

## Proactive anti-financial crime strategies to improve compliance and reduce risk



# Contents

Finding a needle in a haystack.....	1
Shift from a tick-the-box approach to a risk-based, intelligence-led approach.....	1
1. Identify risk categories that should trigger investigations .....	1
2. Establish and follow clear protocols .....	2
3. Collaborate through public-private partnerships when possible ....	2
4. Examine a wide variety of information and sources, internal and external.....	2
5. Understand the value of big data analytics and AI.....	2
See how innovative technologies can help .....	3
Recognize the roadblocks to adopting AI.....	3
Incorporate ML models in phases as you adopt AI.....	5



## Finding a needle in a haystack

Financial institutions (FIs) have invested heavily in anti-financial crime strategies and the tools used to report potential risks to regulatory authorities. This work is vital to countering human, arms and drug trafficking, money-laundering schemes, terrorism and more – cutting off resources to criminals and terrorists.

But many organizations struggle to run efficient anti-money laundering (AML) investigations – so the percentage of detected and successfully prosecuted cases is often disappointing. Two key reasons are:

- It's hard to identify high-risk activities. Due to an overload of alerts and suboptimal use of resources and technology, it's like finding a needle in a haystack to uncover truly suspicious activity.
- The traditional rules-based approach to AML promotes a reactive rather than a proactive response. As a result, many FIs find it hard to stay ahead of today's sophisticated financial crime activities.

## Shift from a tick-the-box approach to a risk-based, intelligence-led approach

With a rules-based AML framework, FIs tend to concentrate on prescriptive compliance requirements during their AML investigative process. This tick-the-box approach promotes inefficient use of resources and leads to less-than-optimal results in a changing business landscape.

To detect financial crime risks proactively and achieve the best possible outcomes, FIs should consider a nimble and holistic risk-based approach. While there is no “one size fits all” way to do it, there are several best practices to follow.

Here's a framework to help you get started.

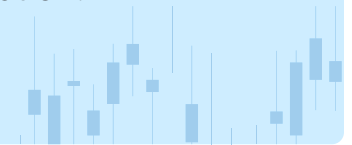
### 1. Identify risk categories that should trigger investigations

Every institution needs a well-defined operating process for initiating investigations – and it begins by defining the types of risk events that should trigger an investigation. These events usually fit into one of the following categories:

- Regulatory inquiries.
- Internal control activities and other findings.
- Adverse media and financial crime trends.

For each risk type, you'll need to clearly define relevant trigger events and corresponding actions to take (e.g., recent cyberattacks on competitors, new money laundering schemes, etc.). As you assess the trigger events, gather evidence of what happened, determine if it can be substantiated, check supporting documentation and determine whether there's justification to open an investigation.

Every FI needs a well-defined operating process for initiating investigations. It starts by defining the types of risk events that should trigger an investigation.



## 2. Establish and follow clear protocols

For events that require investigation, you should define and document the background, scope, methodology and minimum requirements used in the assessment. Along the way, create a communication protocol, track progress and reporting needs, and perform stakeholder management.

Investigative teams should follow the required information-sharing protocols to perform cross-border investigations. You should also define the mitigation measures most appropriate for investigating each type of case.

## 3. Collaborate through public-private partnerships when possible

Historically, there hasn't been enough communication among different organizations in the AML landscape. One reason is that regulated organizations must conform to laws and restrictions around operating or sharing information across jurisdictional borders. This has led to FIs working in silos.

Through public-private partnership (PPP) platforms, public authorities (including financial intelligence units), law enforcement and private entities can share information. Joining forces strengthens the fight against money laundering and can stop illicit movements of wealth - with everyone benefitting from the collaboration.

This information exchange includes strategic and aggregate data related to typologies and threats as well as operational and tactical data. The aim is to enhance financial crime detection by identifying suspicious transaction patterns between FIs and criminal networks on a broader scale.

PPPs are not available at all levels or in all regions. Today, they're used to uncover counterterrorism financing and in areas where local legal gateways are available to support national PPPs. Whenever possible, it should be a priority to expand PPP platforms.

## 4. Examine a wide variety of information and sources, internal and external

To perform the most thorough investigation possible, you'll want to identify all relevant information and triggers, including those from external sources.

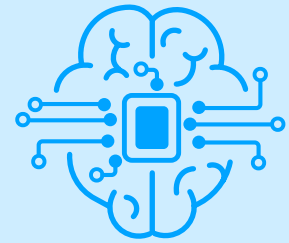
Recommendations include:

- Reviewing information from external databases, websites and research tools.
- Attending meetings of industry associations, working groups or other risk-specific events.
- Meeting with personnel from law enforcement agencies.

## 5. Understand the value of big data analytics and AI

Big data technologies and fast data processing engines provide a centralized infrastructure that makes it more efficient to gather, make searchable, store and promptly access vast amounts of information across different jurisdictions. Such technologies can make you much more successful at fighting financial crimes.

One foundational technology that's helpful with AML investigations is network visualization. This technique visually shows relationships and link analysis to reveal complex, hidden relationships that need deeper investigation.



### Positive changes in today's AI landscape


- Regulators have started to embrace AI.
- Data is managed as part of the AI process.
- AI is a journey that calls for fulfilling different requirements at different stages.
- It's increasingly cost-effective to use AI.

A consolidated view of associated customer information across lines of business via network visualization assists with both investigation and detection capabilities. By exploring data through visualizations, you can improve oversight, monitoring, and operational and management reporting for your AML program. And you can use network analytics to find nested relationships that could signal money laundering schemes.

As you incorporate additional big data technologies into your processes, evaluate the advantages of advanced analytics and AI techniques like robotic process automation, machine learning (ML) and natural language processing.

See how innovative technologies can help


## DEMYSTIFYING AI TERMINOLOGIES



**Artificial Intelligence**

The science of training computers to perform tasks mimicking human reasoning


---



**Machine Learning**

A subfield of AI that automatically learns and improves from experience without being explicitly programmed


- ML enables FIs to use decision trees or neural networks as alert scoring models - setting the algorithm to learn from past compliance dispositions, then scoring future alerts based on the likelihood of them being automatically closed or escalated by compliance officers.



**Natural Language Processing**

A subfield of AI that focuses on using technology to analyze and understand human language

- NLP can auto-generate narration for cases or regulatory reports.



**Robotic Process Automation**

A software that mimics human actions by automating simple and repetitive tasks across applications

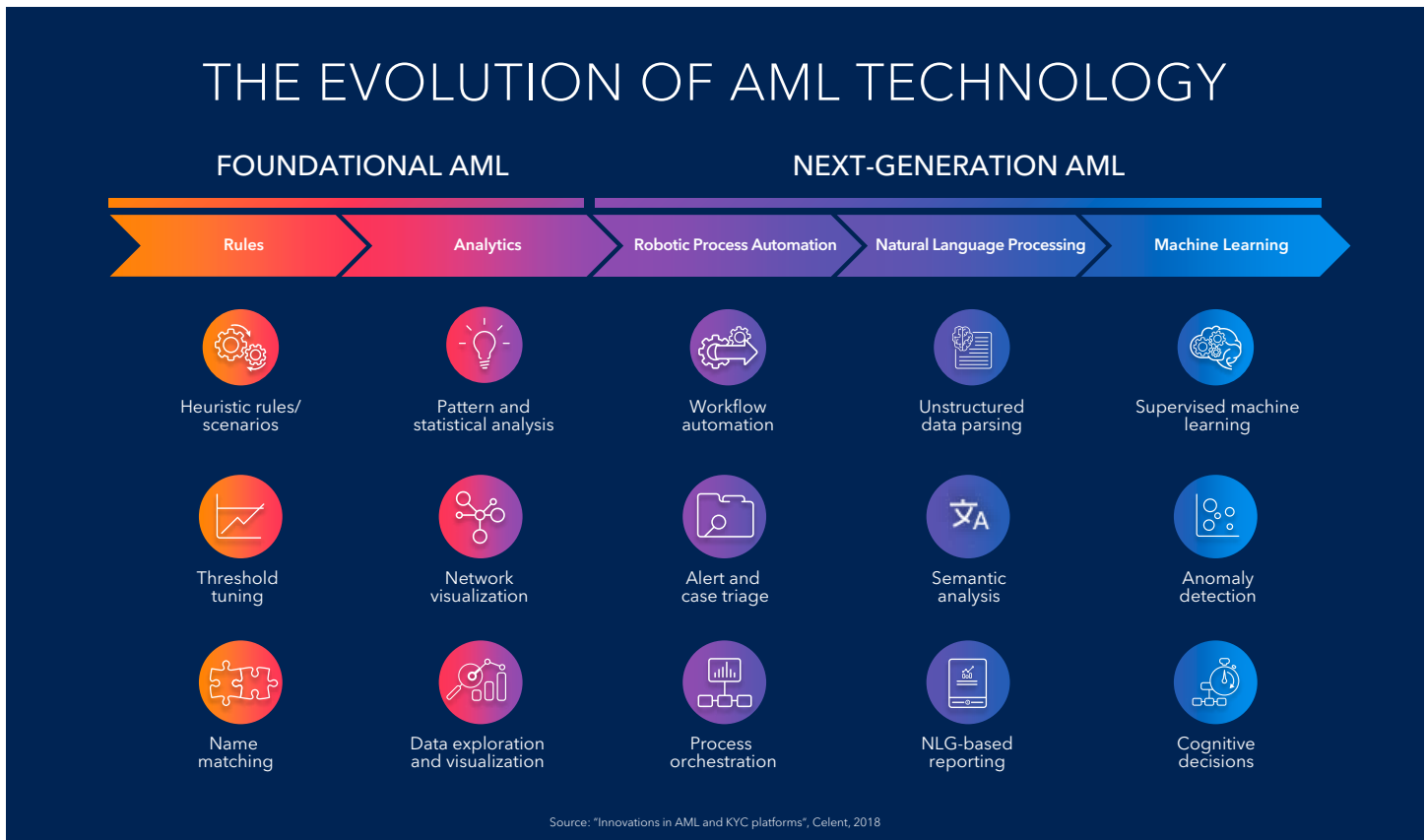
- RPA automates internal and external information gathering and automatically creates case files. In turn, analysts and investigators can make decisions instead of performing mundane, time-consuming tasks. RPA can reduce case review times by 20% to 30%.

## Recognize the roadblocks to adopting AI

When you're implementing new technology, it's helpful to understand behind-the-scenes concerns that can stall efforts to move ahead. Make it a priority to learn whether your organization's stakeholders have any of these common concerns - then you can determine how to address them.

- **Frustration and unrealistic expectations.** It's easy to get discouraged with AI because its benefits don't appear overnight. Teams may give up too soon if they don't understand that AI benefits are cumulative. As you increasingly adopt and use AI, its effectiveness will multiply - you should see a gradual return on investment.

- **The belief that you need to toss traditional tools.** Adopting AI doesn't mean you won't ever need to use traditional tools and techniques again. Simple rules and analytics are still valuable for certain types of risks - they work hand in hand with newer AI technologies.
- **Fear of not keeping up with user, customer or regulator demands.** FIs want to support AI transparency, explainability, responsibility and ease of use. Users need to understand and be able to confidently defend their AI algorithms to regulators. By adopting the right technology platform - from a partner that can guide you through these processes - you can prepare your team for regulatory exams.
- **Concerns about data management and privacy.** Data needs to be managed and transformed as part of the AI process so it can help you uncover new insights. While this use of data is essential, it raises concerns about data quality and privacy. Adopting AI technology that effectively manages both is vital. Ensure that your data protection rules balance with those designed to prevent financial crimes.
- **Failing to update knowledge and resources.** Your knowledge and skilled resources need to evolve along with your use of data and advanced analytics. As tools, techniques and requirements change, you must be prepared to adapt through training or hiring new internal or external resources.
- **Cost and time to market.** The cost of compliance is already high, and FIs are concerned about the cost of implementing AI technologies. But as early adopters have proven, AI helps lower the cost of compliance by enabling efficiency - it's also more effective at identifying threats than humans alone.



**Figure:** AML technology has evolved over time from basic rules and analytics to sophisticated, next-generation techniques.

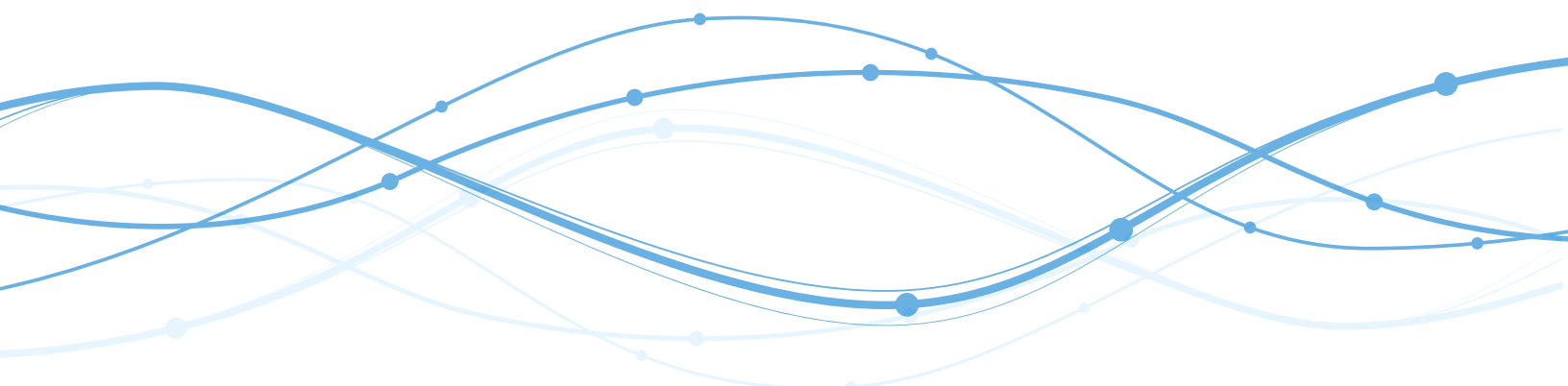
## Incorporate ML models in phases as you adopt AI

FIs must diligently manage the raw customer, account and transaction data fed into their transaction monitoring solutions. The same diligence is required when using AI technologies in AML applications. That includes oversight of human decisions that are crucial components of AI models.

Depending on where your organization is in the technology adoption journey - and how mature your AML programs and analytics are - you can introduce ML models to optimize detection, investigation and reporting capabilities. You can do this in phases.

The first step is to use a comprehensive, trustworthy solution to ingest, wrangle, aggregate and enrich the data pulled from various internal and external sources. Across each phase of the implementation and maintenance life cycle, you should establish rigor and engage appropriate stakeholders. This approach will ensure you incorporate appropriate planning, oversight and governance practices.

Create a framework to build trust in AI solutions by developing and using AI in a way that's consistent with your user requirements, organizational values and regulatory expectations. And work with a financial crime management solutions partner that offers the core elements of fairness, explainability, robustness, lineage and transparency. All these elements are essential to helping you build and deploy responsible AI solutions.



Learn more about [SAS solutions for AML and CFT compliance](#).

