **ML** | Machine Learning |
| **PEP** | Political Exposed Person |
| **RPA** | Robotic Process Automation |
| **SAR** | Suspicious Activity Report |
| **TM** | Transaction Monitoring |
| **TP** | True Positives |

# Key findings

Ranked top

8

in AML:

Finland, Norway, Sweden and Denmark.

See page 10

Up to DKK

10 bn

in fines to a Nordic bank.

See page 11

Between $1.6 to $ 4 trillion are laundered annually.

See page 5

Up to

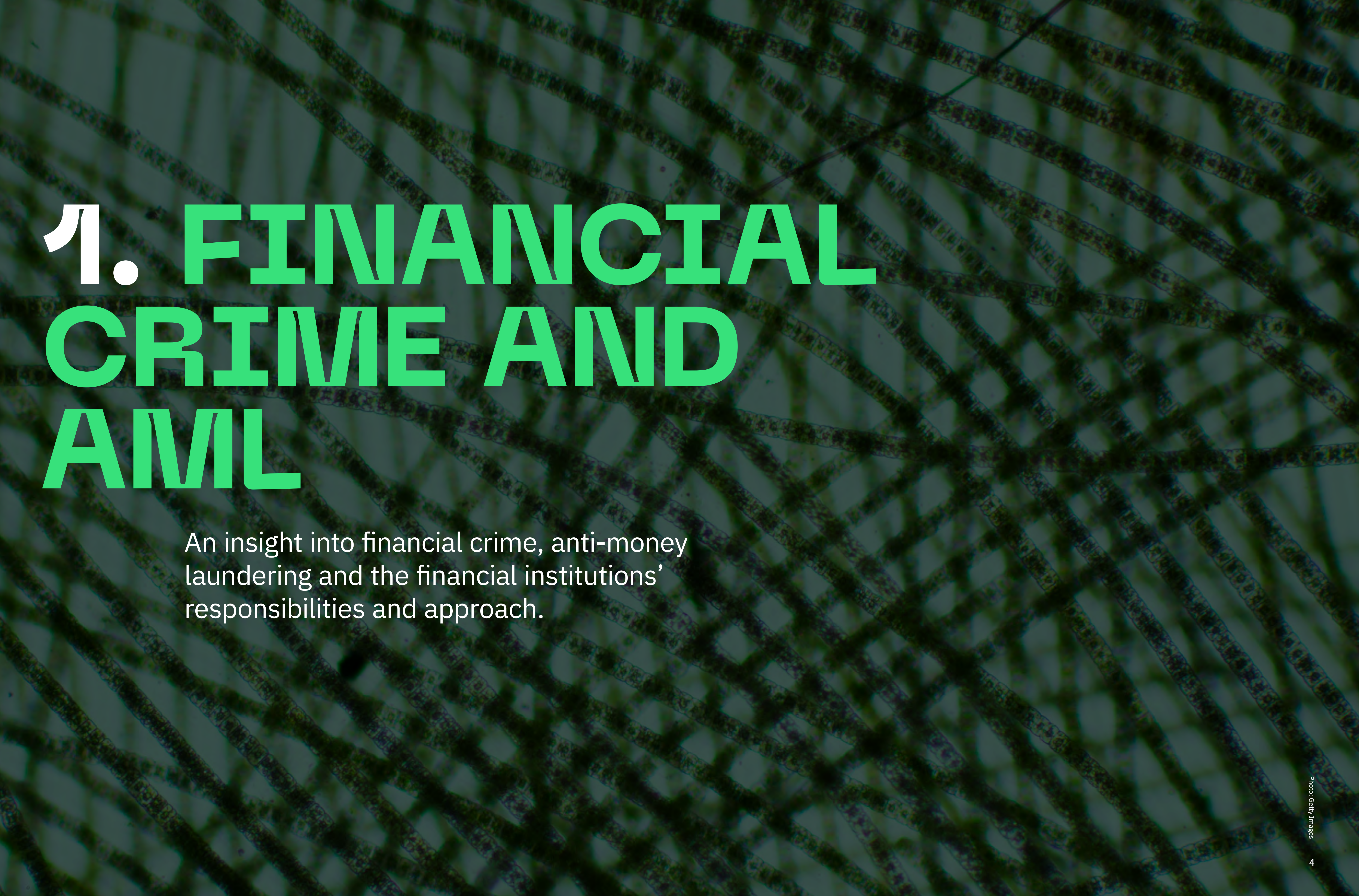
99%

of AML transaction generated alerts are false positives.

See page 19

Transaction monitoring is the area in which Nordic banks recieve the most criticsm.

See page 12



# 1. FINANCIAL CRIME AND AML

An insight into financial crime, anti-money laundering and the financial institutions' responsibilities and approach.

Photo: Getty Images

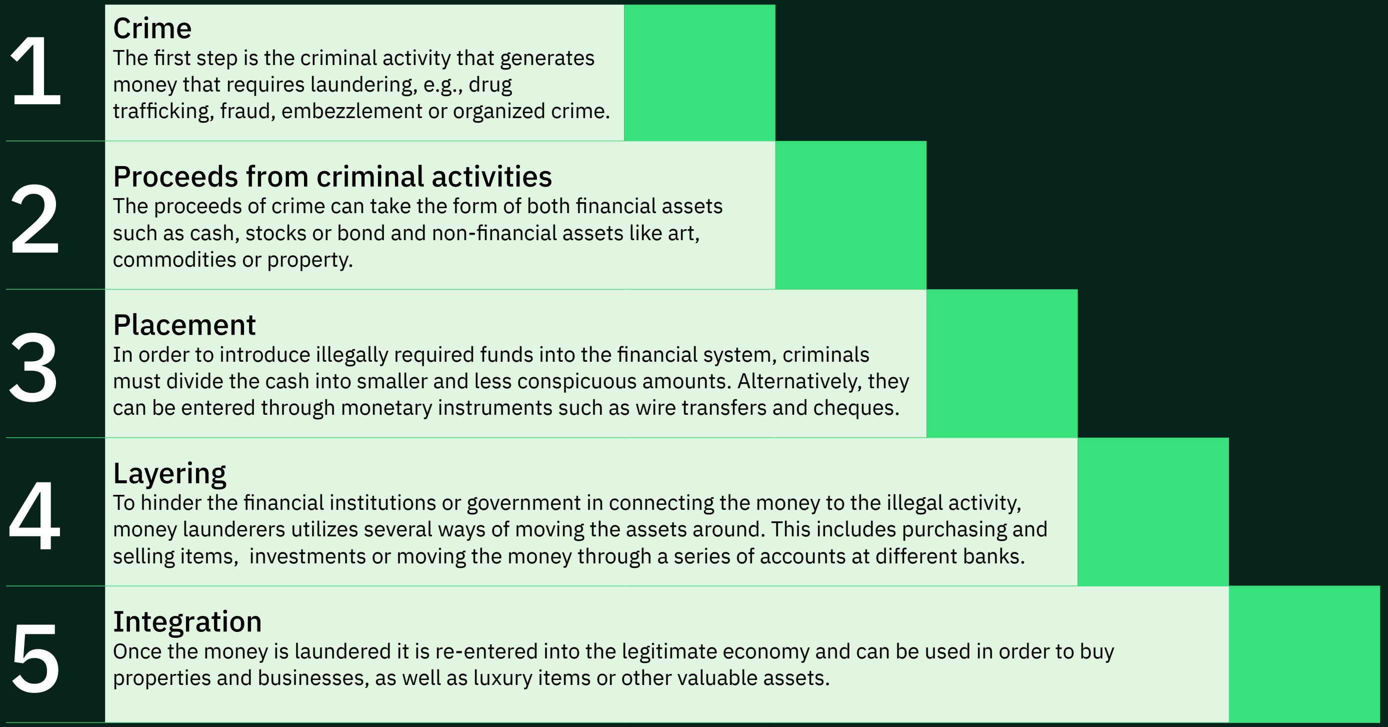
# AML in short

/ The term anti-money laundering (AML) refers to the laws, regulations, procedures and processes meant to detect money that stem from illegal activities and stop it from being concealed as legally obtained funds.

/ AML efforts are an important step in deterring crime by making it more difficult to spend funds that have been acquired through illegitimate actions.

/ In light of the increased focus on terrorism in the early 2000s both US and European AML regulations have specified that the regulations also aims at stopping money going to terrorist organizations.

According to the United Nations, criminals are laundering between $1.6 to $4 trillion (between 2 to 5% of global GDP) annually.



1 **Crime**
The first step is the criminal activity that generates money that requires laundering, e.g., drug trafficking, fraud, embezzlement or organized crime.

2 **Proceeds from criminal activities**
The proceeds of crime can take the form of both financial assets such as cash, stocks or bond and non-financial assets like art, commodities or property.

3 **Placement**
In order to introduce illegally required funds into the financial system, criminals must divide the cash into smaller and less conspicuous amounts. Alternatively, they can be entered through monetary instruments such as wire transfers and cheques.

4 **Layering**
To hinder the financial institutions or government in connecting the money to the illegal activity, money launderers utilizes several ways of moving the assets around. This includes purchasing and selling items,  investments or moving the money through a series of accounts at different banks.

5 **Integration**
Once the money is laundered it is re-entered into the legitimate economy and can be used in order to buy properties and businesses, as well as luxury items or other valuable assets.

# New regulations and higher risks

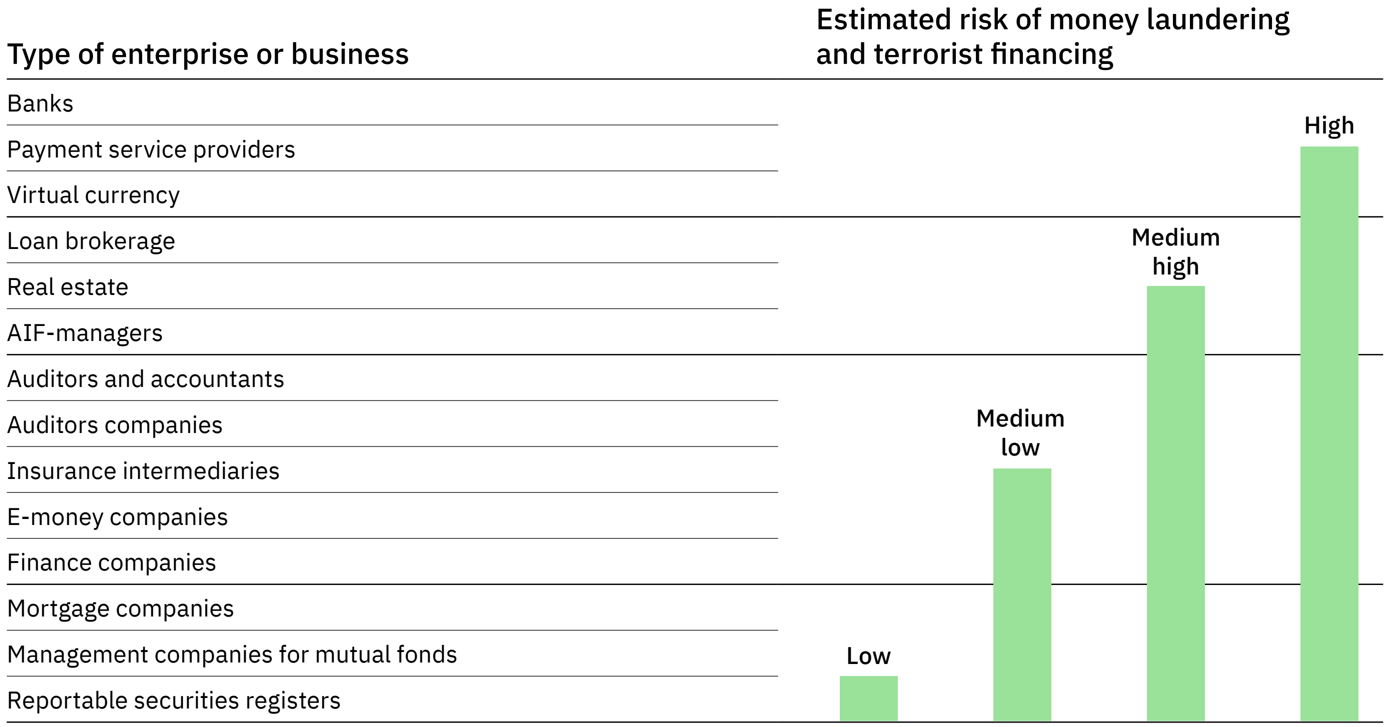
All Nordic countries have implemented the European Union's AML regulations based on recommendations from the Financial Action Task Force. These regulations state that all financial institutions are responsible in detecting and preventing financial crimes.

The banks, being a mediator of millions of daily transactions, are given the responsibility of several AML tasks leading to a massive rise in both personnel working in their financial crimes divisions and the investments in systems designed to prevent money laundering and terror financing.

The sixth AML directive from the European Union, which was implemented in June 2021, included new regulatory changes aimed to extend the criminal liability to legal persons.

Effectively, this allows for harsher punishments for companies that fail to recognize money laundering within their operations. Corporations can now face strict sanctions if any employee within the organization commits an offence that benefit the company.

The latest directive also increases the potential penalties for individuals, demanding that their member states raises the maximum sentence from one to four years when caught money laundering.

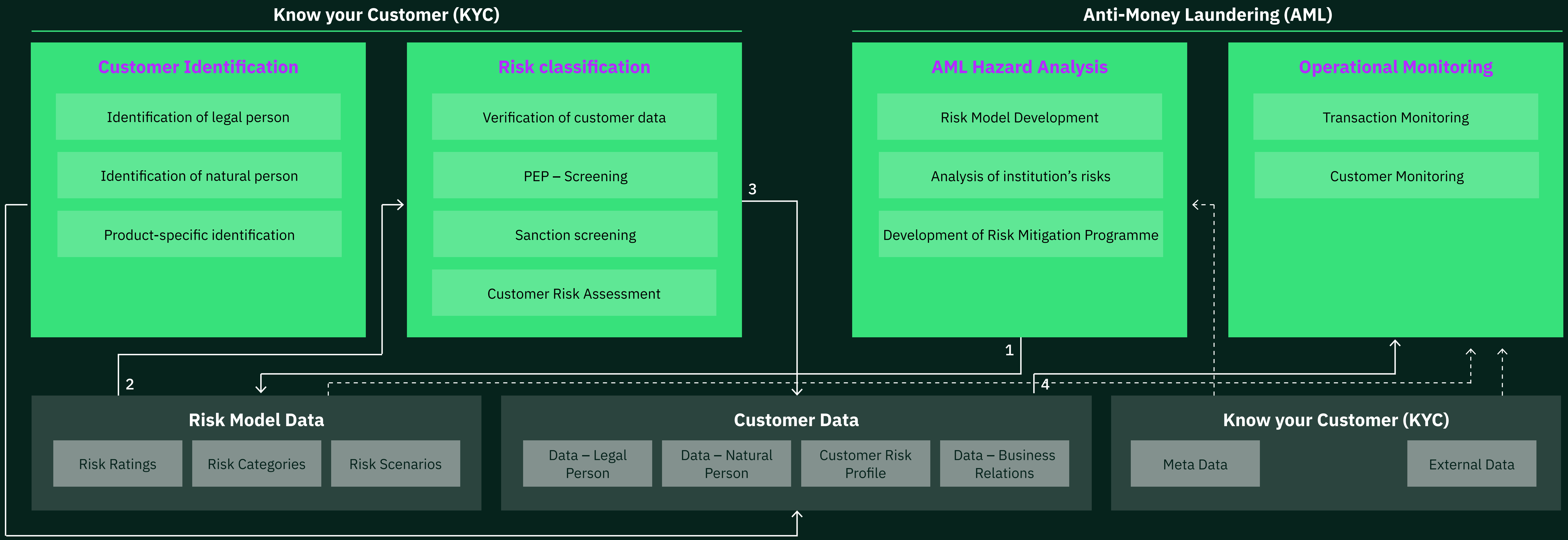


| Type of enterprise or business | Estimated risk of money laundering and terrorist financing |
|---|---|
| Banks | High |
| Payment service providers | High |
| Virtual currency | High |
| Loan brokerage | Medium high |
| Real estate | Medium high |
| AIF-managers | Medium high |
| Auditors and accountants | Medium low |
| Auditors companies | Medium low |
| Insurance intermediaries | Medium low |
| E-money companies | Medium low |
| Finance companies | Medium low |
| Mortgage companies | Low |
| Management companies for mutual fonds | Low |
| Reportable securities registers | Low |

Source: Risikovurdering – hvitvasking og terrorfinansiering (Finanstilsynet, 2019). The risk categories are applicable for Norway.

# KYC is the foundation of succesful AML

While the terms KYC and AML have a tendency of being interchanged, it is necessary to understand the difference. While KYC is an important aspect in money laundering prevention, it is often separated from the AML tasks in financial institutions. Still, without sufficient knowledge of the customers and users, most review- or monitoring processes are doomed. KYC should therefore be regarded as the foundation of good anti-money laundering. The model below show how the different aspects of KYC and AML affect each other with the highlighted lines showing the main processes in the financial institutions' AML efforts.



**Know your Customer (KYC)**

**Customer Identification**
- Identification of legal person
- Identification of natural person
- Product-specific identification

**Risk classification**
- Verification of customer data
- PEP – Screening
- Sanction screening
- Customer Risk Assessment

**Anti-Money Laundering (AML)**

**AML Hazard Analysis**
- Risk Model Development
- Analysis of institution's risks
- Development of Risk Mitigation Programme

**Operational Monitoring**
- Transaction Monitoring
- Customer Monitoring

**Risk Model Data**
- Risk Ratings
- Risk Categories
- Risk Scenarios

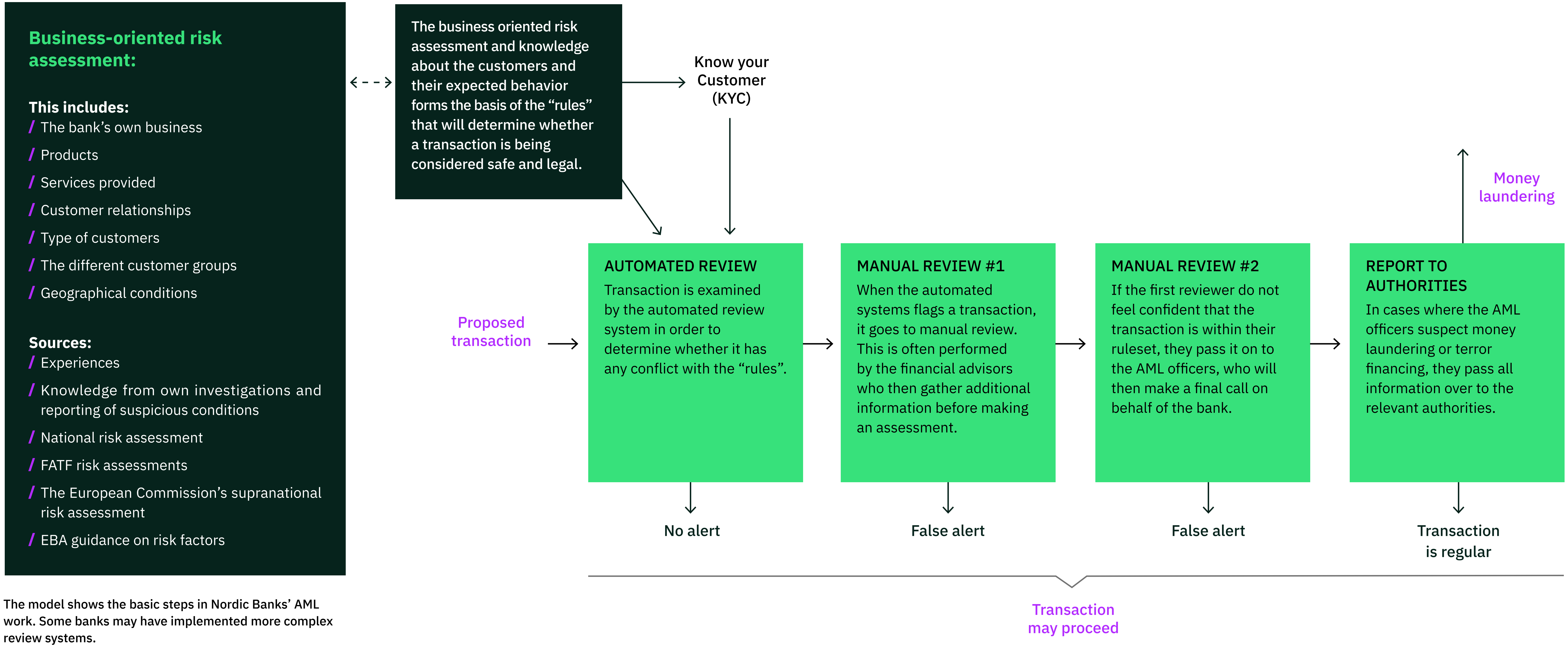
**Customer Data**
- Data – Legal Person
- Data – Natural Person
- Customer Risk Profile
- Data – Business Relations

**Know your Customer (KYC)**
- Meta Data
- External Data

The model show how the different aspects of KYC and AML affect each other – with the highlighted lines showing the main processes in the setup of financial institutions' AML efforts. The dotted lines show where relevant data in the different categories stem from.

# Transaction monitoring is key

Most financial institutions' effort to prevent money laundering is highly focused on transaction monitoring and identifying suspicious activity when money is transferred between accounts. This model explains the transaction process from an AML-standpoint and the different processes that are involved in uncovering assets from illegal activities or money financing terrorism. As shown, the set-up and data input of the automated review systems are essential and determines to what degree criminal activities are discovered and money laundering is prevented.



**Business-oriented risk assessment:**

**This includes:**

- / The bank's own business
- / Products
- / Services provided
- / Customer relationships
- / Type of customers
- / The different customer groups
- / Geographical conditions

**Sources:**

- / Experiences
- / Knowledge from own investigations and reporting of suspicious conditions
- / National risk assessment
- / FATF risk assessments
- / The European Commission's supranational risk assessment
- / EBA guidance on risk factors

The business oriented risk assessment and knowledge about the customers and their expected behavior forms the basis of the "rules" that will determine whether a transaction is being considered safe and legal.

**AUTOMATED REVIEW**
Transaction is examined by the automated review system in order to determine whether it has any conflict with the "rules".

**MANUAL REVIEW #1**
When the automated systems flags a transaction, it goes to manual review. This is often performed by the financial advisors who then gather additional information before making an assessment.

**MANUAL REVIEW #2**
If the first reviewer do not feel confident that the transaction is within their ruleset, they pass it on to the AML officers, who will then make a final call on behalf of the bank.

**REPORT TO AUTHORITIES**
In cases where the AML officers suspect money laundering or terror financing, they pass all information over to the relevant authorities.

The model shows the basic steps in Nordic Banks' AML work. Some banks may have implemented more complex review systems.

# Change in four driving areas within AML

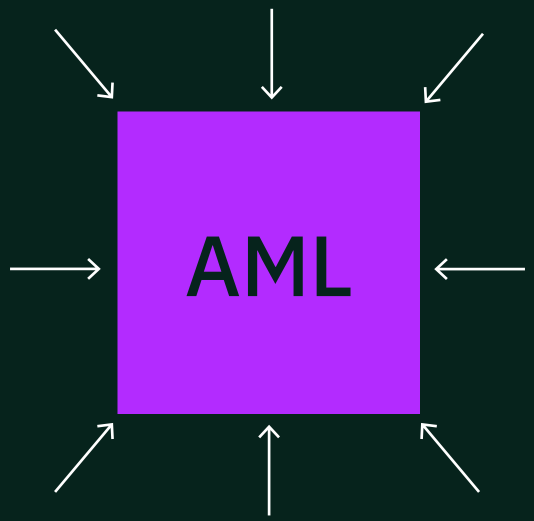
There are four key components driving the approaches and methods utilized in fighting modern financial crime. Three of the key driving forces attempt to prevent crime, while the final important factor is the progression of the criminals’ tactics.

## Regulatory changes

The regulations that affect AML are changing at a rapidly increasing frequency. Since the EU adopted its first AML legislation in 1991, financial crime have received more and more attention from lawmakers – both regarding who should comply, and the requirements imposed on the financial institutions. The later changes in regulations have introduced more responsibility for both financial institutions and individuals, as well as the threat of stricter punishment.

## Evolving criminal activities

Criminal enterprises have been adapting to their environment since the beginning of time, and the increased focus on financial crime prevention is just the latest barrier. Today’s criminals are not only sophisticated, but many have developed great skills in spotting new opportunities as they arise. The constant evolving threat can feel like a never-ending challenge – every time a new form of illegitimate activity is uncovered, another one is created.



## Technology and automation

The impact of new technology in AML are expected to rocket in the coming years. While it is clear that new technology has had a severe impact already, the emergence and rapid improvement in areas such as artificial intelligence, machine learning and RPA are expected to accelerate the financial institutions’ ability to both discover and prevent criminal activity.

## New service providers

With regulatory changes leading to massive needs for AML assistance, several new and existing companies have launched new ventures. Most offer technology-driven solutions with the purpose of saving the financial institutions money while staying compliant in an everchanging legal environment. The potentially massive payouts for those able to provide significant value incentivize innovation and drives AML further.

# 2. CURRENT STATE OF AML IN THE NORDICS

Key issues Nordic banks are struggling with when it comes to anti-money laundering.

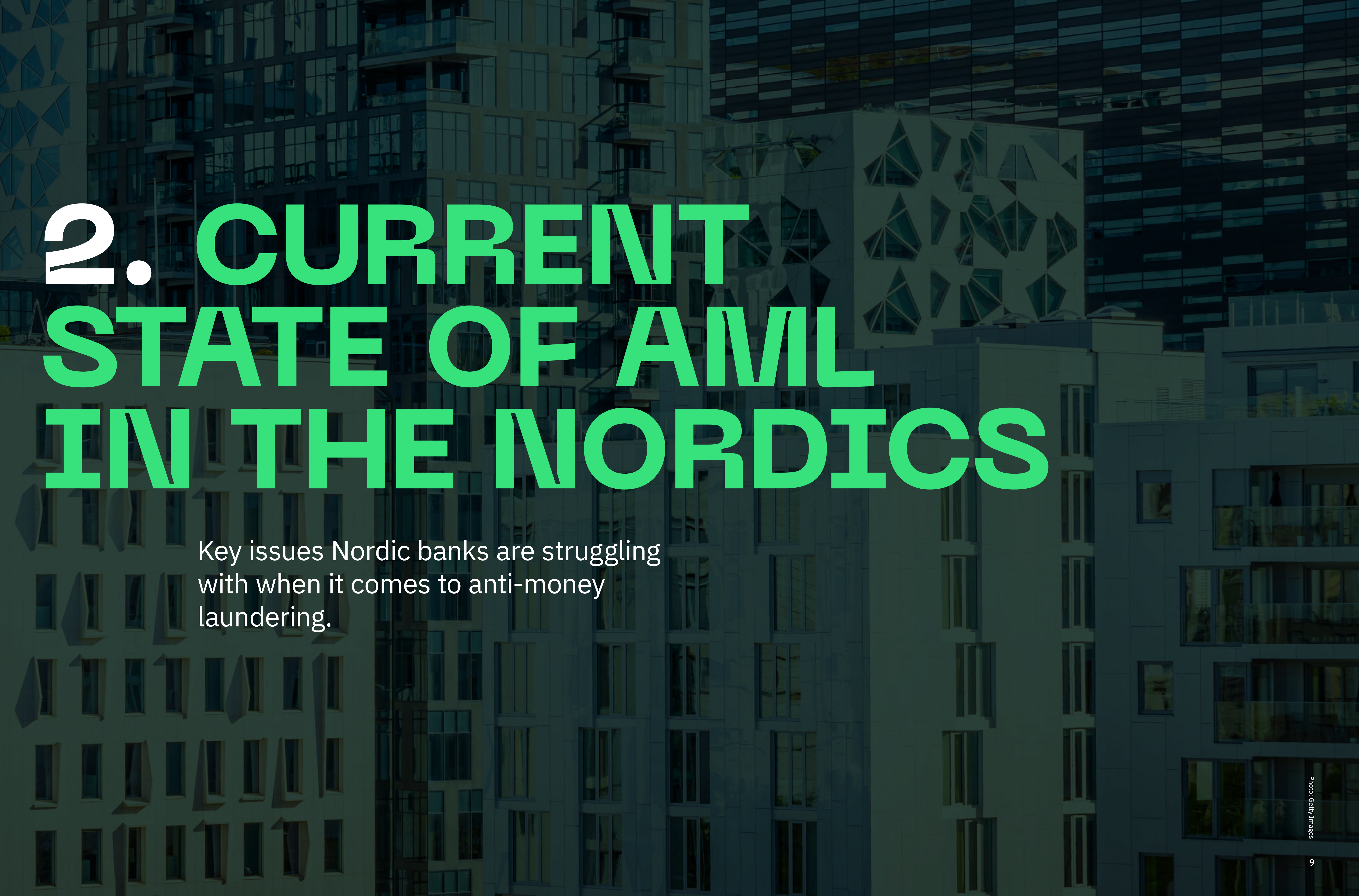


Photo: Getty Images

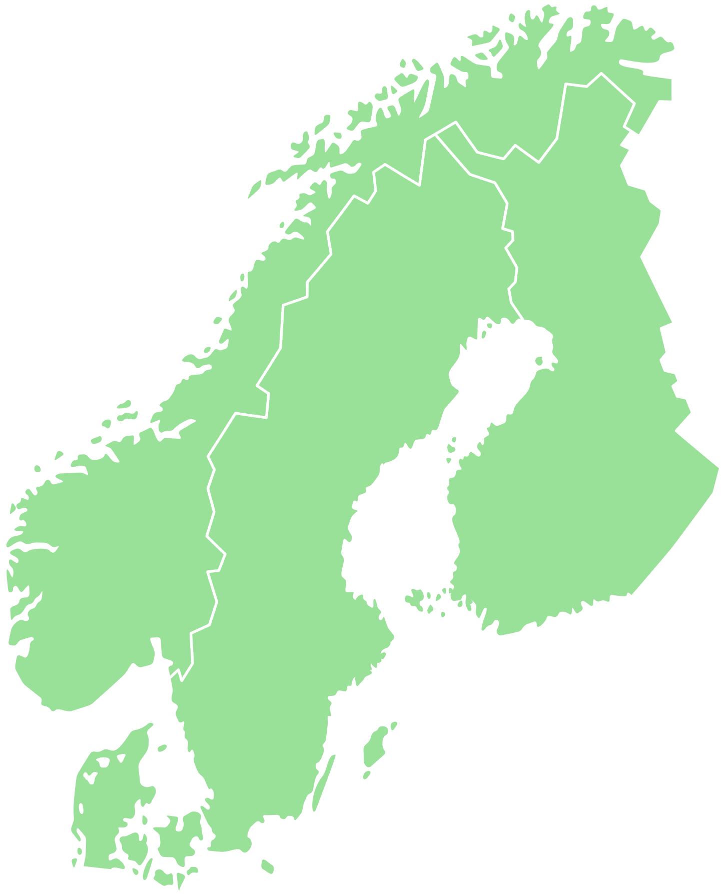
# AML in the Nordics

## A summary

The Nordic banks have already invested heavily in improving their AML effort and becoming compliant under increasingly complex EU anti money-laundering directives regulations.

In addition to staffing up in relevant positions, most financial institutions are working on leveraging innovation and new technology e.g., AI and robotic process automation in order to combat financial crimes.

SEB, Handelsbanken, Swedbank, Nordea, Danske Bank and DNB have introduced Invidem, a collaborative effort in strengthening AML in the region by creating a common KYC utility with data and information sharing across the banks.

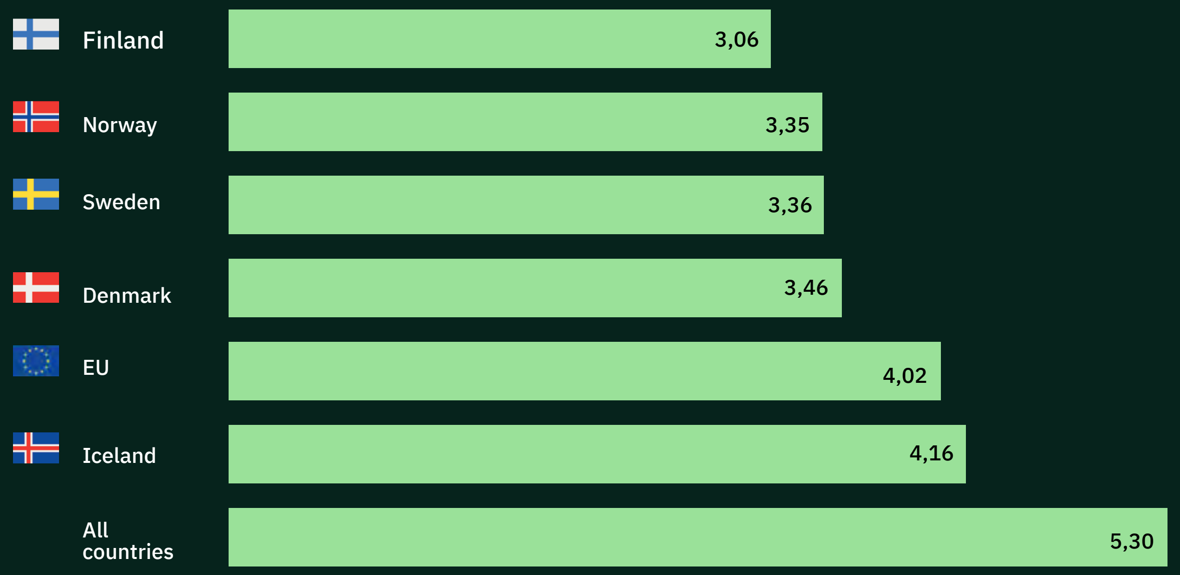


## IMF review due in 2022

The Nordic countries have alongside the Baltic nations asked the International Monetary Fund for an independent review of their AML efforts. The analysis assessing the regional cross-border money laundering and terrorist financing risks was started in January 2021 and is expected to be finalized in the summer of 2022.

# The Nordics are considered low risk

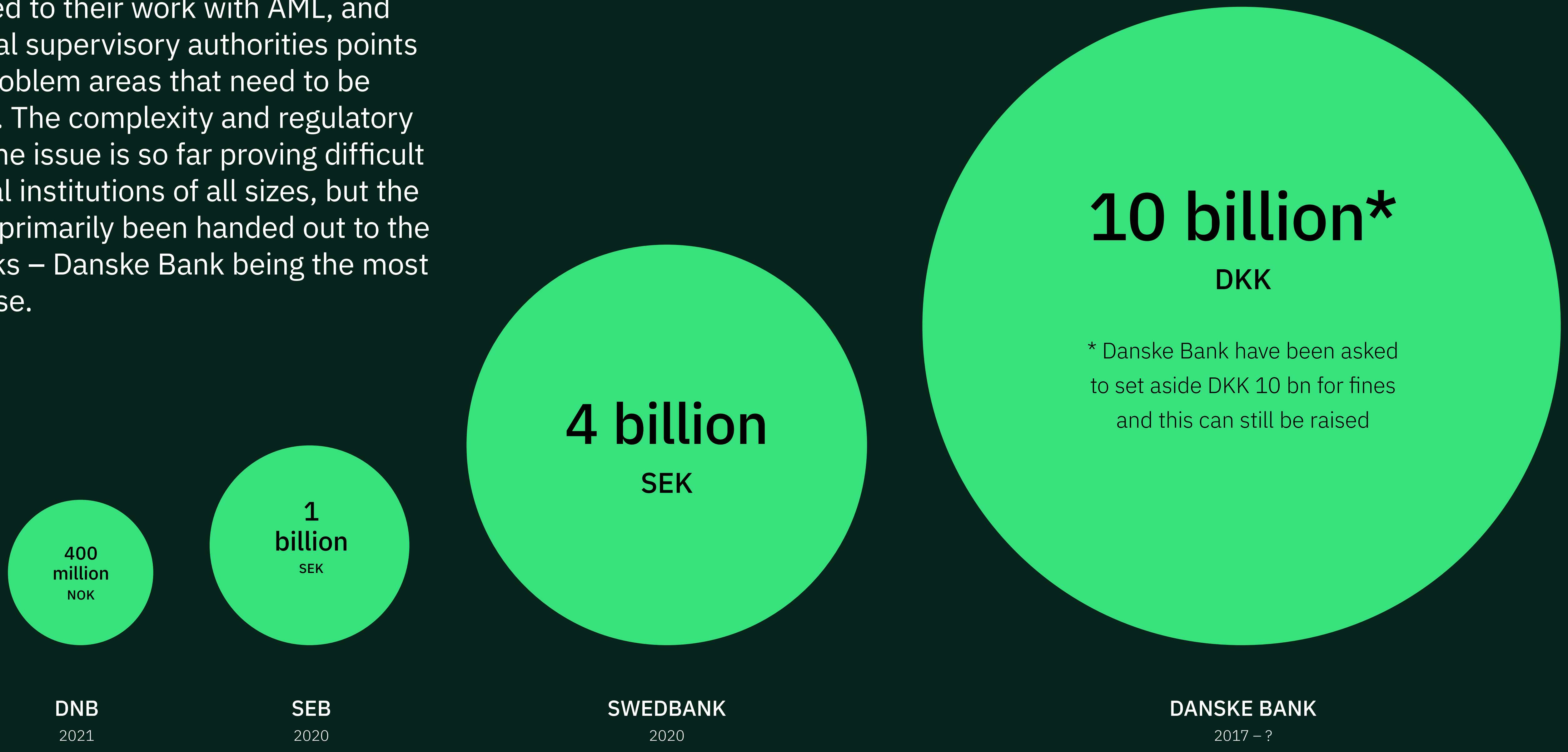
- The Nordic countries are considered among the global leaders in AML – Finland, Norway, Sweden and Denmark are all ranked in the top 8 worldwide in the 2020 Basel AML Index.
- The average Nordic risk score is 3.48, significantly lower than both the European (4.02) and global average (5.30).
- Iceland is an outlier in the Nordics with a much higher risk score than the other nations. The country have received criticism over insufficient mechanisms in place for authorities to coordinate on AML policies and activities.
- Several Nordic banks were heavily scrutinized for their lacking AML efforts following the revelations of the Danske Bank scandal where hundreds of billion Euros was laundered through their Estonian branch over a 9-year period.
- Overall, the index finds that the European region is struggling with the quality of their AML and CFT frameworks, while they have low risk scores related to corruption, transparency and legal and political risks.



The annual Basel AML Index provides risk scores for all nations where there is sufficient data to calculate a reliable AML risk score. They examine data from seventeen publicly available sources and scores the nations based on five areas: quality of AML/TF frameworks, corruption and bribery, financial transparency and standards, public transparency and accountability, and legal and political risks.

# Major fines have been handed out

Several Nordic banks have already received fines related to their work with AML, and the financial supervisory authorities points to many problem areas that need to be addressed. The complexity and regulatory nature of the issue is so far proving difficult for financial institutions of all sizes, but the fines have primarily been handed out to the larger banks – Danske Bank being the most famous case.



* Danske Bank have been asked to set aside DKK 10 bn for fines and this can still be raised

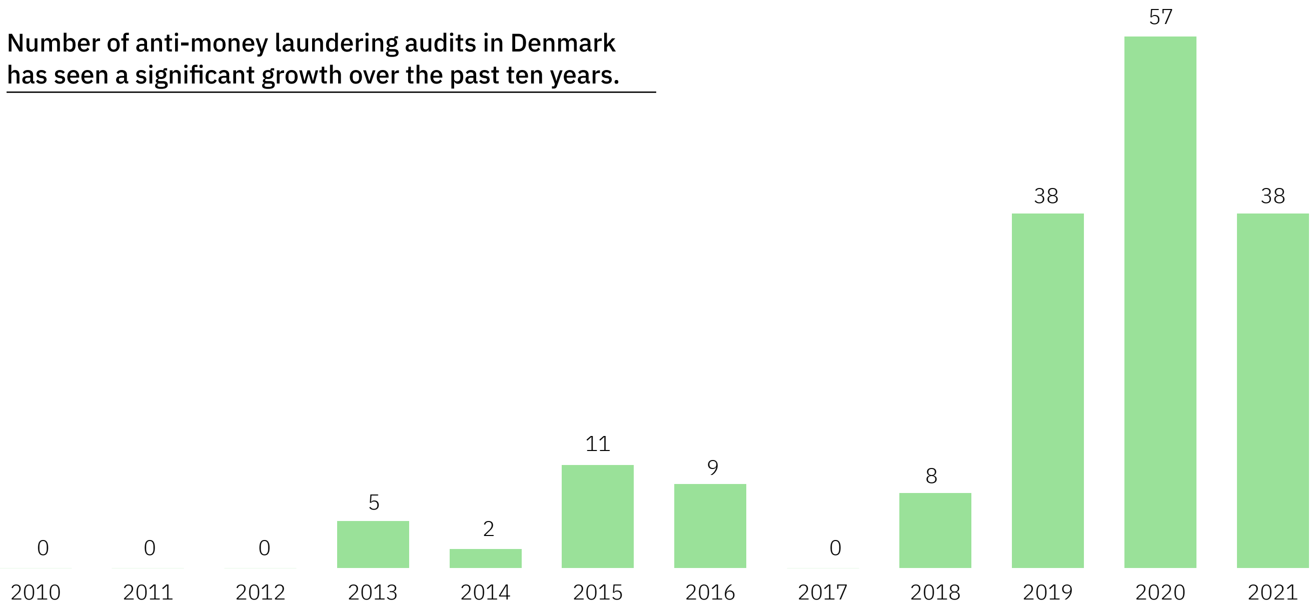
# Increased regulatory demands

The Financial Supervisory Authority in all the Nordic countries have sharply increased their focus and supervisory activity in the anti-money laundering and terrorist financing area in recent years. One motivation for this is attributed to extended sanction options that were authorized by law in 2018. The illustration below shows the number of audits in the money laundering area carried out by the Danish Financial Supervisory Authority since 2010. A similar increase in supervision is also seen in Norway, Sweden and to some extent Finland.

An analysis of all audits in the money laundering area published by the respective countries' financial supervisors, from 1.1.2020 until now, shows that the challenges the Nordic banks face in relation to their work with anti-money laundering and terrorist financing are virtually the same, and the criticism from audits in all four countries comes in all areas throughout the process. The supervisory reports show that several of the banks have had consistent and extensive shortcomings in compliance with money laundering regulations over many years.

The shortcomings are general, from obtaining basic information, understanding who the customer is, following up on the ongoing customer relationship, handling transaction alarms, to examining and reporting these. The analysis also shows fundamental shortcomings in the understanding of risk and the ability to see different customers in the same group in context. Lack of understanding of risk combined with inadequate information gathering means that a decisive basis for complying with the obligations in the money laundering regulations cannot be met.

**Number of anti-money laundering audits in Denmark has seen a significant growth over the past ten years.**

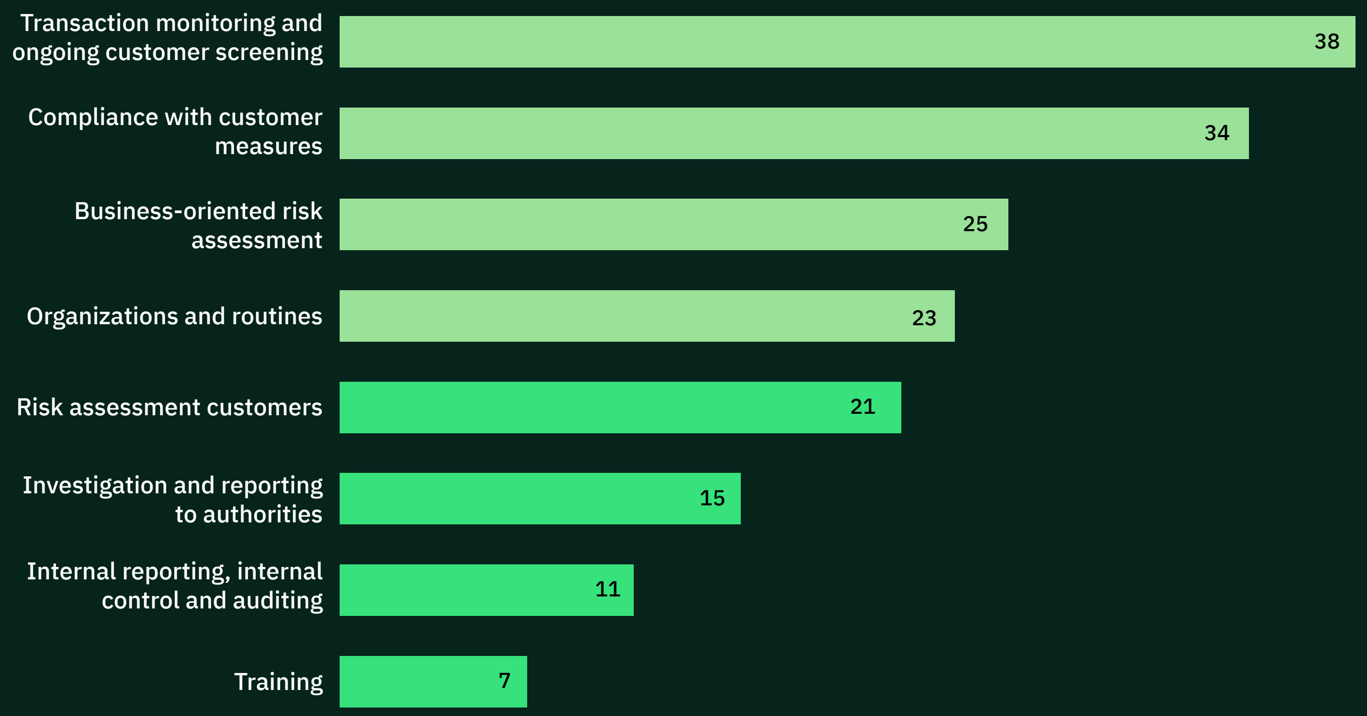


**The number of audits in 2021 are updated as of October 2021**

Source: Finanstilsynet.dk

# Transaction monitoring is a key challenge

**Based on 44 AML audits in the Nordic countries since January 1st 2020, these are the areas where banks receive most criticism.**



The graph show how many banks that have received criticism per area based on 44 audits.

Source: Itera analysis

## AML audits in the Nordics

# Areas where banks are struggling

We have analyzed all public AML audits and reports from the financial authorities in Norway, Denmark, Sweden and Finland since January 1st, 2020. Our analysis concludes with four areas with high degree of criticism, where especially transaction monitoring and ongoing customer screening and compliance with customer measures are areas where most banks receive critique from their national financial authority.

**High degree of critic**

### Organization and routines

- Unclear responsibilities
- Inadequate definition of roles
- Lack of authority to AML manager
- Routines not sufficient operational
- Routines not in accordance with the company's actual risk

### Compliance with customer measures

- Consistent shortcomings in documentation
- No coincidence between customer declaration and transactions
- Difficult to see and understand the result of various measures
- Documentation in different systems, different access, advisor does not have a full overview, leads to assessment- and follow-up errors

### Business-oriented risk assessment

- No sufficiently obvious correlation with actual company risk
- Too general description of risks
- Leads to consequential errors in the rest of the compliance work
- Terrorist financing does not have its own risk assessment

### Transaction monitoring and ongoing screening

- The rules of the monitoring system are too general and not customer-specific
- Does not include obtained customer information in the monitoring
- Alarms often at riskclass level and not customer specific
- Defined threshold values and rules inaccurate
- Poor accuracy of alarms
- Not sufficient ongoing screening of changes in customer relationships or behaviour

**Medium-high degree of critic**

### Risk assessment customers

- Specific risk at the individual level is not captured by systems
- Inadequate documentation
- Information obtained by customers is not taken into account
- Obvious risk invoices omitted in the assessment
- Major weaknesses in electronic risk classification

### Training

- Poorly adapted to own business
- No specific requirements for self-study
- Weakly concretized requirement and varying quality of electronic training
- Deficiencies in the training of the board
- Poorly documented

### Investigation and reporting to authorities

- Documentation is stored in too many different systems
- No comprehensive overview
- Alarms are closed manually without documentation
- Lacks a system that ensures that alarms are followed up and ensures accountability
- Significant improvement potential on TM reporting to Authorities

### Internal reporting, internal control and auditing

- Weak line controls
- Findings not well enough followed up
- Findings not sufficiency documented
- Lack of control over the quality of information obtained

# 3. THE NEXT GENERATION OF AML

How AI and smarter use of data can enable banks to further prevent money laundering in the future.

Photo: Getty Images

# AML 2.0

## The transformation vision towards next generation AML

> “The the next generation of AML focus on identifying financial criminals rather than financial crimes.”

Illustration photo / Getty Images

AML 2.0 leverages new techniques and an integrated approach to merge Customer Life Cycle Management (CLM) and Client Activity Monitoring (CAM) processes and data into a seamless identification of risk and mitigation by focusing on continuous, holistic reviews of customer activity.

| FROM WHO CUSTOMERS ARE ... | TO WHAT CUSTOMERS DO |
|---|---|
| Siloed KYC and TM approaches provide only a partial view of customer risk | Converge CLM and CAM to focus on **customer risk and behavioral changes** |
| Risk rating on static factors inefficiently predicts risk and increases due diligence | Use shared data to understand context and risk, maintain dynamic **profiles** and **reduce duplicative activities** |
| Excessive focus on the noise, not the signal results in unproductive alert volume | Evaluate activity across institutions to focus on **high-value analysis** and report **truly risk activity and bad actors** |

Focus on ongoing entity risk rather than individual transactional risk

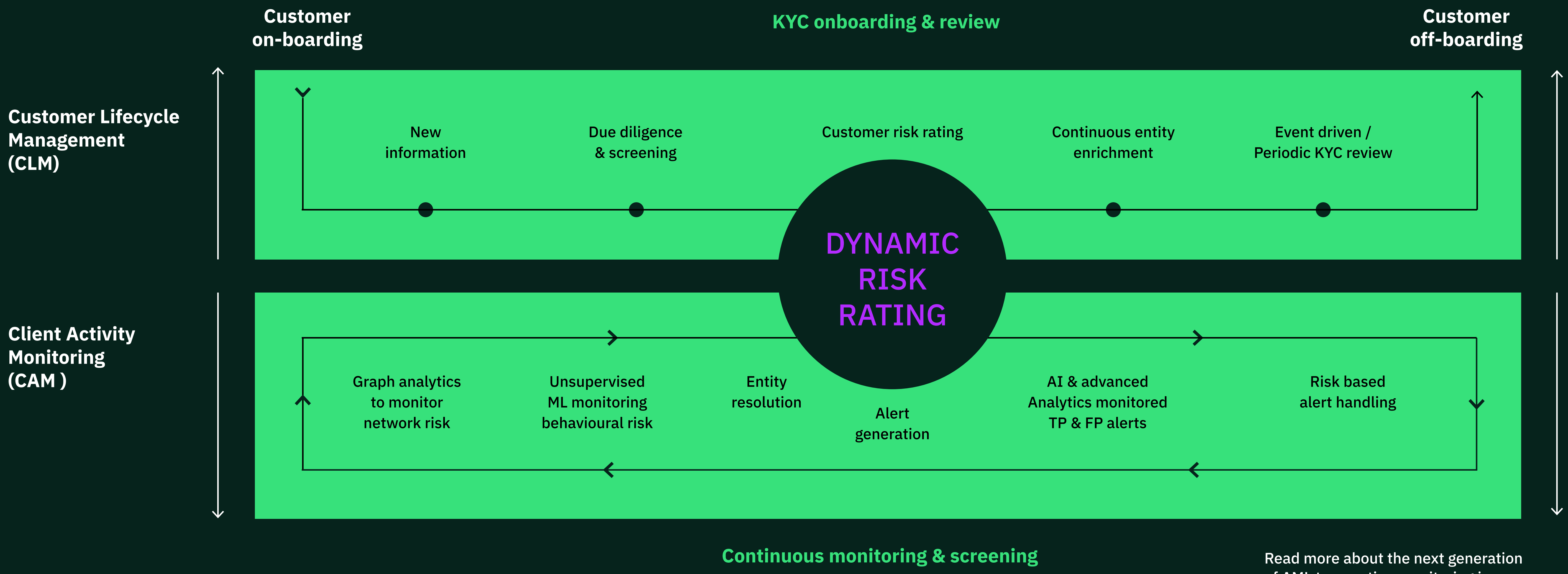
# Continuous KYC and monitoring becomes a strategic value driver

**The key technology pillars of a bank's attempts to detect suspicious criminal flows are Customer Lifecycle Management (CLM) and Customer Activity Monitoring (CAM).**

CLM typically consists of activities such as customer onboarding, customer due diligence, customer risk rating, enhanced due diligence and periodic review. CAMrefers primarily to AML Transaction Monitoring, and Transaction List screening for international payments.

Typically, when a client transaction is executed on an FI's core banking system, the transaction will be inspected on a secondary system, the AML Transaction Monitoring system, to identify whether a transaction is likely to be part of a money laundering attempt. The AML TM system executes a set of rules or scenarios (compound rules) which are applied to the transaction. If any of the conditions in these rule sets are satisfied then the transaction is deemed suspicious, an AML alert is created and routed for processing by a human.

If the human agrees with the AML alert created by the AML TM system, a Suspicious Activity Report (SAR) is generated and sent to law enforcement. However, experience shows that these systems, which are required by financial regulators in every jurisdiction, generate vast numbers of false positives (all of which must be remediated by people) and fail to identify suspicious transactions with any degree of consistency.


Customer on-boarding
KYC onboarding & review
Customer off-boarding
Customer Lifecycle Management (CLM)
New information
Due diligence & screening
Customer risk rating
Continuous entity enrichment
Event driven / Periodic KYC review
DYNAMIC RISK RATING
Client Activity Monitoring (CAM )
Graph analytics to monitor network risk
Unsupervised ML monitoring behavioural risk
Entity resolution
Alert generation
AI & advanced Analytics monitored TP & FP alerts
Risk based alert handling
Continuous monitoring & screening

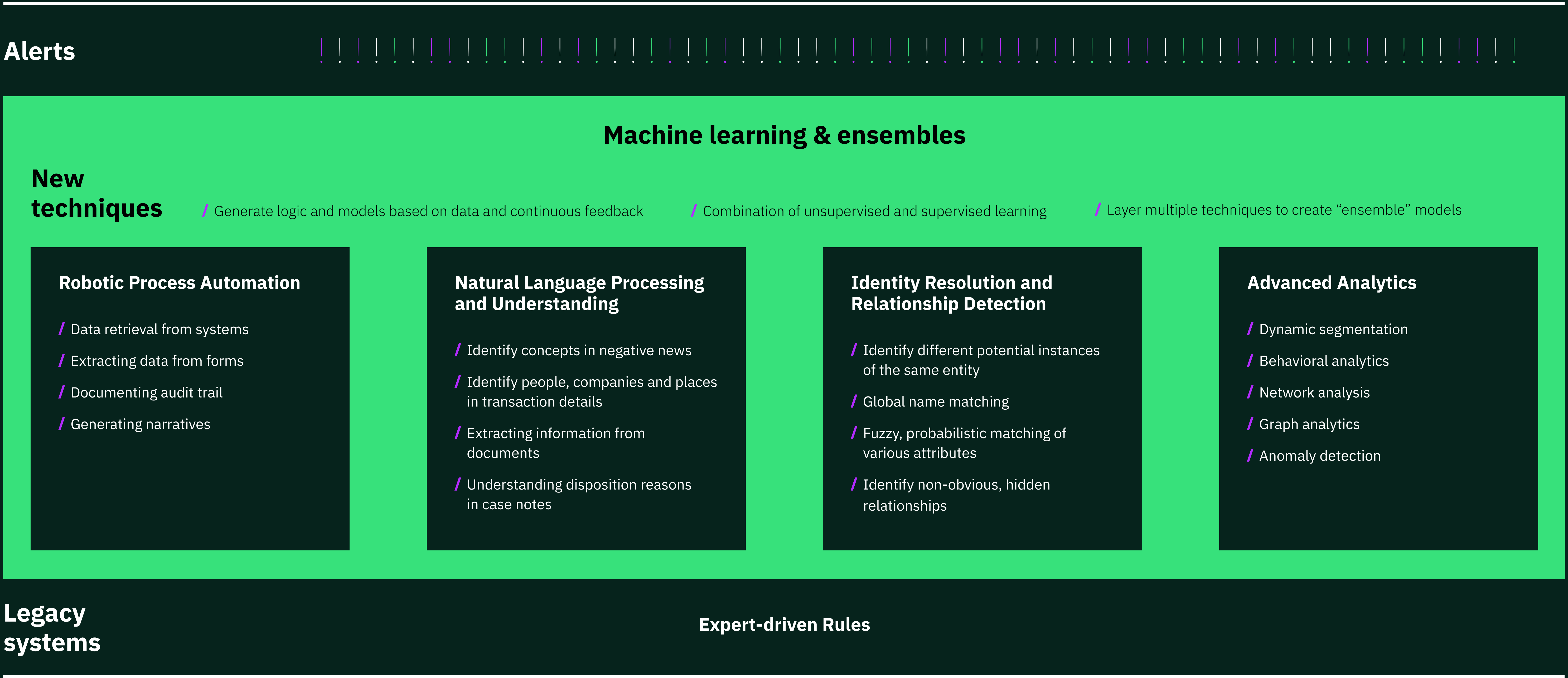
Read more about the next generation of AML transaction monitoring in Paul Clandillon's POV on page 20 →

> "Our experience show that it can take up to nine months to introduce new rules and scenarios to address emerging threats."

**IBM** & **Iteras experience**

# Transforming AML by enabling data and technology

Currently financial institutions rely heavily on human involvement in labour-intensive, manual compliance processes. Legacy systems often have low efficiency levels and imprecise models for detecting criminal activity. In some cases 99 per cent of generated alarms are false positives, in IBM and Itera's experience.
The combination of new techniques such as machine learning, advanced analytics and automation represents opportunity to to gain greater insight, make better decisions and reduce time and costs.



## Alerts

## Machine learning & ensembles

### New techniques

- / Generate logic and models based on data and continuous feedback
- / Combination of unsupervised and supervised learning
- / Layer multiple techniques to create "ensemble" models

### Robotic Process Automation

- / Data retrieval from systems
- / Extracting data from forms
- / Documenting audit trail
- / Generating narratives

### Natural Language Processing and Understanding

- / Identify concepts in negative news
- / Identify people, companies and places in transaction details
- / Extracting information from documents
- / Understanding disposition reasons in case notes

### Identity Resolution and Relationship Detection

- / Identify different potential instances of the same entity
- / Global name matching
- / Fuzzy, probabilistic matching of various attributes
- / Identify non-obvious, hidden relationships

### Advanced Analytics

- / Dynamic segmentation
- / Behavioral analytics
- / Network analysis
- / Graph analytics
- / Anomaly detection

### Legacy systems

**Expert-driven Rules**

> “Our experience show that up to 99 per cent of AML transaction generated alerts are false positives.”

**IBM** & **Iteras experience**

*Point of View:*

# Improving efficiency and effectiveness of current generation of AML transaction monitoring solutions

/ **Paul Clandillon**
Practice leader financial crime, IBM

> “We need to change our focus from just looking at individual transactions, to including a perspective on the overall behavior.”
>
> *Paul Clandillon* / IBM

**Banks face two problems in seeking to prevent money laundering. The first is one of efficiency and the challenge to reduce the escalating costs of AML alert handling, and the second is one of effectiveness and the need to identify suspicious actors who are not being detected by the current AML TM systems.**

To improve both the efficiency and effectiveness of AML TM, we need first to start by changing our focus from just looking at individual transactions and start to include a perspective on the overall behavior of the entity involved in these transactions and the risk that they are engaged in money laundering. Understanding the context and intent of a single financial transaction is almost impossible without further insight.

An understanding of the overall behavior and likely risk posed by the entity conducting the transaction gives us an insight into context and intent and enables more informed decision making about whether an AML TM alert is likely to be a true or false positive.

If we see an AML alert on an entity whose behavior we have identified to this point as low risk then we will be more likely to dispose of the alert. Similarly, an alert on a high-risk entity will garner more focus then might previously have beenthe case.

Of course, banks attempt to do exactly this, and assign a customer risk rating to each customer, when they are onboarded. Based on a variety of demographic factors such as where a potential client is based, the business they are in, their source of wealth etc. the bank assesses the risk that the customer will engage in money laundering. The result of this demographic assessment whether the client will be regarded and treated as a “high”, “medium” or “low” risk for financial crime. These categories will set the thresholds to be applied by the rules and scenarios used by the AML TM system to identify suspicious transactions. Thus, a customer who is rated high risk will typically generate high rates of AML alerts.

A new perspective, which I call dynamic disk rating (DRR), can be derived from continuous behavioral monitoring of clients. DRR is a factor derived from several different observations of customer behavior.

→

→

The first of these is entity complexity. It is observably true that more complex entities (those with many different accounts and varying identities) pose higher risks of financial crime. AML alerts and suspicious activity reports (SAR) increase with growing entity complexity. Continuous entity resolution across the client base will yield an index of entity complexity which can be used as an input to the ultimate calculation of dynamic risk rating for each entity.

The second key technique is dynamic segmentation. Using unsupervised machinelearning techniques, we can cluster entities around many derived behavioral features. Each of these clusters represent groups of entities which behave in similar ways. As we know the names of the entities in each segment it's possible, based on the past behavior of this group of customers in terms of the number of AML TM alerts and SARs created, to assign a behavioral risk factor which is included in the calculation of the dynamic risk rating.

The final element is risk by association. Using modern graph analytic techniques, it is possible to examine, using graph machine learning queries, the pattern of interaction of a particular entity. If the entity is doing business with other high-risk entities, then they are inclined to have an elevated risk.

Continuously calculating a dynamic risk rating based on these three inputs and combining them, using ensemble machine learning models, with the CRR calculated at onboarding time enables a much more accurate view of the true risk of financial crime posed by each entity within the customer landscape.

## Improving the efficiency

In most cases it is probably unreasonable to seek to replace current AML TM solutions. These are regulated systems and, although the regulator in many jurisdictions have been open to the application of new technologies and techniques, an evolutionary rather than revolutionary approach will be required.

A bank can use a dynamic risk rating calculated as described as a very effective tool to triage false positives alerts and to identify likely true positives for accelerated handling. As part of a non-intrusive triage layer, transparent to current AML TM solution, the dynamic risk rating can be combined with several other AI techniques, such as supervised machine learning and AI generated high value rules, to automatically reduce the number of false positives generated by the system. An alert triage layer of this type, when combined with an optimized target operating model for alert handling, should reduce in a dramatic reduction in the amount of human interaction and consequently cost required to manage current alert volumes. Many banks which have successfully implemented these types of techniques have seen 30 – 70 percent workload reductions.

## Improving the effectiveness

In the past, banks have segmented their clients into a small number of risk categories, typically “high”, “medium”, or “low”, because of the difficulty of managing many different segments and tuning thresholds appropriate to all these segments. However, big data and AI techniques allow us to manage many different segments, clustered across many different axes, which allows a more fine-grained distribution of risk across the segments. In addition, most customer risk ratings never change once they have been assigned at onboarding time. The hyper segmentation approach described here allows for the continuous, dynamic, re-segmentation of customers based on their current, not just their past, behavior, allowing us to proactively identify new risks as they emerge. If, for example, we observe that a particular customer has conducted some transactions that have caused them to be moved to a new and higher risk segment, then we might choose to surface that customer to the financial intelligence unit for a deeper investigation of their behavior. As a bank we then start to get a proactive insight into emerging financial crime risk before any AML alerts have even been created for that customer.

In addition, we can feed updated financial crime risk information derived from a combination of CRR and dynamic risk rating back to the customer activity monitoring (KYC). Typically, in current KYC systems, the financial crime risk rating assigned at onboarding is used to identify customers who require deeper investigation prior to onboarding (enhanced due diligence) and to schedule periodic reviews for higher risk customers. A high risk customer might require a scheduled review every six months and enhanced due diligence checks, while a lower risk customer might be reviewed every year or even every two or three years. If our identification of high risk customers is not accurate we can end up doing large numbers of complex and costly reviews on customers who pose no significant risk of financial crime. By refreshing the customer risk rating provided at onboarding with the behavioral insights provided by a dynamically generated risk rating we can ensure we spend less time on less risky customers and focus our resources where the real threats lie.

“Many banks which have successfully implemented these types of techniques have seen 30–70 per cent workload reductions.”

Paul Clandillon / IBM

Case study I

# PAYMENT FRAUD PREVENTION AT A NATIONAL PAYMENT SWITCH

An inter-banking company, helps banks combat fraud using IBM Safer Payments.

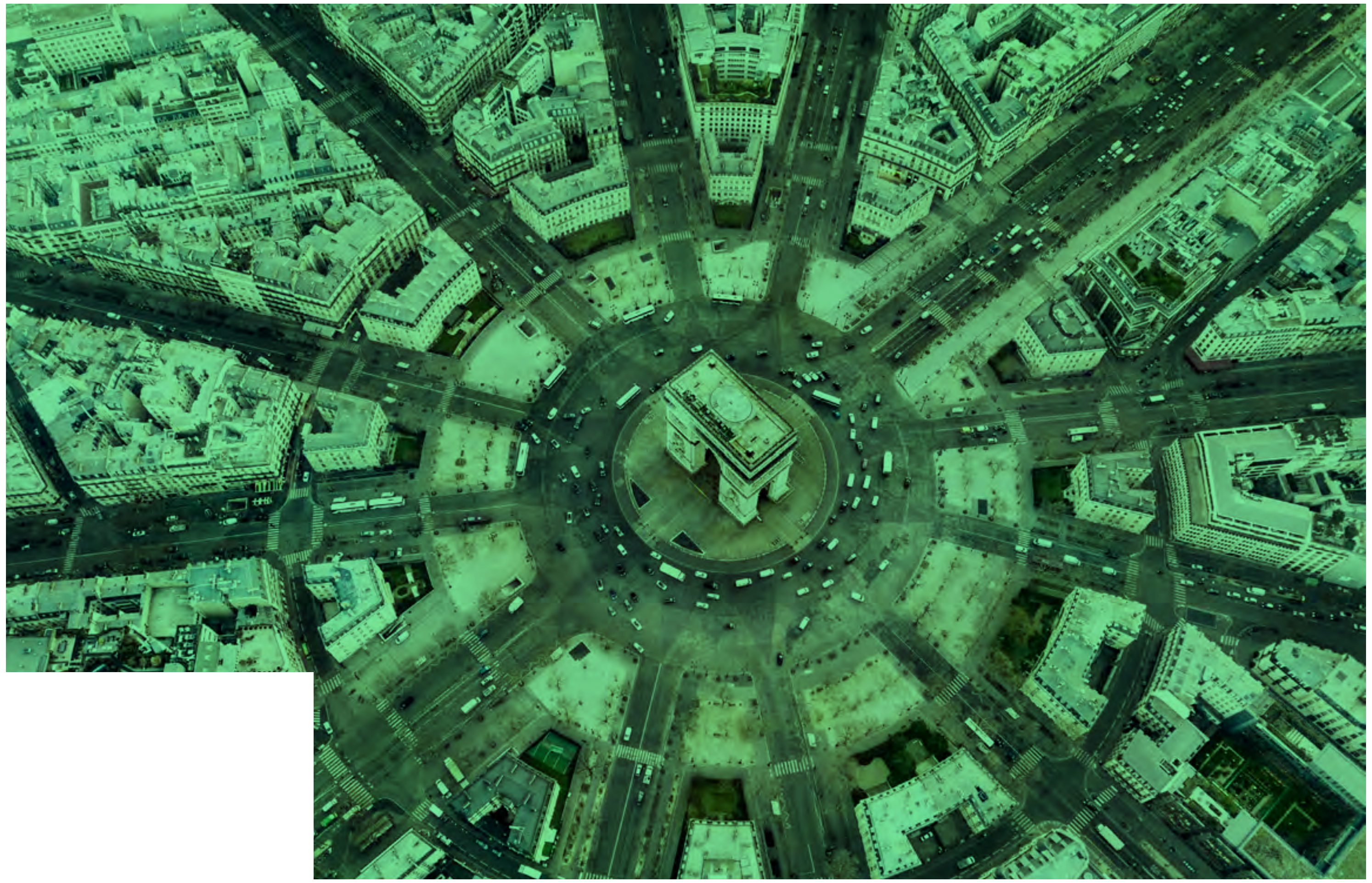


Illustration photo / Getty Images

stet

## Facts

STET is a major European Automated Clearing House servicing the payment industry and providing processing services for SEPA and domestic instruments. STET provides a fully secure and flexible platform, supporting the specificities of the European markets and delivering efficiencies through consolidation.

## Business challenge

The National Payment Switch in France, STET, is owned by a consortium of financial institutions and processes more than 30 billion credit and debit card, cross-border, domestic and on-us payments annually. After being among the first countries to introduce the Clearing House Interbank Payments System (CHIPS) and personal identification number (PIN) countrywide, France's fraud rates were minimal for decades. But as criminals became more sophisticated, fraud losses returned and were roughly double the eurozone average for payment cards.

STET turned to IBM Safer Payments to help assess the fraud risk for every authorization request in real time. This score is passed to banks, issuers and acquirers that combine the risk score with customer information to form a final decision on declining fraudulent transactions.

## Transformation

**Build for speed and resiliency:** Given the high volumes, IBM Safer Payments was engineered to process up to 1,200 transactions per second, and can compute a risk score in less than 10 milliseconds. The switching infrastructure is also distributed to operate 24x7 and design for 99.999 percent uptime.

**Use limited data to gain understanding:** STET doesn't have any customer data or data from other payment channels. It doesn't even know if a debit and a credit card in its portfolio belong to the same cardholder. However, IBM Safer Payments compensates for this issue by being able to look across all transactions, countrywide, as well as creating deep behavioral profiles for millions of cards and merchants. This insight allows it to detect more sophisticated fraud patterns that are often committed by organized crime.

**Future-ready payments infrastructure:** In addition to helping ensure stability and scalability, IBM Safer Payments was designed to help STET adapt more quickly to new fraud trends, as well as provide fraud coverage to new and emerging payment types like real-time payments.

Illustration photo / Getty Images

## Results

**USD 100 million saved annually:** Reduced investigation times from more than 13 minutes to just over five minutes by automating much of the manual search and data entry process.

**A 1:1 false-positive rate:** Enhanced detection accuracy and the need to retrace investigation steps by automatically collecting comprehensive information in the investigation dossier.

## Business impact

**Reduced operational costs:** Time saved in identifying emerging threats can greatly reduce the banks' losses and more accurate rules should lessen false positives.

**Enabled future-ready fraud prevention:** STET expects to glean insights from its transaction data that will help its team continually devise fraud detection rules even more quickly and accurately.

**Fueled business growth:** This effective fraud prevention solution increases STET's ability to enter new markets and offer services for newer transaction types, including instant payments and Single Euro Payments Area (SEPA) payments, as well as achieve its ultimate goal of reducing payment fraud in France, Belgium and across the EU.

> "One of the benefits from IBM Safer Payments is that the transactions are scored in less than 10 milliseconds and that's allowing us to do real time scoring."

Rodolphe Meyer

/ Marketing & Business Development Director, STET

Case study II

# LARGE UK BANK LOWERS FALSE POSITIVES 70 PERCENT

The bank looked to IBM to streamline its AML investigations and better understand where its process could be improved.

Illustration photo / Getty Images

## Business challenge

A large financial institution based in the United Kingdom was dealing with a triple threat of AML inefficiency. First, its AML transaction monitoring system was generating 99 percent false-positive alerts, leading to wasted analyst effort. Second, the firm had multiple data sources across multiple lines of business with inconsistent data, leading to lengthy reviews to understand which data was accurate and which was outdated. And third, compounded by the prior points, it incurred high costs to conduct customer list screening across its large customer base.

The bank looked to IBM to streamline its AML investigations and better understand where its process could be improved.

> "Eliminating false-positive alerts using a combination of strategies to better understand individuals, as well as underlying risk."

## Transformation

**Start with the data:** Over a two-week period, IBM connected to the bank's disparate data sources across multiple lines of businesses. From this consolidation effort, subsequent analysis provided insight into previously unknown relationships and behaviors.

**Identify entities and networks:** With this combined data set, IBM found more than 20,000 alerts that were connected with entities that had more than one customer ID. In addition, by better understanding individuals, previously hidden relationship networks were exposed, providing not only fewer false positives, but fewer false negatives, as well.

**Improve accuracy and outcomes:** Lastly, using ML and statistical models, IBM scored alerts based on past dispositions to improve risk prioritization and eliminated time wasted on low-risk investigations. Using this priority ranking, the highest risks were sent directly to senior investigators.

## Results

**There were 70 percent fewer false positives:** Eliminated false-positive alerts using a combination of strategies to better understand individuals, as well as underlying risk

**There were 50 percent less false negatives**: Improved accuracy and reduced overlooked risks by better understanding connections between entities and relationship networks

## Business impact

**Improved use of limited resources:** By providing greater insight and eliminating duplicates, analysts can focus on the truly suspicious behaviors and quickly resolve low-risk alerts.

**Increased customer visibility:** With a consolidated view of customer accounts, the bank has improved its understanding of customer behavior and risk.

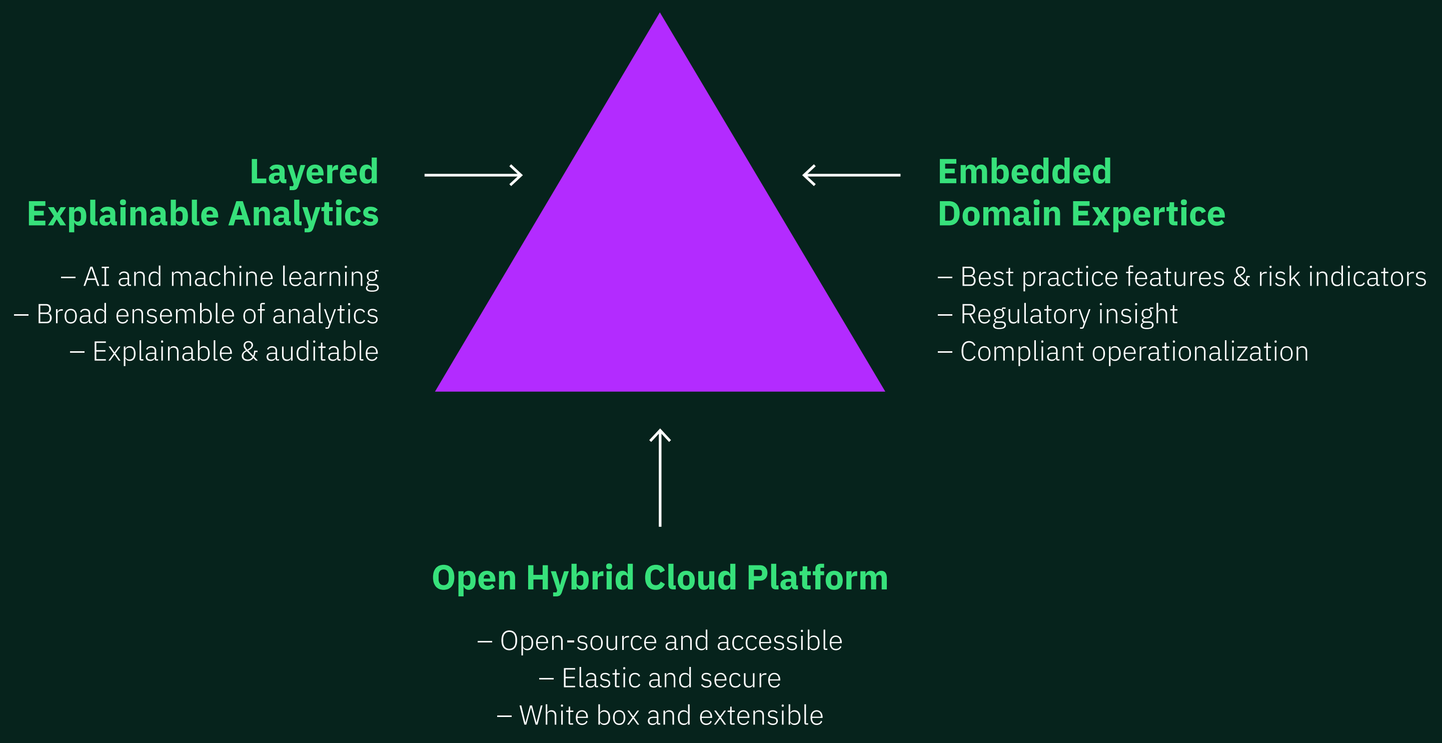
**Faster responses to emerging risks:** By proactively collecting and presenting contextual information to analysts, risks can be prioritized and resolved more quickly.

Moving forward

# How Itera & IBM can assist

Understanding where to focus and apply AI and cognitive solutions can be a daunting task. Itera and IBM are combining local and global capabilities, industry experience, proven software, and a data-driven approach with use of advanced cognitive solutions and AI. We offer our clients an agile deployment methodology, with significant return on investment based on proven track record.

## Our Unique Value Proposition



**Layered Explainable Analytics**

– AI and machine learning
– Broad ensemble of analytics
– Explainable & auditable

**Embedded Domain Expertice**

– Best practice features & risk indicators
– Regulatory insight
– Compliant operationalization

**Open Hybrid Cloud Platform**

– Open-source and accessible
– Elastic and secure
– White box and extensible

/ **Arne Mjøs**
Group CEO and founder, Itera
arne.mjos@itera.com

/ **Stefan Astroza**
Head of Financial Services, Itera
stefan.astroza@itera.com

/ **Paul Clandillon**
Practice leader financial crime, IBM
paul.clandillon@ie.ibm.com

The authors would like to especially thank Irène Sætre, Gro Matthiasen, Merete Brekke Skara, Anne-Gro Vonlanthen, Petter Solerød and Petter Nybakk for their contribution to this report.

Design: Itera
Photo: Itera (Olav Løkke), GettyImages

IBM × ITERA

Photo: Getty Images

Itera delivers digital solutions and services to innovative businesses in data-intensive market segments. The core competencies are technology, strategic consulting and design, and the solutions are developed in interdisciplinary, distributed teams across national borders. The group has 600 employees, operations in Norway, Denmark, Iceland, Slovakia and Ukraine and is listed on the Oslo Stock Exchange under the ticker ITERA.

**For further information about this report or how Itera can help your organization with the next generation of AML, please reach out to:**

Stefan Astroza
Head of Financial Services, Itera
stefan.astroza@itera.com

Paul Clandillon
Practice leader financial crime, IBM
paul.clandillon@ie.ibm.com