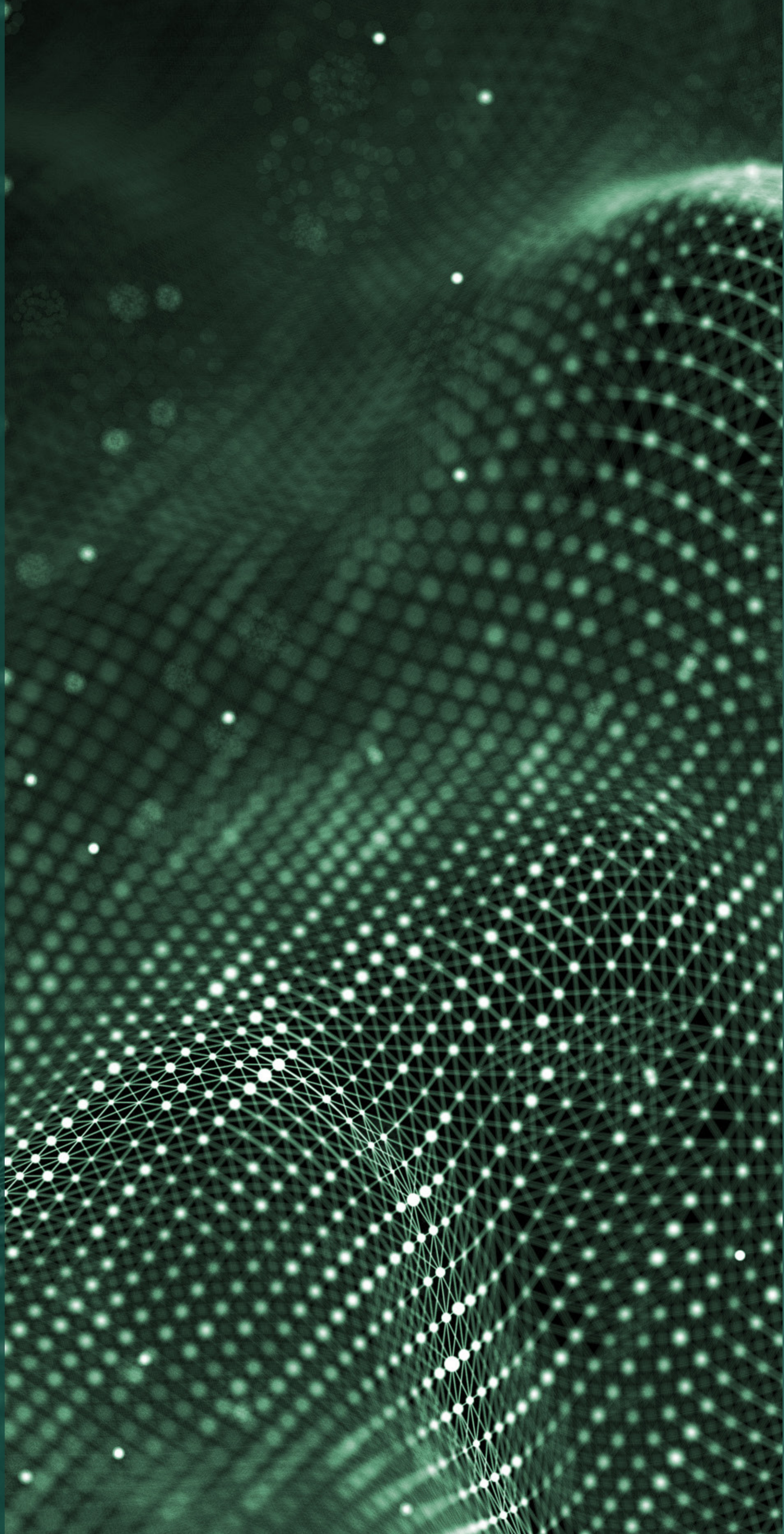
An Advisense Insights report

AML State of Play Special edition on AI

Table of Contents



Foreword

The financial sector continues to evolve under the combined influence of regulatory developments, operational pressures, and advances in technology. One area where this convergence is particularly visible is financial crime prevention. As regulatory expectations increase and data volumes grow, institutions are looking to AI to enhance efficiency, improve detection, and reduce risk.

This report offers a data-driven look at how financial institutions are progressing in their adoption of AI for financial crime prevention. Drawing on insights from senior leaders at 28 institutions, we assess where the industry stands, what is holding it back, and what is needed to move forward.

The findings show cautious momentum. While interest in AI is strong, most organizations remain in the early stages of implementation. Core challenges persist - legacy systems, poor data quality, lack of internal AI expertise, and regulatory uncertainty, particularly around the forthcoming EU Anti-Money Laundering Regulation.

Yet these barriers are also strategic priorities. Institutions that address them now - by investing in cross-functional capabilities, modernizing infrastructure, and aligning compliance and technology strategies - will gain a clear advantage. Not only in meeting regulatory demands, but in building more resilient, efficient financial crime frameworks.

At Advisense, we work closely with clients at the intersection of compliance, risk, tech and innovation. Our aim with this report is to offer not just a snapshot of current practice, but practical guidance for institutions looking to take the next step in using AI as a tool for smarter, more effective financial crime prevention.

Christine Ehnström
CEO Advisense

About this Report

The Advisense AML State of Play report was launched in 2022, a first in its kind, in order to establish just that – The state of play within AML, taking a broad and candid look at how AML has progressed since the money laundering scandals surfaced in the Nordics some years ago. The concept is based on the ability to obtain input from interviews on anonymous basis with senior AML executives in first and second line functions.

This special edition on AI expands the scope of the State of Play concept to capture the accelerating pace of AI adoption, identify common goals and challenges together with key opportunities where AI can add value. It is based on a qualitative survey involving respondents from 28 financial institutions across various sectors.

The objective of the report is to provide a focused view on the current state of AI implementation across various organisations and help advance strategies to move from pilots towards large scale transformation and greater efficiency, away from today´s view of AI as a hurdle or black box.

The survey comprised four sections with approximately 40 questions designed to capture a broad view of AI adoption:

1. **Current Capabilities Assessment:** How far have companies really come in their endeavours to leverage AI? First section sets the scene, and examines existing AI implementations, data utilisation, and operational applications.

2. **Future Direction Planning:** Given how far companies are right now, what can reasonably be said about how plans are made to set a future direction? The second section explores what respondents have to say about emerging technologies, implementation timelines and strategic priorities.

3. **Challenges and Barriers:** What hinders organisations from moving forward? The third section cover questions that help us shed light on and identify what is perceived as technical, regulatory and organisational obstacles.

4. **Organisational Readiness:** Are organisations geared up and ready once the direction is set? In the final section, the report presents results from questions assessing governance structures, expertise levels, and change management capacity.

The Respondents and Our Data

The survey was conducted during the spring of 2025 involving respondents from 28 different institutions participating on anonymous basis. Although the dataset is limited, it does provide a representative snapshot of the current landscape and approaches to AI in financial crime prevention. It should be noted that percentage numbers presented in this report are rounded. This means that in some cases, adding up the percentages of responses to a given question may not result precisely in 100%.

The respondents represent a diverse cross-section of the financial services industry, including payment service providers (21%), digital banking platforms (32%), lending platforms (25%), investment/wealth management platforms (11%), and crypto/digital asset service providers (7%). Some respondents represent traditional banks, however chose to classify themselves as payment service providers.

Understanding the profiles and categories of respondents provide essential context for interpreting, the survey findings and understanding the current state of AI adoption in financial crime prevention explored in the following sections.

The organisations that respondents represent range in size: startups with 1-20 employees (11%), small organisations with 21-50 employees (28%), medium-sized with 51-200 employees (25 %), and large organisations with 201+ employees (36%). This diversity allows us to examine how organisational size impacts AI adoption, resource allocation, and implementation challenges in financial crime prevention.

The majority of respondents are compliance professionals, with 64% classifying themselves as Compliance/AML Officers, while 29% selected "Other" roles and 7% from Business Development.

We can tell the following from the results considering the varying profiles and categories of respondents:

1. **Diverse ecosystem:** The financial services industry continues to evolve and specialise in core capabilities, each with unique financial crime risk profiles and compliance requirements.

2. **Compliance-driven perspective:** Since respondents are predominantly AML professionals, their input naturally tends to focus on how the use AI in AML should be approached from a compliance perspective to meet regulatory requirements, rather than focusing on AI tools as strategic technology investments. This is important to keep in mind when interpreting or drawing conclusions from the survey results.

3. **Size variation:** The relatively even distribution of respondents across organisations of different sizes indicates that the use of AI in financial crime prevention is relevant across the board, not just for large institutions with substantial resources.

4. **Digital transformation:** The large representation of digital-native organisations, that means companies that were founded in the digital era and have technology and digital processes embedded into their core operations from the start such as payment providers, digital banks, crypto platforms, reflects the current digital transformation of financial services and the need for a more progressive approach to compliance in line with consumer expectations and the speed of digital services.

Setting the Scene

Financial crime prevention has undergone several transformational stages over the past decades. The traditional approach relied heavily on rule-based systems and manual reviews, which has served as the cornerstone of compliance programs from the 1990s through the early 2000s. These systems flagged transactions based on predefined thresholds and typologies, creating alerts for human analysts to investigate.

The mid-2000s saw the introduction of more sophisticated statistical methods and basic machine learning approaches, including regression models and decision trees. These advanced techniques improved detection capabilities but still relied on structured data and predetermined patterns. During this period, financial institutions continued to face challenges with high false positive rates and resource-intensive investigation processes.

Crossing the Chasm Towards Transformation

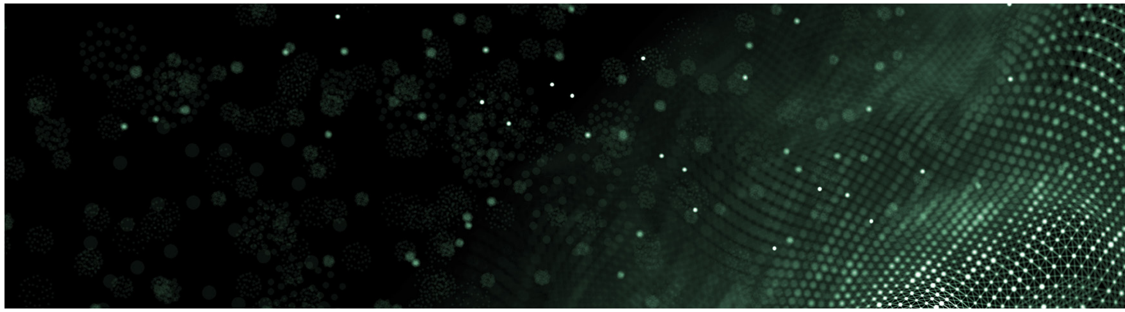
A key obstacle to effective financial crime prevention is the continued reliance on legacy systems, often patched-together infrastructures that were not designed to support today's data-driven compliance demands. These systems often lack flexibility, interoperability and the processing power needed for real-time risk detection or adaptive decision making. AI, however, can act as a bridge. Through layered implementation, AI-powered tools can complement existing infrastructure by enriching data quality, identifying patterns across silos, and automating rule refinement. This allows organisations to extract more value from legacy environments while gradually modernising their compliance architecture, minimising disruption and accelerating capability uplift.

Compliance Will Need Significantly more Data

As the regulatory landscape evolves, the upcoming EU Anti-Money Laundering Regulation (AMLR) marks a major shift in compliance expectations across the financial sector. One of the key challenges for institutions is ensuring readiness for this harmonised framework while maintaining operational efficiency. Here, AI becomes not only a tool for detection, but a strategic enabler. By leveraging advanced AI capabilities firms can strengthen their ability to meet AMLR's heightened requirements on data quality, governance and risk-based monitoring etc.

Beyond compliance readiness, AI also present a powerful opportunity to increase operational efficiency in financial crime prevention. Traditional methods often rely labour-intensive processes putting pressure on compliance teams and driving up costs. AI-driven solutions can streamline workflows, reduce manual intervention, and enable faster more targeted decision making. This leads to a more cost-efficient function, better use of internal resources, and ultimately more effective detection of financial crime.

While both AML and fraud prevention share the goal of protecting the financial system, the application of AI often diverges significantly between the two. Fraud detection typically operates in real time, with AI models trained to flag anomalous behaviour immediately to prevent losses or customer harm. In contrast, AML processes often occur after the fact, with AI used to prioritise alerts, identify hidden networks, or refine risk scoring based on historical data. These different timelines and objectives require tailored AI approaches: speed and precision in fraud, versus explainability, traceability, and regulatory defensibility in AML. Recognising this distinction is essential when designing or implementing AI solutions in financial crime programmes.



From Rules to Intelligence

The transition from rule-based to AI-enhanced financial crime prevention represents more than a technological shift. It's a significant shift in how organisations chose to approach their financial crime prevention efforts and objective. While rule-based systems fundamentally ask, "Does this activity break a predefined pattern?" AI systems ask, "Is this activity consistent with expected behaviour?" This distinction is crucial as financial criminals increasingly operate within technical rule boundaries while exhibiting subtly anomalous behaviour patterns.

In our implementations, we've found that the most powerful solutions maintain rule-based foundations for clear typologies while layering AI capabilities to detect the nuanced deviations that rules alone cannot identify.

Act to Impact

Our experience implementing solutions across organisations of various sizes reveals a counterintuitive pattern: smaller institutions sometimes achieve faster success with AI in financial crime prevention than their larger counterparts. While larger organisations have more resources, they often face greater complexity in data integration, more entrenched legacy systems, and more intricate decision-making processes. Smaller organisations can benefit from agility, cleaner data environments, and more streamlined approval processes. The key success factor is not size but rather the clarity of use cases, quality of available data, and organisational alignment - areas where targeted external expertise can significantly accelerate progress.

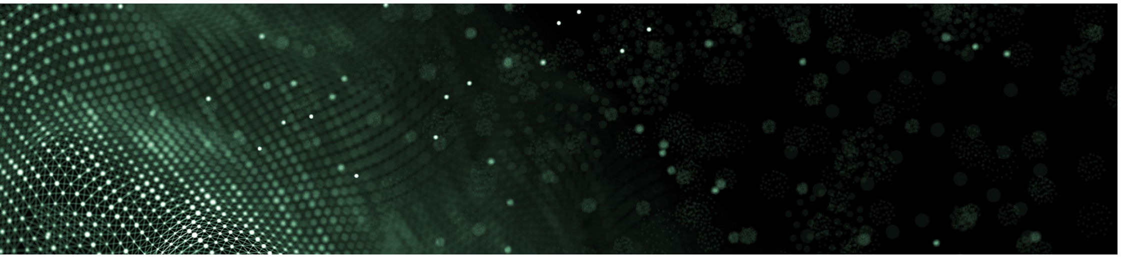
The adoption of AI in financial crime prevention represents more than a technological upgrade; it signifies a fundamental shift in how financial institutions approach compliance and risk management. However, as our survey reveals, many institutions are still in the early stages of this transformation, facing challenges related to expertise, data quality, and integration with legacy systems.

1. How is AI Applied in Financial Crime Prevention Today?

Where are financial companies today, is it more talk than shop or is there a silent revolution taking place behind closed doors?

To get an idea of this, the first section of the survey discusses how financial institutions are currently applying AI within their financial crime prevention frameworks. The results reveal an industry in the early stages of adoption, with variation in implementation areas and capabilities.

In summary, financial institutions are predominantly in the exploratory or early implementation phases of AI adoption for financial crime prevention. While there is broad movement towards AI, most organisations have little to show beyond pilot stages. No respondents suggested that they have a full implementation in place to any extent at all. In other words, people are cautious and the barriers to more advanced implementation are short of significant still.

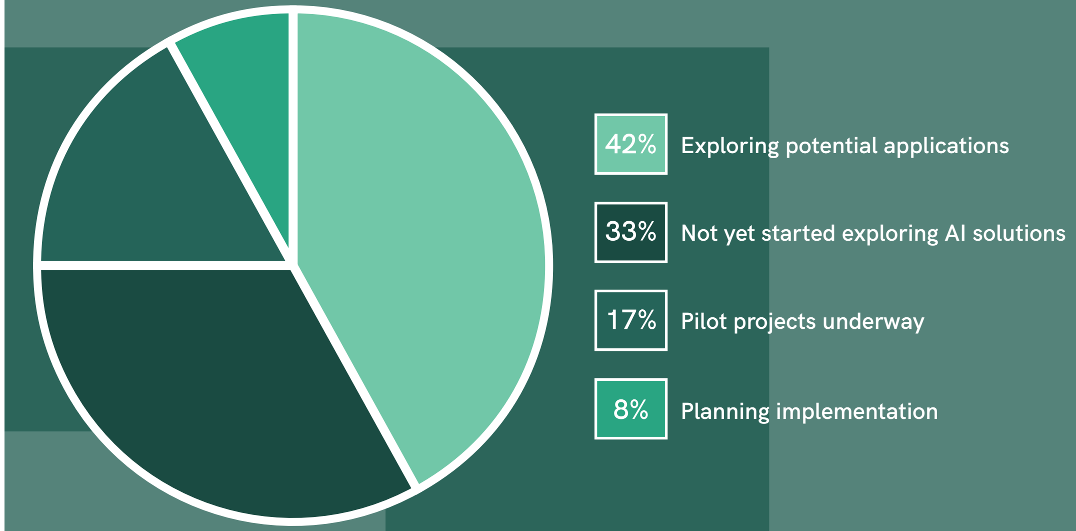


As to the question "What is your organisation's current stage in AI adoption within Financial Crime Prevention and AML/CTF?", one in three (33%) said they not even started exploring AI solutions yet while 42% confirmed that they are exploring potential applications. 17% said they have pilot projects underway while 8% said they are planning implementation of some sort. No one chose to say that they have already implemented AI solutions or have advanced AI implementation with ongoing optimisation.

The survey further asked what respondents see as their primary challenges, in order words, what´s stopping them from moving forward with implementation. Very summarily, the answer provided is that people don´t have either the necessary AI skills (a whopping 62%), nor do they believe that their data is sufficiently qualitative, or, there is just no data available (54%). Regulatory concerns is an important issue which 46% of the respondents could confirm. Another brick in the wall separating today´s manual work and AI-enabled automation is and old and persistent showstopper – integration with legacy systems (50%). Other deterrents include the cost of implementation (42%), but also explainability/transparency concerns and the ability to warrant investments because it is hard to measure effectiveness and payback up front (12%).

AI Adoption Status

Figure 1: Current state of AI adoption in financial crime prevention



Closing the Pilot-to-Production Gap, Or Just Launching a Pilot to Start With?

The concentration of organisations in the exploration and pilot phases, and no respondents confirming a full implementation, point towards what may be called the "pilot-to-production gap." This is in itself nothing extraordinary, but rather a common challenge observed in conjunction with technology shifts, and drawing upon general hard-earned experience, it might point us towards some potential explanations including unclear success metrics for pilots, inadequate planning for production, scale data and infrastructure requirements, and/or insufficient governance frameworks.

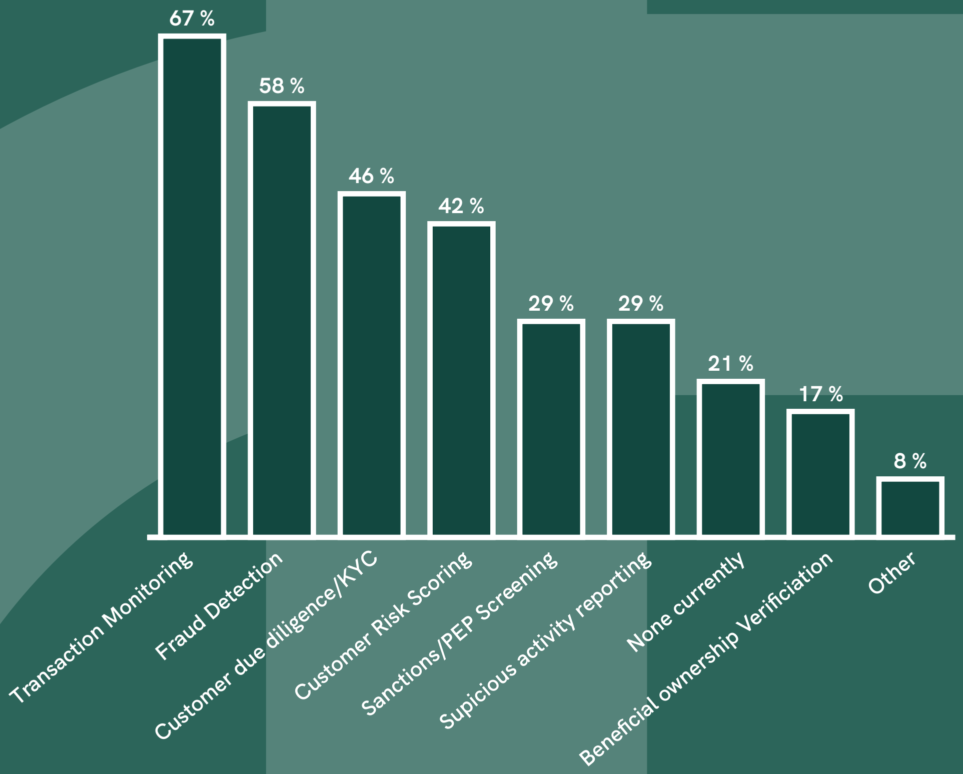
Successful transitions to production require defining specific success criteria before pilot initiation, involving production teams early in the process, and developing governance frameworks that can evolve with the AI implementation. Organisations that address these factors proactively are significantly more likely to bridge this gap successfully.

Prioritised Areas of Application

Even if the responses tell us that it is still early days, in what areas are companies already applying, or where would they prioritize applying AI in their future developments?

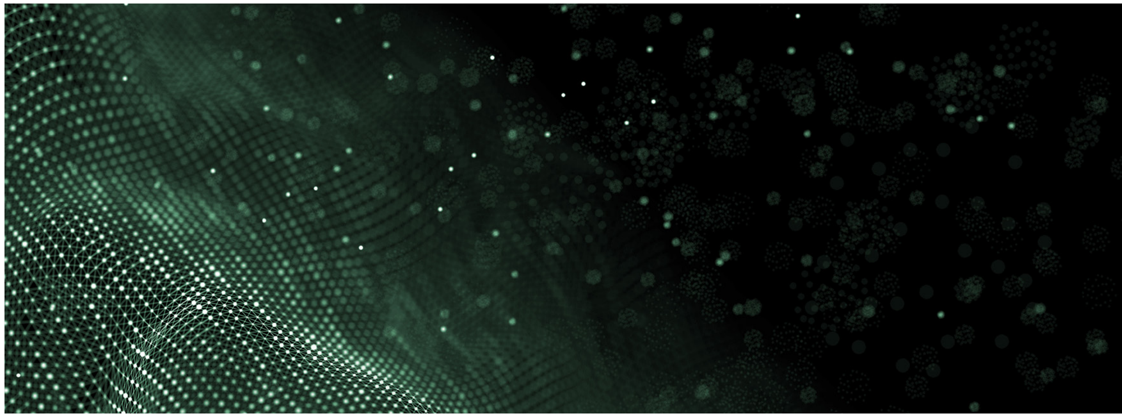
Transaction monitoring stands out as a clear key priority rallying 67% of respondents, closely followed by fraud at 58%. Other important application areas underway or on the wish-list are customer due diligence or "KYC" (Know Your Customer) at 46% and customer risk scoring at 42%. This distribution aligns with areas that have high alert volumes, significant manual processing requirements, and established typologies — making them natural candidates for AI enhancement. Other areas where AI is thought to be able to help the most include sanctions/PEP screening and automation of suspicious activity reporting, both arriving at 29% or responses. A slightly more modest 17% said they would be looking to apply AI in order to verify unique beneficiary owners.

Figure 1: Current state of AI adoption in financial crime prevention



What Is Triggering Companies to Move Ahead? (If They Are Not Moving Already)

Given what we now know about what the perceived stumbling blocks are, what are the primary motivations then to eventually move ahead and incorporating AI into financial crime prevention programs? Using a 1-5 scale where 1 is "not important" to 5 "critical priority", respondents said that they want to improve detection and increase operational efficiency (both rating at 3.8). AI is also hoped to be the final antidote for false positives (3.3) and a pathway towards (smarter) regulatory compliance (2.4). At current stage, using AI to achieve a competitive differentiation only scored 1.6, which might have different explanations. Cutting false positives means cutting cost and improving detection accuracy and operational efficiency etc, which logically would by the same token help any organisation sharpen its competitiveness in some senses.



Something Else – or More – Than Just Replacing Humans

What´s more important, cutting costs or improving the robustness and delivery of systems to serve the ultimate purpose, that is preventing money-laundering?

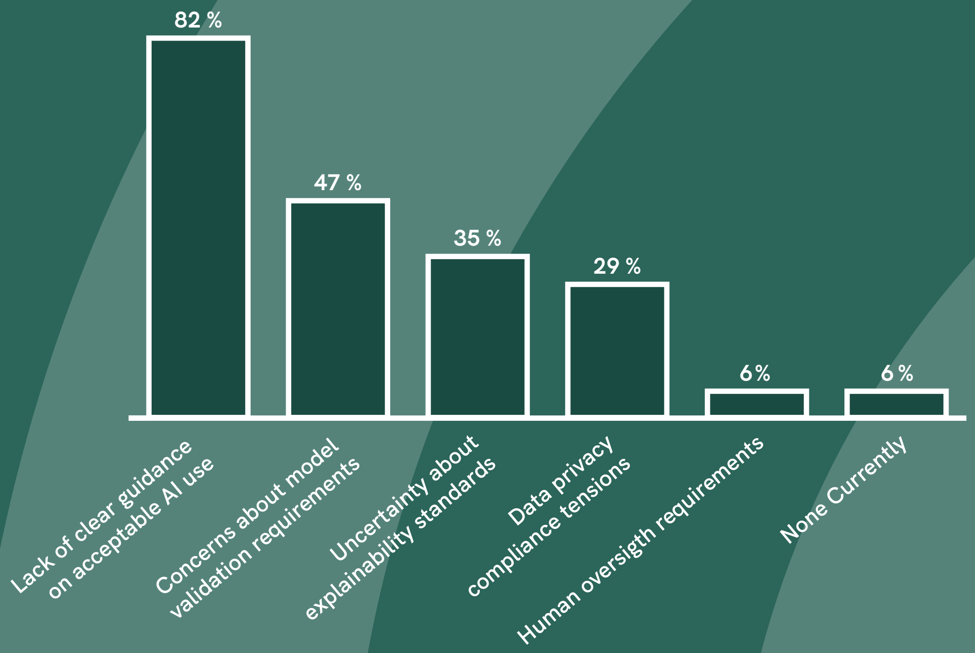
The focus on detection and accuracy signals a maturing understanding of how AI can contribute to both organisational effectiveness and compliance. The ability to integrate AI into detection processes is eventually the only rational way forward in continuously reinforce first line AML processes and models, which is something more than an issue of replacing human expertise. The result is greater acceptance across the organisation, stronger governance structures, and more sustainable use of AI that enhances both operational performance and the organisation's ability to fulfil its regulatory and ethical responsibilities.

Expectations of the Financial Supervisory Authorities – Hope or Halt?

The stance of the financial supervisory authority is always a concern. We asked the question "What concerns do you have about the expectations of the Swedish Financial Supervisory Authority regarding the use of AI in financial crime prevention". Only 11 out of 17 were prepared to comment, which leaves room for interpretation. For sure it is both a very complex and perhaps sensitive issue.

Among those who chose to respond, a large majority (82%) said there is a lack of clear guidance on what constitutes acceptable use of AI. This could be pretty worrying in a market which is renowned as hotbed for fintech companies and innovation. Other issues keeping respondents up at night include concerns about model validation requirements (47%), uncertainty about explainability standards (35%) and data privacy compliance tensions (29%). Human oversight requirements qualified only as a marginal runner up at 6% with and equal share saying they have no concerns at all with the FSA regarding AI.

Figure 2: Regulatory concerns regarding AI implementation



Data, Data and Data

As the saying goes, there are three kinds of lies: lies, damned lies, and statistics. This phrase is widely used to highlight how statistics can be manipulated to support weak or misleading arguments. The same might be applied to data. As we have established, data quality and the availability of data is a make-or-break when implementing AI in any process. We asked the question "what types of data are you leveraging or planning to leverage for AI in financial crime prevention or AML/CTF." A difficult question given the point of departure where many organisations still find themselves.

An overwhelming majority (78%) are or will be leveraging transaction data, followed by behavioural patterns (67%) an equal share stating customer profile data and external data sources (such as news, watchlists) (61% respectively). Device and digital identity data and social network or relationship data is also quite interesting according to 17% of the respondents, while 28% said "none currently", which can only be understood as they are not leveraging any data for AI as is right now.

Are Companies Prioritising "The Right Data"?

While transaction data, customer profile data, and external data sources are among the most prioritised types of data, whether currently in use or planned to be used, the significantly lower utilisation of device/digital identity data (17%) and social network/relationship data (17%) represent a substantial missed opportunity for many organisations.

Experience from implementation projects in the financial industry suggests that these alternative data sources can provide a critical context that transaction data alone cannot offer. For example, device intelligence can reveal account takeover attempts that appear normal from a transaction perspective, while relationship mapping can uncover coordinated money laundering rings that operate below threshold-based detection systems. Organisations able to leverage broader data sources to develop a multi-dimensional view of customer activity and risk may be the winners in the quest to drive AI-powered financial crime prevention efforts in both the short and long-term.

Advisense Insight

What respondents tell us about their data strategies reflects an understanding that effective financial crime prevention requires a multi-dimensional view of customer activity and risk. The lower percentages for device/digital identity and social network data may indicate privacy concerns or implementation challenges.

The Balance Between Man and Machine: Explaining What You Do

How are companies reasoning around striking an optimal balance between machine and humans? What levels of integration do their AI/ML systems have with human analysts in the investigative workflow and are people able to explain what they do?

A relative majority of 36% of the respondents say that they have minimal or no integration with human analysis in this workflow, while 14% point towards automated alerts with contextual investigation aids as what they do in terms of integration. As a red thread in this report, a large chunk of respondents opted to refrain from replying or said they are unsure about this.

However, based on those responses that tell us that there is a lot of development and piloting taking place, how are those companies addressing explainability and transparency requirements for regulatory purposes? One in three companies say they are not addressing this yet, while 40% say they are not sure. Only 7% say they have explainability assured by using inherently explainable models such as decision trees or that they are developing model documentation frameworks (also 7%).

Overall, this particular response points towards a significant issue not in the least considering the link to the concern around the financial supervisory authority´s role in bringing clarity around expectations on AI applications to AML/CTF not earlier in this report.

Measuring the Effectiveness of AI Applications

As discussed earlier in this report, there are some uncertainties that might deter companies from moving forward, including the cost of implementation but also explainability/transparency concerns and the ability to warrant investments because it is hard to measure effectiveness and payback up front.

However, when, perhaps rather than if, companies advance, what metrics do they use or plan to use to measure the effectiveness of their AI applications in financial crime prevention and AI/CTF (recalling the truism what gets measured gets done)?

Almost a third, 29% of respondents say that they will use suspicious activity detection rates as an efficiency measure, which mirrors the prioritisation of AI into transaction monitoring. There is also a fair share of 24% responding that processing time improvements and cost savings are their measures. 17% unsurprisingly said the reduction in false positives rates is key, or that regulatory feedback is a good measure (12%). Again, 29% have nothing determined and 41% remain unsure.

2. An AI-driven Future

While current AI implementation is in its infancy or in exploratory stages, what can be said about what financial institutions are thinking about emerging capabilities and future directions? Are there clear objectives and strategies taking shape already?

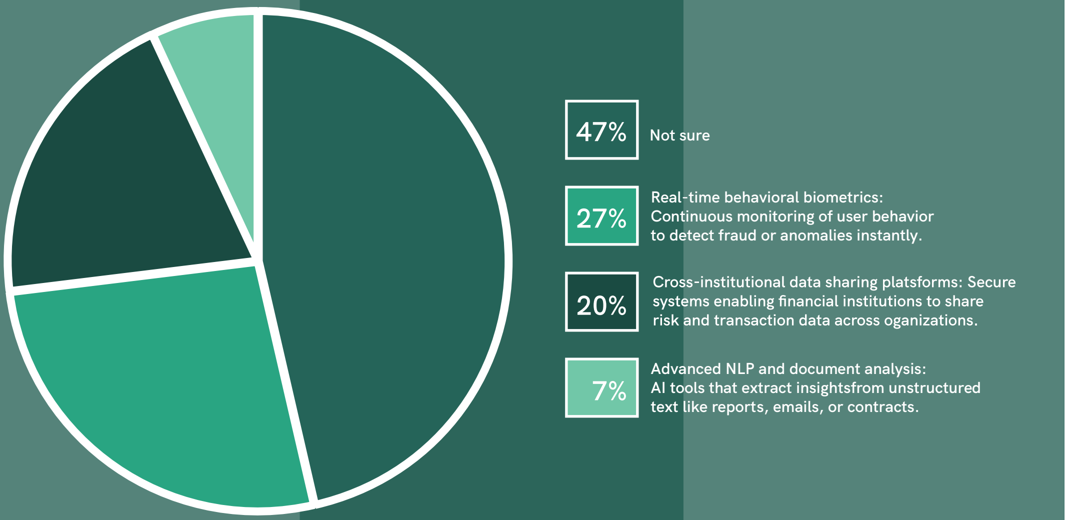
The second section of our survey deals with future perspectives on technologies, data approaches, and how advanced applications could shape financial crime prevention in the coming years.

The short-term view

Whatever is a new stride today in AI applications will be yesteryears news tomorrow. The rapid pace of development suggest that a short-term view of two to three years is already too long. However, we asked the question what emerging AI technologies that respondents think would have the biggest impact on financial crime prevention in the next two to three years' time.

Discounting the 47% that are not sure enough to comment, a relative majority of 27% said that they expect real-time behavioural biometrics to have the greatest impact, exemplified by the use case continuous monitoring of user behaviour to detect fraud or anomalies instantaneously. The runner up in the quest for impact is cross-institutional data-sharing at 20%, referring to secure systems enabling financial institutions to share risk and transaction data across organisations, followed by advanced NPL and document analysis at 7% with regards to how AI tools can extract insights from unstructured text such as reports, emails and contracts. It is worth noting that no one chose quantum computing applications as an option.

Figure 1: Current state of AI adoption in financial crime prevention



The significant percentage of respondents who said they are unsure, indicates the current uncertainty about future technological directions and/or potential limitations, while no doubt, there is also a recognition of the value of cross-institutional data sharing platforms and collaborative approaches to financial crime prevention.

Where Will Emerging AI Technologies Have the Greatest Impact?

Respondents say the greatestimpact of AI applications that are now emerging will be real-time behavioural biometrics. This suggests a shift in detection philosophy. Traditional systems ask, "Does this transaction fit the rules?" Behavioural biometrics asks, "Is this actually the customer?" By analysing patterns in typing rhythm, mouse movements, and device handling, such systems create a unique digital fingerprint for each user.

The appeal of the technology lies in its dual benefit: enhanced security but without customer friction. In contrast to the option to add authentication steps which frustrate users, behavioural biometrics operate silently in the background, continuously validating identity throughout a session. This obviously represenvts an opportunity to leapfrog traditional detection limitations. Rather than chasing increasingly sophisticated account takeover schemes with more rules, behavioural biometrics offers a fundamentally different approach, one that adapts automatically as criminal techniques evolve.

The potential usages of real-time behavioural biometrics:

- Dynamic Authentication: Continuous verification based on typing patterns, mouse movements, device handling, and navigation behaviours.
- Account Takeover Detection: Real-time identification of unusual behavioural patterns indicating unauthorised access.
- Fraud Pattern Recognition: Detection of subtle behavioural deviations from established customer baselines.
- Session Risk Assessment: Continuous risk scoring based on behavioural anomalies during transaction sessions.
- Synthetic Identity Detection: Identifying artificial behavioural patterns that indicate synthetic identity fraud.

3. Closing the "pilot-to-production" gap

As financial institutions explore the potential of applying AI to prevent financial crime and AML/CTF, several key strategies emerge for addressing challenges and capitalising on opportunities. With the results from this survey at hand, what can be said about what organisations may want to consider when setting their strategic priorities ahead?

1. Establishing a Strong Foundation

The pursuit of advanced AI/ML capabilities will require that organisations first resolve some fundamental issues:

Expertise development: These include the ability to build internal capabilities through training, hiring, and partnerships to overcome the expertise gap, identified by 63% of **the respondents.**

Cross-functional alignment: Creating governance structures that facilitate collaboration between compliance, technology, and business units is essential to meet the noted demand for extensive enterprise-wide alignment. This further needs to involve the implementation of data governance, standardisation, and quality improvement programs addresses the data challenges, as cited by 54% of respondents.

Data quality initiatives: Implement data governance, standardisation, and quality improvement programs to address the data challenges cited by a majority of respondents.

2. Incremental Implementation

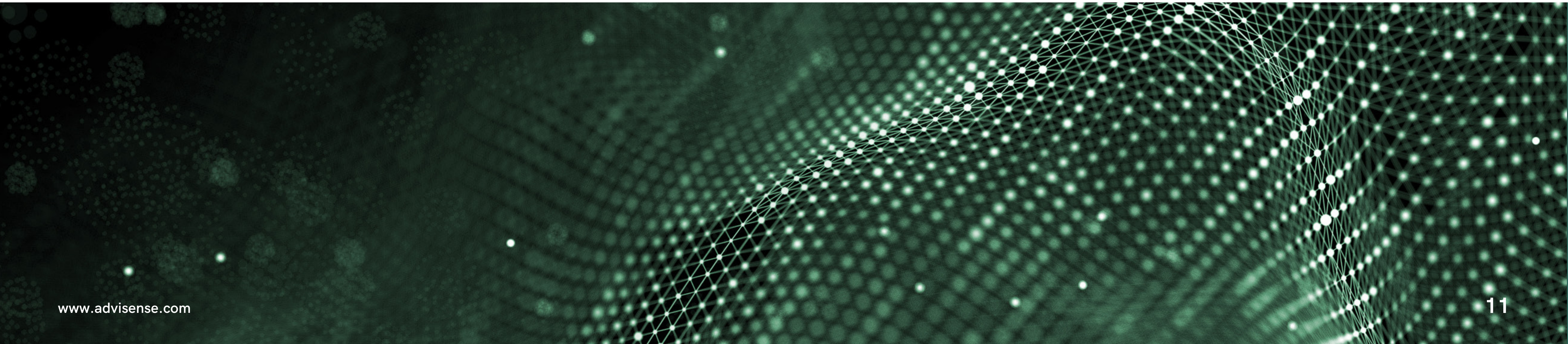
Define, delimit, design. Small wins will make a bigger success in the end. Rather than attempting comprehensive AI transformation, organisations may consider pursuing a phased approach, perhaps starting with high value use cases and focusing initially on transaction monitoring and fraud detection, which are identified by respondents as priority areas. The potential to build on existing processes by enhancing rather than replacing current systems to address integration challenges should not be underestimated. Prioritise initiatives with measurable outcomes to address known pain points and build organisational support:

- Start with high value use cases: Focus initially on transaction monitoring and fraud detection, the top areas identified by most respondents.
- Build on existing processes: Enhance rather than replace current systems to address integration challenges.
- Demonstrable results: Prioritise initiatives with measurable outcomes to address known pain points and build organisational support

3. Collaboration and Engagement Will Count

To address regulatory uncertainties and concerns, organisations may be encouraged to participate in industry working groups to help shape regulatory expectations, engage with regulators early in the AI implementation process, and develop comprehensive documentation of AI approaches, testing, and governance:

- Industry collaboration: Participate in industry working groups to help shape regulatory expectations.
- Proactive dialogue: Engage with regulators early in the AI implementation process.
- Governance frameworks: Develop and deploy comprehensive documentation of AI approaches, testing, and governance.



4. A Practical Approach

The move from exploring AI to implementing AI across processes will not have to require a massive transformation program. Advisense experience from successful implementations point towards four practical ways how organisations can begin immediately and very practically, each addressing specific gaps identified in our survey.

Executive AI Literacy Programs

You and your leadership team, from board members to middle management, need to understand AI not as a mysterious black box, but as a practical tool with clear capabilities and limitations. Without this understanding, your organisation cannot make informed decisions about investments, risk tolerance, or strategic direction.

Consider establishing a structured 3-6 month program with monthly 2-4 hour sessions. Start by demystifying AI through hands-on "AI Labs" where executives can interact with actual models from your financial crime systems. Show them how a machine learning model flags suspicious transactions, let them adjust parameters and see the results. This tangible experience transforms abstract concepts into concrete understanding.

Your curriculum should cover three core areas:

- **First**, what AI can and cannot do in financial crime prevention - be honest about limitations.
- **Second**, regulatory implications and how to discuss AI with supervisors.
- **Third**, strategic frameworks for evaluating AI investments and measuring success.

Bring in your own data scientists to lead sessions, supplemented by external experts who can share cross-industry perspectives. The goal is creating informed leaders who can ask the right questions and make confident decisions about your AI journey.

Breaking Down Silos Through Simulation

You and your leadership team, from board members to middle management, needs to understand AI not as a mysterious black box, but as a practical tool with clear capabilities and limitations. Without this understanding, our organisation cannot make informed decisions about investments, risk tolerance, or strategic direction.

Breaking down silos between compliance, technology, and business teams requires more than meetings - it requires shared experiences. Design practical simulation exercises where mixed teams work through realistic AI implementation challenges together.
Start with a concrete scenario: Your AI system has identified an unusual pattern of transactions that existing rules would have missed. Bring together 8-10 people from different functions and spend a full day working through the implications. How should the compliance team investigate? What additional data might technology provide? How should the business communicate with affected customers? Use your own anonymised data to make it real. Engage an external facilitator who can challenge assumptions and ensure all voices are heard. Run these simulations quarterly, each time tackling a different challenge-data quality issues, model validation processes, or regulatory reporting requirements. Document the outcomes in practical blueprints that guide actual implementation. After each simulation, participants return to their teams with shared understanding and personal connections that smooth future collaboration.

Regulatory Navigation Workshops

You need a structured approach to regulatory engagement that moves beyond reactive compliance. Organise focused workshops that prepare your organisation for productive dialogue with supervisors about AI initiatives.

Gather your key stakeholders: C-Suit and Tech Management. Over 1-2 intensive days, develop your regulatory engagement strategy. Map out your AI initiatives against known regulatory concerns. Practice explaining complex technical concepts in a language that regulators understand. Prepare demonstration scenarios showing how your AI systems enhance rather than replace human judgment.

Create templates for documenting AI governance, validation procedures, and outcome monitoring. Role-play regulatory meetings, with team members taking turns as sceptical supervisors asking tough questions.

Consider reaching out to peer banks to explore joint workshops that benefit everyone.

Peer Learning Forums

You don't need to solve every challenge alone. Learning from peers - even competitors - on non-competitive technical issues accelerates everyone's progress while reducing individual risk and cost.

Look to successful international models: The UK's Joint Money Laundering Intelligence Taskforce (JMLIT) brings together over 40 financial institutions with law enforcement to share typologies and best practices. Singapore's Association of Banks runs working groups on specific AI applications, sharing technical standards while protecting competitive advantages. The Netherlands has created regulatory sandboxes where banks can test AI innovations together under supervisory guidance.

In Sweden, you could initiate similar collaborations through the Swedish Bankers' Association or Swedish FinTech.

Getting Started

You don't need to launch all four initiatives simultaneously. Assess your organisation's most pressing needs:

- If leadership scepticism blocks progress, start with executive literacy programs.
- If implementation keeps stalling, focus on cross-functional simulations.
- If regulatory concerns dominate, prioritise navigation workshops.
- If you feel isolated in your efforts, champion peer learning forums.

Choose one initiative and commit to a three-month pilot. Measure its impact, refine the approach, and then expand. Each step forward builds momentum for the next, gradually transforming your organisation's ability to leverage AI in the fight against financial crime.

Measurements and Maturity

One of the most common misconceptions we encounter is that governance frameworks restrict AI innovation in financial crime prevention. In reality, well-designed governance enables innovation by providing clarity on acceptable approaches, required documentation, and approval processes. The most effective AI governance frameworks we've helped implement share three key characteristics: they are principle-based rather than prescriptive, they scale requirements based on risk impact, and they evolve alongside technological capabilities.

Organisations that treat governance as a foundational enabler rather than a compliance afterthought can innovate more rapidly while maintaining appropriate risk controls. Effective governance frameworks also facilitate regulatory engagement by demonstrating the organisation's commitment to responsible AI implementation.

To provide a roadmap for progressive advancement, the following roadmap may be proposed to support organisations as they to build capabilities incrementally while addressing foundational challenges.

Advisense Insight

According to the experience of Advisense experts, successful implementations to date have followed a 'targeted capability' approach rather than attempting comprehensive transformation. Such an approach focuses on implementing specific AI capabilities that address well-defined pain points within existing financial crime prevention processes.

For example, implementing behavioural analytics within transaction monitoring for a specific customer segment, or applying network analysis to high-risk banking relationships. These targeted implementations deliver measurable value quickly, build organisational confidence in AI capabilities, and provide valuable learning that can inform broader implementation. By starting with focused use cases where AI can demonstrably outperform existing approaches, organisations build the foundation for wider adoption while avoiding the risks of overly ambitious transformation initiatives."

advisense