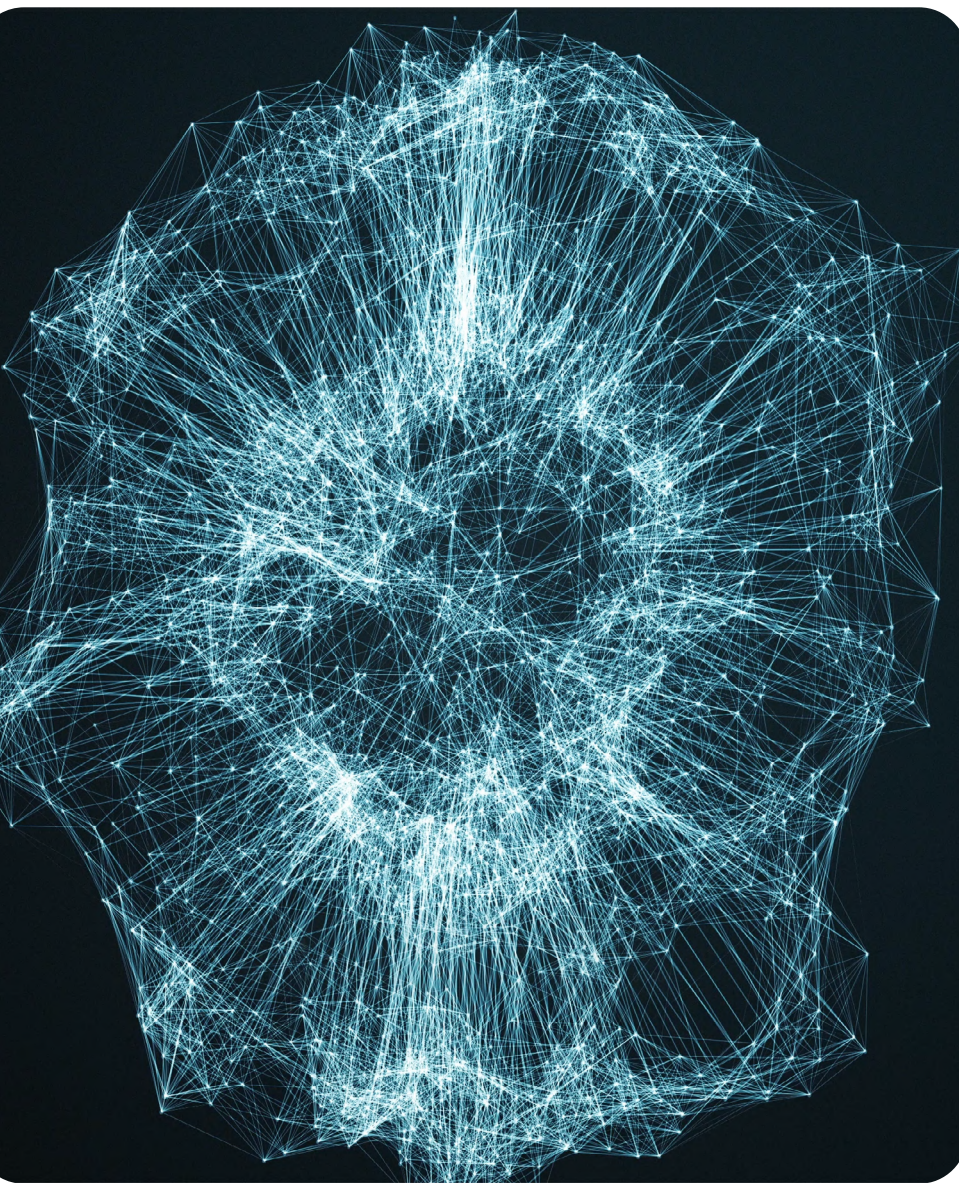
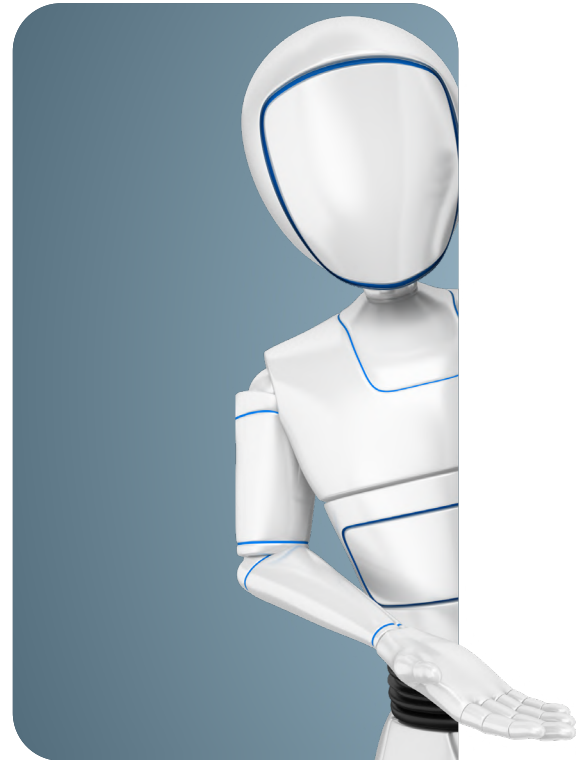


# AI in Anti-Financial Crime:

The State of Adoption in 2025



JUNE  
2025



# Executive Summary

Artificial intelligence (AI) presents opportunities for transformational solutions to many of the world's most pressing challenges. The threat of financial crime, which provides the lifeblood for the illicit economy in which organised crime, terror groups, and other serious criminal actors operate, is no exception.

AI offers new possibilities for the range of critically important anti-financial crime (AFC) and compliance activities undertaken by governments, law enforcement agencies, non-governmental organisations and private sector institutions around the world. From customer due diligence and money laundering risk detection to forensic investigation and asset recovery, the vital processes that defend global societies against financial crime are open to be transformed by new developments in the field of AI.

To understand the nature of the fast-evolving role of AI in AFC and equip organisations to take full advantage of new opportunities, Themis, an illicit finance specialist and trusted research partner to government, law enforcement and the private sector, carried out a survey of CEOs, boards, and executive leadership teams (across industries, in public and private sectors) for our latest report, **AI in Anti-Financial Crime: The State of Adoption in 2025**.

The survey aimed to assess how decision

makers in organisations involved in AFC (across industries, in public and private sectors) are developing strategies and use-cases for AI. We asked nine questions to 74 hand-selected participants. 82% of respondents were senior leaders in their organisations, holding positions as CEOs, founders, owners, directors, board members, heads of compliance and money laundering reporting officers (MLROs). Remaining respondents had roles within their organisations' compliance, operations and finance functions.

Our analysis of participants' responses revealed three key findings:

**Key finding 1: While technology currently presents challenges to organisations, a wave of AI adoption in AFC is imminent**

- **Current Challenges:** Existing technology systems (predominantly non-AI) were seen as a major obstacle to AFC and compliance activities, with 39% of respondents identifying this as a significant challenge.
- **Limited Scale of Implementation:** A substantial 69% of respondents have not yet implemented AI for AFC and compliance. However, those who have adopted AI report a wide range of use cases, including due diligence, know-your-customer (KYC) processes, and investigations.
- **Future Growth:** The adoption of AI in AFC is expected to increase rapidly. 51% of respondents who are not currently using AI plan to acquire it within the next three years.
- **Diverse Use Cases:** The breadth of AI use cases already acknowledged by respondents suggests that AI tools are (or soon will be) available to meet the needs of most organisations. These tools aim to address both internal AFC processes and external challenges such as regulatory changes and evolving threats.

**Key finding 2: Many senior leaders understand how AI can improve and innovate across the range of AFC practices they carry out**

- **Leadership Awareness:** 85% of respondents believe their organisation's senior leadership has at least an intermediate understanding of the risks and opportunities associated

with AI in AFC, with 50% considering senior leaders to understand this somewhat or extremely well.

- **Drivers of Adoption:** AI adoption in AFC is likely to be driven by a desire to improve existing processes and develop new capabilities. The urgency of AI adoption is expected to increase as new types of risks become more prevalent and sophisticated.
- **AI Improves Existing AFC Processes:** Respondents see new AI technology as able to save time and cut costs, with many organisations motivated to adopt AI for AFC to improve the efficiency and effectiveness of their existing AFC and compliance processes.
- **AI Drives AFC Innovation:** Respondents see novel AI tools as essential contributors to their ability to deal with a rapidly evolving risk landscape, with the development of innovative AI-driven AFC capabilities perceived as necessary simply to keep pace with emerging financial crime threats.
- **Wide Range of AI Requirements:** The majority of respondents had clear, developed ideas of how AI could support their organisations' AFC and compliance activity, with areas such as transaction monitoring, behavioural risk assessment, KYC/due diligence/onboarding, data integration, adaptive AI, and document management workflows being seen as priorities for organisations.



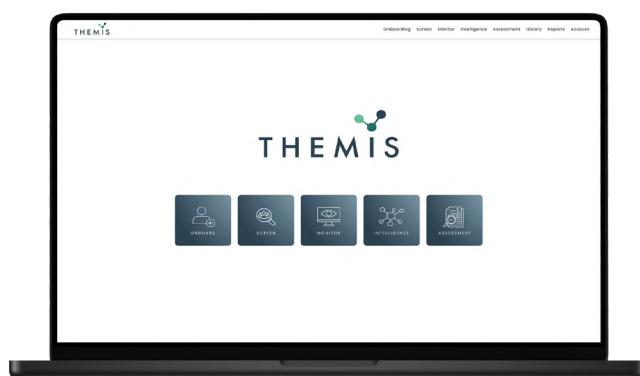
**Key finding 3: While organisations perceive significant barriers to adopting AI for AFC, there are clear pathways to overcoming these**

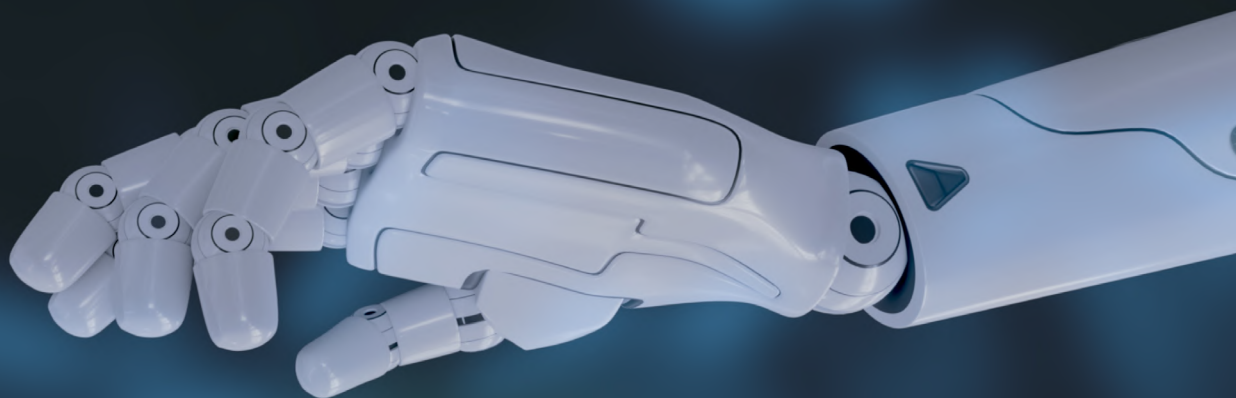
- **Perception of Three Main Categories of Barriers to Adoption:** The barriers to adoption identified by respondents derive from issues inherent in AI technology, an organisation's own approach to and use of AI, and ongoing uncertainty about regulators' approaches to AI in AFC.
- **Issues with AI Technology:** Concerns about reliability and accuracy, privacy and security, and the perceived high costs of AI technology were raised by respondents. In addition, over 30% of respondents indicated that there is currently a lack of suitable AI products that they are aware of.
- **Obstacles within Organisations:** Gaps in organisations' staff's knowledge about AI technology and its capabilities were seen as a significant obstacle to AI adoption, with 45% of respondents highlighting this issue. This contrasted with perceptions that senior leaders had high levels of AI familiarity. This concern was more pronounced than the issue of internal scepticism towards AI, which was identified by only 16% of respondents as a concern. Both adoption and implementation of AI in AFC are limited by knowledge deficiencies.
- **Regulatory Uncertainty:** Over a third of respondents selected 'uncertainty about regulators' views' as a chief obstacle to adopting AI. However, with at least 75% of respondents aiming to adopt AI within five years, and regulation fast developing, there is large potential for uptake within a time when the regulatory landscape will be clearer.

- **Barriers Able to Be Overcome:** While some of the larger challenges to AI are expected to remain for the long term, they are not fundamental barriers to adoption. Processes of knowledge building and engagement around AI development will be key to helping organisations overcome internal and external barriers to adoption they face.

From these findings, Themis has developed six key recommendations for organisations seeking to leverage AI opportunities for their own AFC and compliance practices; we set these out in the conclusion to this report.

The next one to three years present a critical window for the development of AI in AFC. The opportunities open to organisations are clear and are well understood by many senior leaders. Although significant barriers to adoption remain, efforts to build organisational capacity can largely overcome many of these. **Now is the time for organisations involved in AFC to move from recognition to action – ensuring readiness for the AI-enabled future that lies ahead.**





# Table of Contents

Executive Summary	2
Glossary	7
Background	8
Methodology	9
Key Finding 1 – While technology currently presents challenges to organisations, a wave of AI adoption in AFC is imminent	12
Key Finding 2 – Many senior leaders understand how AI can improve and innovate across the range of AFC practices they carry out	17
Key Finding 3 – While organisations perceive significant barriers to adopt AI for AFC, there are clear pathways to overcoming these	23
Conclusion – While challenges remain, AI’s transformative potential for anti-financial crime is fast becoming reality	28
Recommendations	29
How Themis Uses AI	31
Themis UK Research and Innovation Grant Project	32
About Themis	34
Appendix: Overview of results	36
Get in Touch	51

# Glossary

In this report, we use several key terms and acronyms. Although some of these terms have a variety of possible meanings, for the purposes of this report we define them as follows:

**Anti-financial crime (AFC)** – *AFC* refers to the broad range of activities implemented to prevent and combat financial crimes such as money laundering, fraud, bribery, corruption, and terrorist financing. Depending on the nature of a particular organisation, AFC practices may include activities such as monitoring transactions for money laundering, analysing and disseminating financial intelligence related to suspicious activity, or implementing customer due diligence measures.

**Artificial intelligence (AI)** – *AI* refers to algorithm-based technologies that can perform tasks that traditionally required the input of human thought and intervention. We use AI as an umbrella term covering a number of different types of technology, some of which are mentioned separately in this report.

**Compliance** – *Compliance* refers to the policies, procedures, and practices that organisations implement to adhere to legal and regulatory requirements aimed at preventing and detecting financial crimes. In this report, compliance is limited to activity carried out

to adhere to legal obligations concerning financial crime; it does not refer to activity organisations undertake to comply with other areas of regulation.

**Organisation** – *Organisation* refers very broadly to institutions involved, in various ways, in AFC activity, including public bodies, private companies, and non-governmental/non-profit organisations. In the public sector, organisations include entities such as supervisory authorities and law enforcement agencies, while private sector organisations include entities such as financial institutions, and designated non-financial businesses and professions ([as defined by the Financial Action Task Force](#)), e.g. law firms, accountants and real estate firms.

**Respondent** – *Respondent* refers to the 74 individuals who participated in this research by completing our nine-question survey. Responses from these participants are the primary data source for this report.

# Background

The past few years have seen an explosion in the prominence of AI in discussions about the future of societies and economies around the world. From [transforming the way in which warfare is conducted](#) to [revolutionising healthcare](#), there are vanishingly few contemporary challenges for which AI solutions have not been proposed.

The threat posed to businesses, countries and communities by the illicit economy, which provides the lifeblood for organised crime, terror groups, and [other serious criminal actors](#), is no exception. **AI has been widely described as offering new opportunities for the fight against financial crime, promising to deliver new capabilities to both public and private sector practitioners.**

Analysis of the effectiveness of current anti-financial crime (AFC) efforts makes clear that there is ample scope for improving how we address financial crime threats. Although increasing resources are invested by businesses to detect and prevent illicit financial activity, a [2023 Europol](#) report estimated that under 2% of organised crime proceeds are recovered every year. Put another way, the [estimated \\$85 billion](#) spent on financial crime compliance in the EMEA region each year yields a return of under \$5 billion in recovered criminal assets. Other regions may have even less success –

[global evaluations](#) of asset recovery suggest that around 1% of global illicit financial flows are recovered.

It is hard to conclude that the current suite of legacy AFC systems are delivering value for money. **AI's potential to [revolutionise the data processes](#) underpinning these systems therefore represents a momentous opportunity for improvement.** However, the question of exactly how the full potential of AI will be realised in AFC remains unclear. If we want to see genuine improvements in effectiveness rather than simply increases in compliance costs, it is critical that the direction of AI developments is shaped by financial crime subject matter experts and practitioners – those who best understand what their organisations need from new technology.

In response to this uncertainty, **Themis has conducted latest survey, AI in Anti-Financial Crime: The State of Adoption in 2025. The**



**survey aims to understand how CEOs, Boards & Executive Leadership teams (across industries, in public and private sectors) are approaching the evolving role of AI in AFC.** This initiative aimed to evaluate the current rate of adoption of AI, uncover specific organisational needs in this domain, and identify emerging trends that will shape the future of the use of AI in AFC practices.

By equipping senior leaders with the knowledge of how their peers and counterparts in other sectors are approaching AI in AFC, Themis aims to empower organisations to adopt new and innovative AI solutions that truly make a difference in the fight against financial crime.

## Methodology

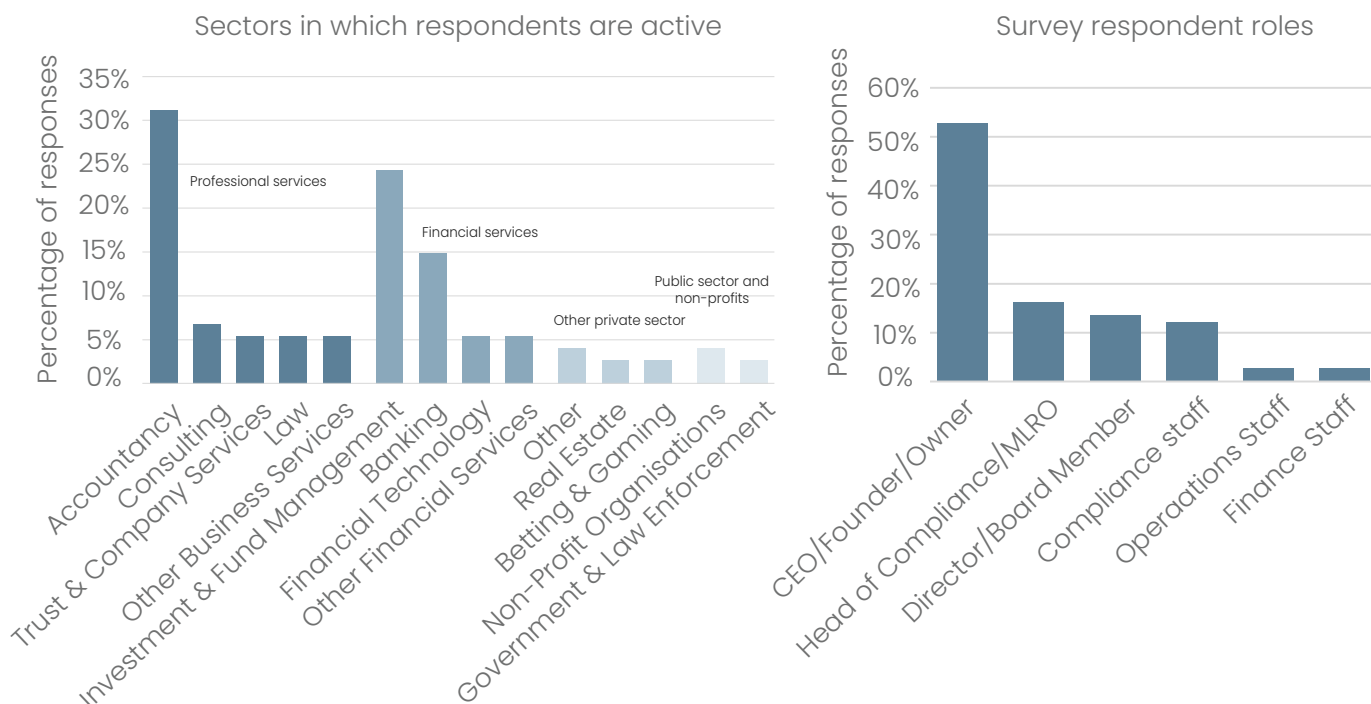
There is **great variety among the range of organisations which engage in AFC and compliance, given their vastly differing jurisdictions, sectors and organisational natures,** presenting a challenge for any attempt to produce a general analysis of AI's role in AFC. This research did not attempt to comprehensively capture this variety, but rather focussed on gathering richer, detailed data from a smaller sample of senior decision-makers.

While these data cannot, therefore, be considered representative of the entire AFC landscape, they aim to offer a view of how key individuals setting strategic direction for their organisations are approaching the development and application of AI for their AFC functions.

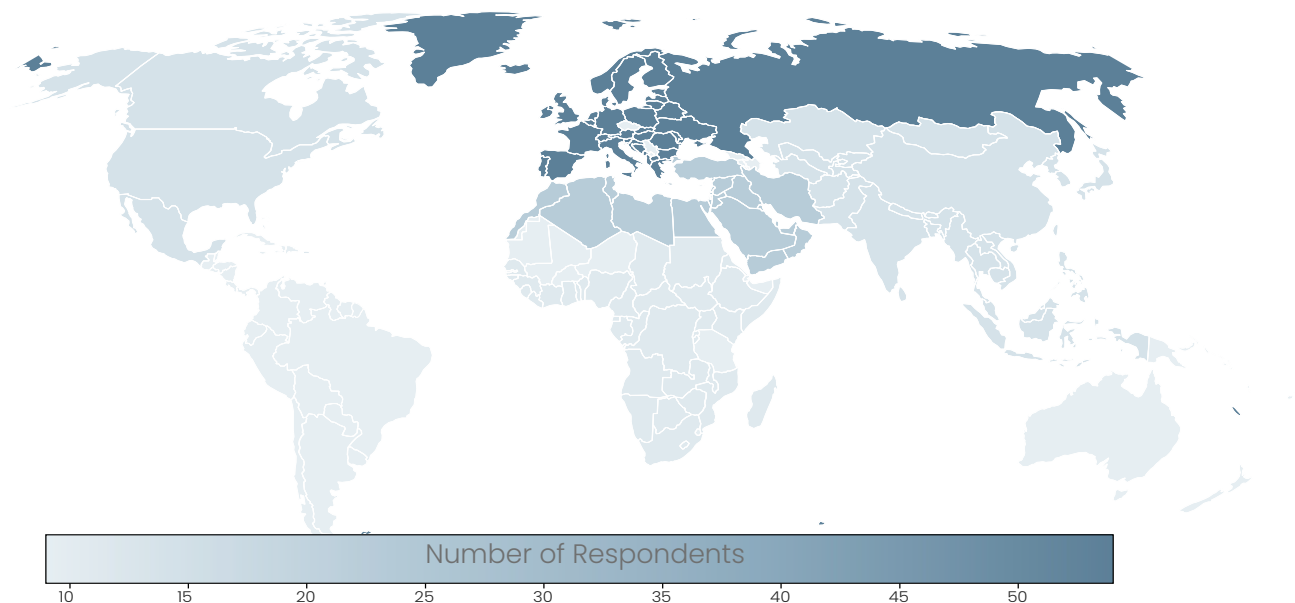
Senior leader perspectives were gathered from a wide range of organisations involved in AFC activity across different jurisdictions. **While**

**both public and private sectors were targeted for participation, businesses (both financial and non-financial) made up the vast majority of our research sample.** Respondents were accessed through our network of financial crime and compliance leaders, and through the generous collaboration of the International Accountants' Association, UK Finance, and the Arab Bankers' Association, which disseminated the survey to their members.

**The survey ran from October 2024 until February 2025.** We asked all respondents three qualification questions to determine the sectors and jurisdictions in which their organisations operate, and to determine their roles. The survey received 93 responses, of which 19 were incomplete, leaving **a final total of 74 complete responses.** The respondent profile of the complete sample is given in the figures below:



Respondent organisations' regions of activity



The survey completed by respondents consisted of nine questions, comprising both multiple-choice and open-ended answer formats. For most multiple-choice questions, an 'Other' option with open text entry field was included, to allow for participant-led responses where answer options did not reflect their views.

The nine questions were:

01

What are the major challenges your organisation faces in its anti-financial crime and compliance practice?

02

For what purposes within anti-financial crime and compliance practice does your organisation currently use AI technology?

03

In what timeframe do you think your organisation is likely to acquire new AI technology in anti-financial crime and compliance?

04

What are the major reasons you would consider procuring new AI technology for your organisation's anti-financial crime and compliance practice?

05

If you could commission a bespoke AI product to help your anti-financial crime and compliance practice, what would you request?

06

How well does your organisation's senior leadership understand the risks and opportunities that AI might bring for your anti-financial crime and compliance practice?

07

What are the major reasons you would consider procuring new AI technology for your organisation's anti-financial crime and compliance practice?

08

If you could commission a bespoke AI product to help your anti-financial crime and compliance practice, what would you request?

09

How well does your organisation's senior leadership understand the risks and opportunities that AI might bring for your anti-financial crime and compliance practice?

We then analysed all responses, identifying three broad themes – our *Key Findings*. This analysis was used to formulate several recommendations for organisations approaching AI in AFC; these are included in the *Conclusion*. Brief individual analyses of responses to each question are given in the appendix *Overview of Results*.

The analysis contained within this report has been produced by Themis, an illicit finance specialist and trusted research partner to government, law enforcement, non-governmental organisations and the private sector. This report has not been written as an academic study but rather **aims to provide survey respondents and other readers with a practical knowledge resource they can use to enhance their organisation's efforts to combat financial crime.**

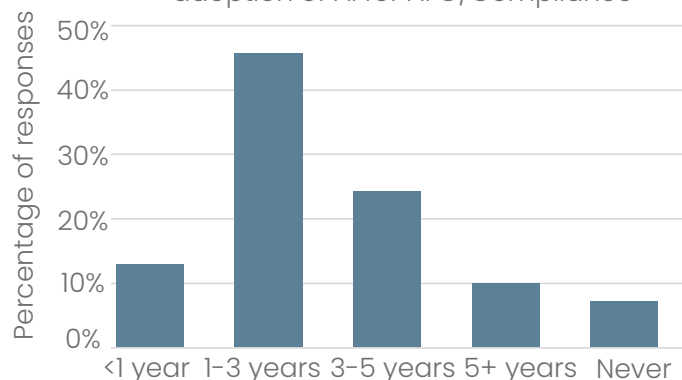
## Key Finding 1

While technology currently presents challenges to organisations, a wave of AI adoption in AFC is imminent

The first key finding concerns the present and future role of technology in AFC and compliance. Although the purpose of technology is to support and enable organisations to implement more effective AFC processes, survey data suggest that, for a significant portion of organisations, legacy technology currently does not achieve this, with **39% of respondents even considering technology to be a major obstacle to their work.**



Respondents' timelines for organisational adoption of AI for AFC/Compliance



Indeed, the survey results suggest that the usage of AI applications in AFC will increase significantly over the next five years, with over 80% of respondents planning to do so within the next five years.

AI, therefore, appears to have the potential to transform the long-established role of technology in AFC and compliance. This section analyses the status quo of technology's role in AFC, identifying areas in which AI is already being used and areas where its further implementation may be able to effect positive change.

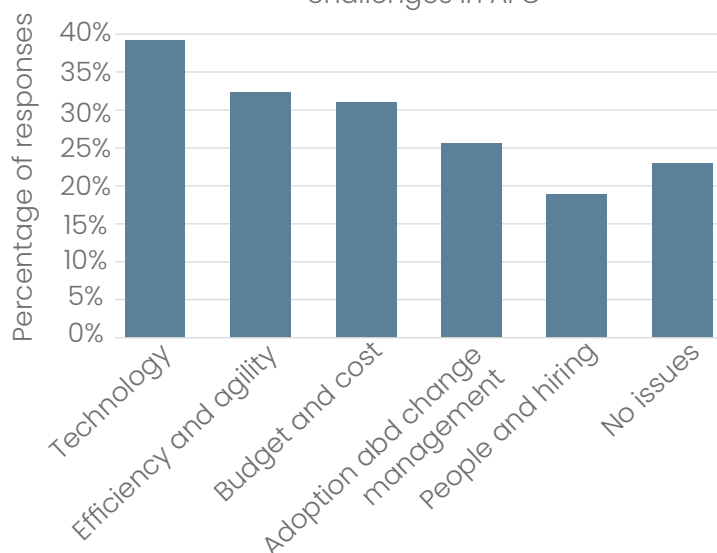
**The most common 'major challenge' faced by organisations was technology** – a result that is both striking and challenging. In theory, [the only reason technology exists for AFC and compliance is to act as an enabler for organisations](#), removing or at least mitigating the challenges they face from criminal threats and/or regulatory obligations. Yet over a third of respondents found legacy technology systems to play the opposite role, presenting a significant challenge.

According to respondents, AI plays a limited role within their current usage of AFC and compliance technology, with 69% of respondents not currently using AI for these purposes. This appears set to change rapidly in the next few years; **51% of respondents not currently using AI stated that they will acquire AI within the next three years.**

*Technology currently presents a challenge to many organisations' AFC and compliance activity*

The first question we asked in this survey aimed to assess the landscape of challenges faced by organisations carrying out AFC activity, to establish the areas in which AI might present opportunities for solutions. The vast majority of respondents identified major challenges: only 23% of respondents reported that they had "no issues" in their AFC and compliance practices.

Respondent organisations' biggest challenges in AFC



But what is the nature of that challenge? The other obstacles highlighted by respondents offer some indication, with **key difficulties faced by organisations including efficiency (32% of respondents), costs (31% of respondents) and change management (26% of respondents)**. These challenges chiefly relate to deficiencies in the efficiency and effectiveness of intra-organisation AFC processes (e.g. initial due diligence and risk assessment of new customers).

Other challenges of AFC raised by respondents appear to some extent to transcend organisations' power to directly resolve them; for example, people and hiring challenges (faced by 19% of respondents) may be driven by wider market shortages of qualified staff, with [2022 research](#) finding that "two-thirds (67%) of firms said they expect the cost of senior compliance officers to increase due to the competitive labour market and skills shortages". Issues around changing regulation and the rapidly evolving threat environment are driven by large-scale global processes over which individual organisations have limited influence, as the [US Treasury's decision to end enforcement](#) of the US business ownership register (created under the Biden administration) demonstrated.

While no organisation may expect to fully remove all challenges they face in carrying out AFC and compliance activity, many go to great lengths to mitigate the internal process-related difficulties they encounter, a fact underlined by the significant amounts [the global private sector spends on financial crime compliance](#). The implementation of technology solutions would in theory offer an effective way to achieve efficiency improvements, but the reality appears to be that, for many organisations, the

use of outdated legacy systems means that technology's effectiveness remains limited.

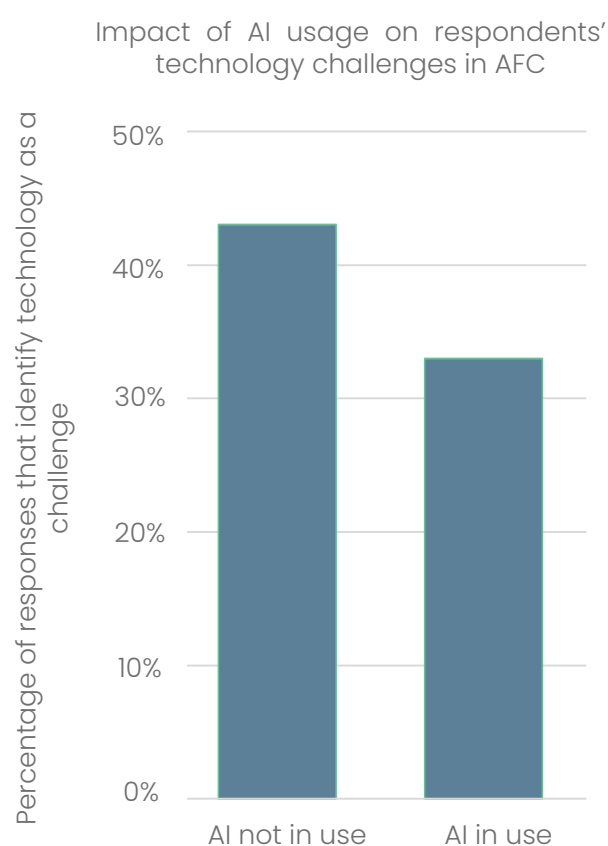
This presents an opportunity for new AI solutions, given that a variety of technology-related challenges remain unresolved, but it also presents a warning. **Previous cycles of technology development have aimed to address AFC and compliance challenges, but limited success in doing so has resulted in cases where technology has become a major AFC and compliance challenge in its own right.** In 2024, [Metro Bank was fined £16 million](#) by the Financial Conduct Authority for anti-money laundering failures 'attributed to a software error'. It is essential that AI developments do not repeat the mistakes of past cycles of technology innovation in AFC.



## How is AI already being used?

That **many organisations have not yet implemented AI in AFC and compliance (69% of respondents)** means that the nature of its impact is largely undetermined. An early assessment can, however, be gained by analysing the responses of organisations that have embarked upon AI implementation.

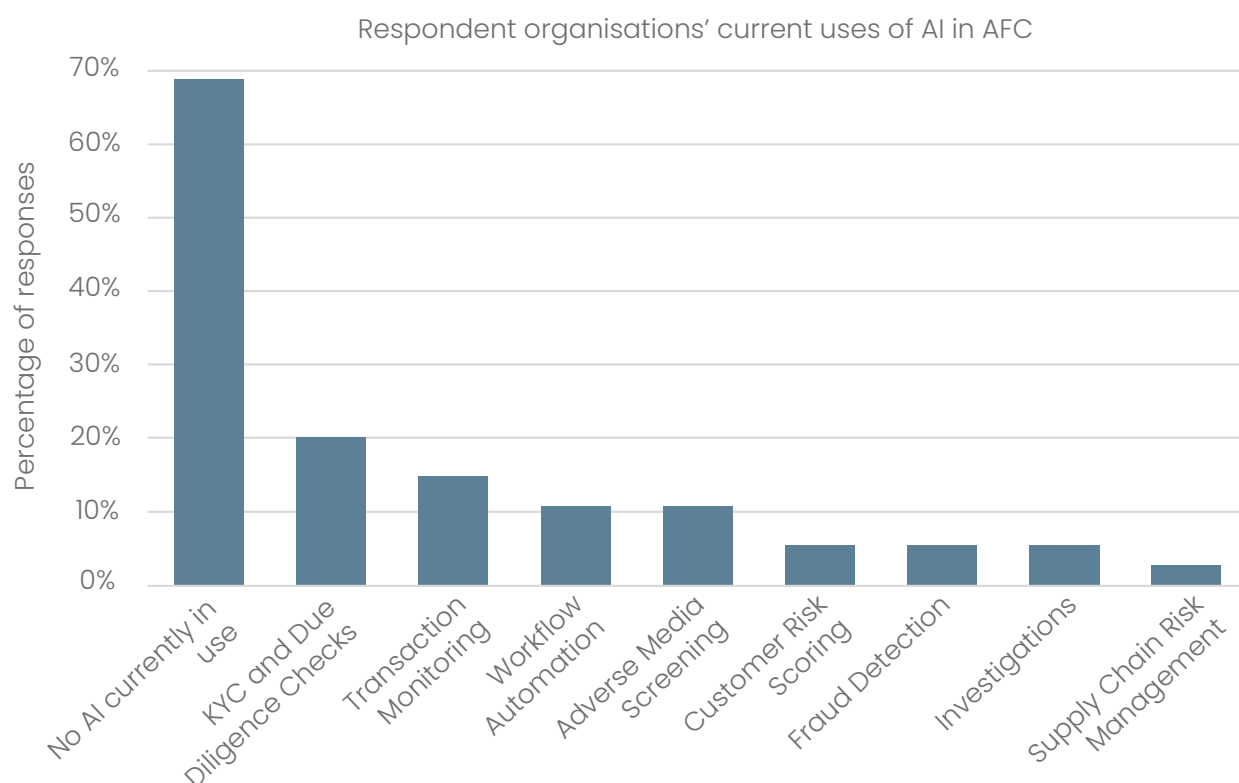
Survey data suggest some degree of connection between AI implementation and reduced technology challenges in AFC and compliance. As seen in the figure here, **organisations that currently utilise AI in AFC are less likely to view technology as an obstacle.**



The wide range of AI use cases highlighted by respondents supports the notion that organisations can use the technology to successfully address challenges. Respondents stated use of AI in eight separate categories of activity that cover the full range of AFC and compliance processes (KYC and Due Diligence Checks, Transaction Monitoring, Workflow Automation, Adverse Media Screening, Customer Risk Scoring, Fraud Detection, Investigations, Supply Chain Risk Management). 'Other' responses included usage of AI for operations and communications functions, as well as other document analysis and research purposes.

These responses suggest, therefore, that **while AI may not currently be used very widely in AFC and compliance, it is being used in a rich variety of ways, with AI tools already in use for a diverse set of different processes across AFC practices.** This suggests that

future implementation of AI has the potential to be carried out broadly, across different areas of organisations, rather than narrowly, in a limited domain of activity; indeed, this 'cross-functional' model of AI implementation was [described in the Harvard Business Review in 2019](#) as a key method to achieving the biggest impact from an organisation's adoption of AI.



## What is the forecast for future AI implementation?

The limited use of AI in AFC and compliance appears set to change rapidly. Survey results suggest that subsequent years should see a sharp growth in AI adoption, with 51% of respondents not currently using AI stating that they will acquire it within the next three years. This prediction of an imminent spike in adoption indicates that **AI implementation in AFC may replicate recent trends in other areas of the economy, where AI usage has increased rapidly year-on-year**. McKinsey's 2025 State of AI report illustrated this, [finding that 78%](#) of organisations globally use AI in at least one business function, up from 72% in 2024 and 55% earlier.

Moreover, the breadth of AI use cases already acknowledged by respondents suggests that there are, or soon will be, AI tools that suit the needs of most organisations. The key challenges these tools will seek to address are both the

internal processes of AFC and compliance, especially the difficulties organisations face around technology, and the external challenges of regulatory changes and an ever-evolving threat landscape.

To conclude, we are in a key developmental phase for AI in AFC. While AI tools are already being implemented to some extent to address organisations' longstanding AFC challenges, survey data suggest that a major wave of adoption is set to occur in the next three years, with implementation across a large majority of organisations likely in five to ten years from now. The present moment is thus a crucial opportunity to direct the trajectory of AI development, avoiding the flaws of previous waves of technology development for AFC to deliver truly transformative change.

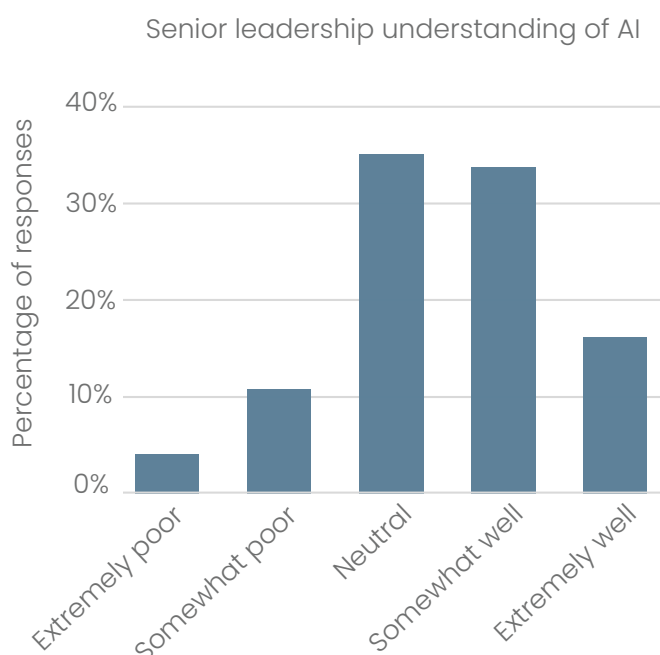


## Key Finding 2

Many senior leaders understand how AI can improve and innovate across the range of AFC practices they carry out

The second key finding we identified concerns how organisations are looking to AI solutions to support their AFC and compliance work. The demands of senior leaders in the market will majorly influence how AI technology companies develop new products, playing a pivotal role in shaping the future trajectory of AI development in the field of AFC overall.

The survey aimed to understand these demands in detail; to identify what AFC leaders are seeking to gain from AI, and why. In order to qualify leaders' perspectives on AI, we aimed to assess the levels of understanding senior leaders have of the risks and opportunities of AI for AFC and compliance.



The results found that organisations' leadership generally has at least an adequate, and often highly developed, understanding of the implications of AI. In fact, more respondents considered senior leadership to have an extremely good understanding of AI in AFC (16%) than those who considered them to have a somewhat or extremely poor understanding (15%).

Given that the majority of these responses represent senior leadership self-reporting, they must be treated with an element of caution, but, at the very least, they do suggest that **consideration of AI in AFC is an active area of discussion and strategic**

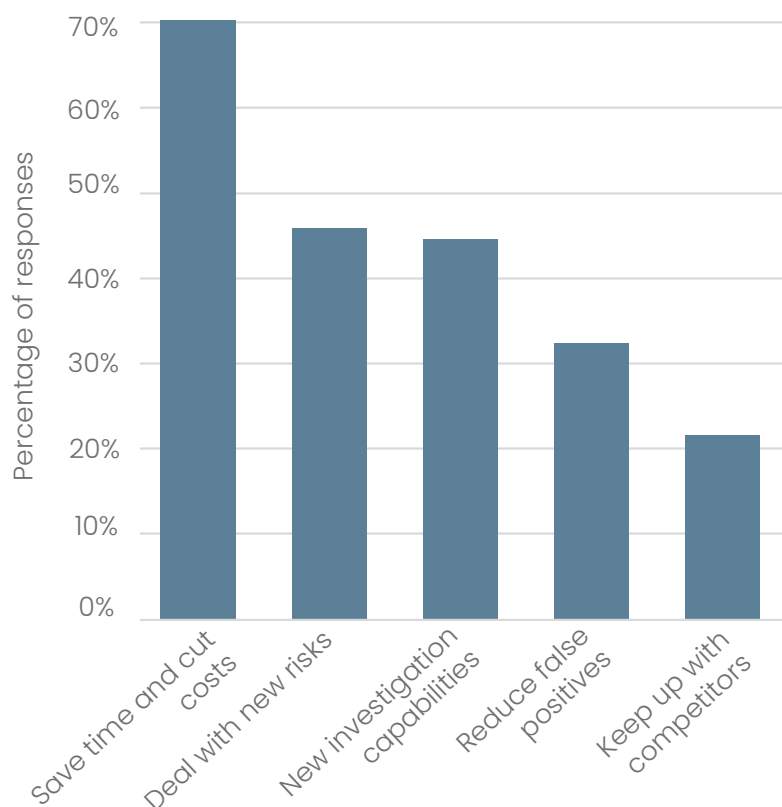
**thinking across many organisations** (heightened interest may in part be driven by the increasing complexity of financial crime threats, alongside [mounting regulatory expectations](#)). This suggestion is reinforced by the range and depth of sophistication in many responses to survey questions about what organisations are looking to gain from new AI applications in AFC.

This key finding summarises the essential themes regarding what types of capability AFC leaders are seeking to gain from AI, and why. Although a number of those surveyed were unclear about their aspirations for new AI tools (for example, 31% of respondents were unsure about what type of AI tool they would ideally commission), the large majority of those surveyed had detailed conceptions of what an AI-enabled future for their AFC and compliance activity could and should look like.

## What reasons drive the adoption of AI for AFC?

By a significant margin, the most common reason respondents gave for why they would procure new AI technology was "to save time and cut costs". By incorporating other common responses, such as the desire to reduce the number of false positive risk alerts, we can summarise one category of motivation for adopting AI for AFC as the desire to improve the efficiency and effectiveness in existing AFC and compliance processes. **Leaders see AI as presenting the opportunity to develop cheaper and better solutions to the existing challenges they face, in particular the significant challenges they face from outdated legacy technology.**

Respondent organisations' reasons for procuring new AI technology for AFC

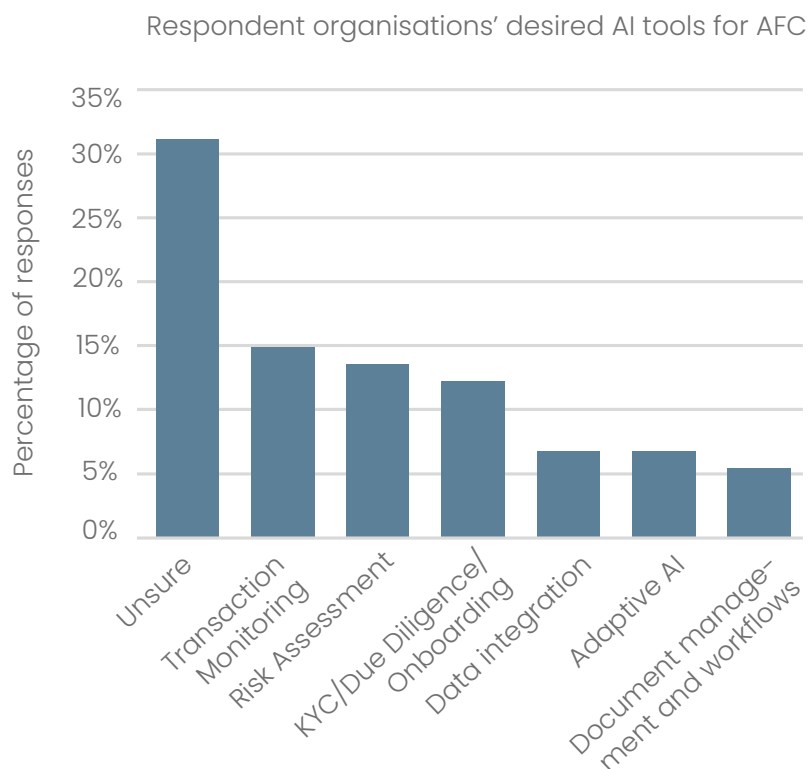


Another category of response, however, related to the development of entirely new capabilities in investigation/analysis – innovation rather than improvement. Notably, the desire for new capabilities appears to be driven by an understanding of a rapidly evolving risk landscape; the second most common reason for procuring new AI technology was “to deal with new types of risk”. These types of response suggest that there is both a desire for AI to be a game-changing enabler of AFC innovation, and an understanding that this type of paradigm-shifting technology development may be necessary simply to keep pace with financial crime threats (particularly AI-enabled criminality).

**Adoption of AI in AFC will, therefore, likely be driven by a mixture of a desire to improve existing processes and a need to develop new capabilities.** Although the procurement of AI was most commonly seen by respondents as of medium priority to their organisations, the moderate urgency of AI adoption will likely be greatly increased as the “new types of risk” participants identified as a motivating factor become more prevalent and sophisticated.

Themis has been tracking how the threat of new forms of financial crime, enabled by AI and other emerging technologies, has grown in scale over the last five years. In [2023 research](#) carried out in partnership with the UAE’s Executive Office of Anti-Money Laundering and Counter Terrorism Financing (EO AML/CTF) and Abu Dhabi Global Market (ADGM), Themis analysed how criminals were exploiting generative AI chatbots, synthetic identities, decentralised finance services and other evolving tech trends; our [2025 assessment of fraud trends](#) confirmed this, finding that many of the fastest-growing threats are likely to be AI-powered.

## What types of AI tools are organisations seeking for AFC?



An analysis of respondents' views on the ideal AI tool they would commission reveals some key qualities that would render AI of particular value to surveyed organisations' AFC and compliance activity. Although many respondents were unsure what AI tools they would commission, **a large majority (69%) had clear, practical ideas for new AI-driven systems their organisation could benefit from.**

### REAL-TIME

Tools which are constantly updated, such that they are accurate in real-time, were seen to be of value in both regulatory compliance and financial crime detection/mitigation activity. It is critical to any organisation involved in AFC and compliance to have access to fully up-to-date information, whether that be regulatory information (e.g. lists of sanctioned entities) or threat understanding (e.g. suspicious activity typologies). Time lags in updating systems present vulnerabilities which criminal actors can exploit; AI tools which carry out these processes such that they occur in real time offer organisations vast potential value.

### INTEGRATED

The integration of AI tools with existing systems and data sources was seen as crucial. Respondents emphasised the importance of seamless integration to ensure that AI solutions can work effectively within their current technological infrastructure. Integrated AI systems can leverage data from multiple sources, providing a comprehensive view of financial activities and enabling more accurate risk assessments. This integration would also facilitates better communication and coordination across different departments and systems within an organisation.



#### ADAPTABLE

Similarly, respondents saw tools which can be adapted for changing business requirements and a shifting risk landscape as holding crucial value for their AFC activity. The ability to customise AI tools to meet evolving regulatory demands and specific organisational needs was highlighted as a significant advantage. Adaptable AI systems can be tailored to address unique challenges faced by different sectors, ensuring that they remain relevant and effective over time.

#### AUTOMATED

Automation was a key feature desired by respondents, particularly for repetitive and time-consuming tasks such as transaction monitoring, KYC processes, and report generation. Automated AI tools can significantly reduce the manual workload, allowing compliance teams to focus on more strategic activities. By automating routine tasks, organisations can improve efficiency, reduce human error, and ensure consistent application of compliance protocols.

#### HIGHLY SPECIFIED

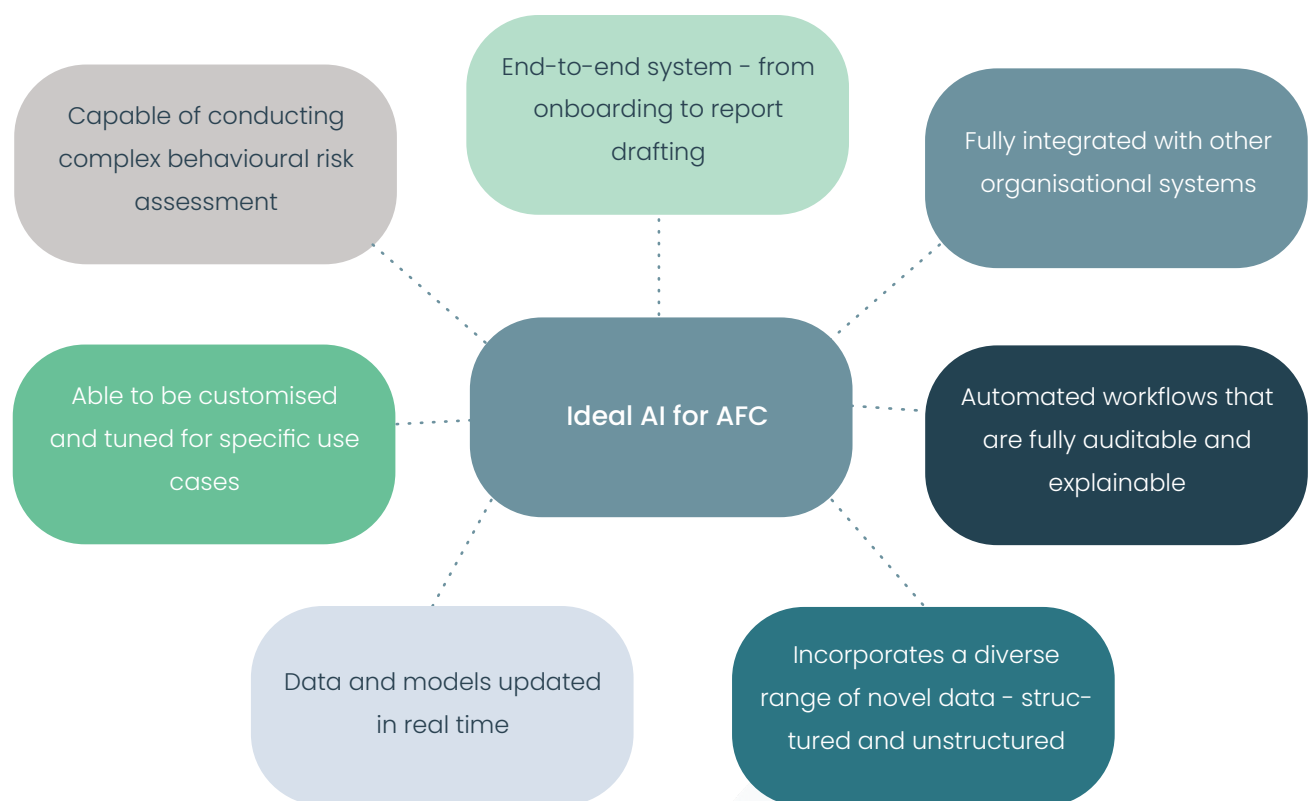
Respondents expressed a need for AI tools that are highly specified to their particular industry and regulatory environment. This includes tools designed to handle specific types of financial crime, as well as individual predicate crime types such as illegal logging. Specified AI systems can provide more accurate and relevant insights, enhancing the effectiveness of AFC measures. These tools would be required to be developed with a deep understanding of the nuances and complexities of different financial crime scenarios, making them more effective in identifying and mitigating risks.

#### AUDITABLE/EXPLAINABLE

Transparency and explainability were critical concerns for respondents. AI tools must be auditable and provide clear explanations for their decisions and actions. This is particularly important in the context of regulatory compliance, where organisations need to demonstrate that their AI systems are making decisions based on sound logic and data. Explainable AI helps build trust among stakeholders, including regulators, by providing insights into how decisions are made and ensuring that AI-driven processes are transparent and accountable.

## What could an ideal future AI – enabled AFC and compliance system look like?

By amalgamating various participant responses, we can put forward a composite description of what an ideal AI-powered AFC and compliance system could look like:

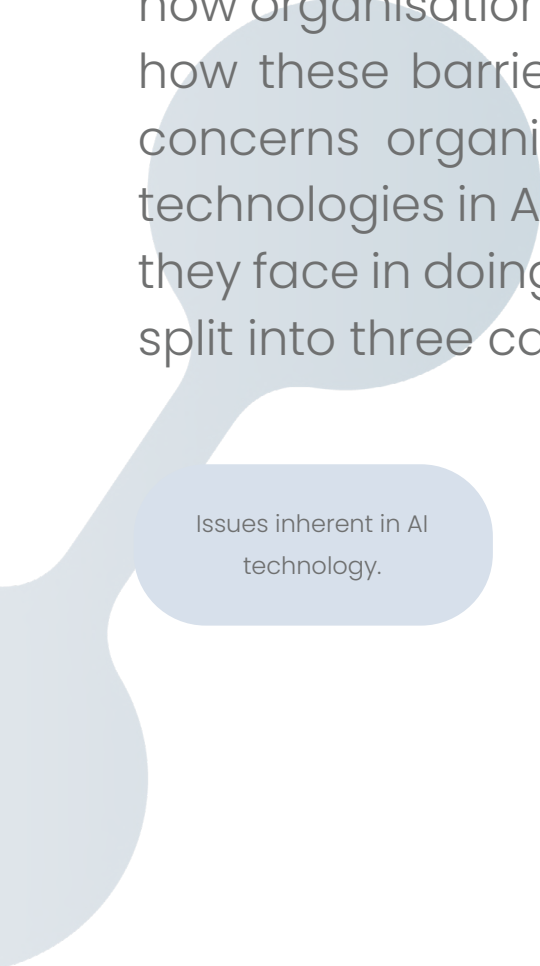


Ideal systems like this would cover the full scope of AFC and compliance processes – addressing organisations’ desires to improve existing capabilities and their need to develop new capabilities, confronted by a rapidly shifting threat environment.

## Key Finding 3

While organisations perceive significant barriers to adopt AI for AFC, there are clear pathways to overcoming these

The third and final key finding we identified related to how organisations perceive barriers to AI adoption, and how these barriers can be overcome. Issues included concerns organisations have about implementing AI technologies in AFC and compliance, and the obstacles they face in doing so. Broadly, perceived barriers can be split into three categories:



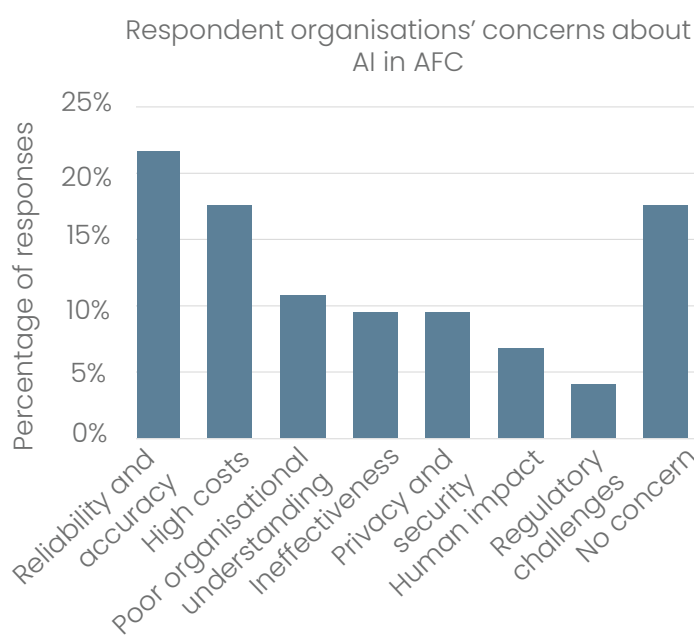
Issues inherent in AI technology.

Organisations' own approach to and use of AI.

Regulatory concerns, particularly ongoing uncertainty about regulators' approaches to AI in AFC.

This key finding discusses how and why organisations perceive obstacles to new implementation of AI in AFC and compliance, identifying some ways in which they can be overcome, by organisations responsible for AFC and by their partners in AI technology development. While the issues identified by respondents may not be universally seen as challenges (for example, regulatory concerns, as we discuss below, may appear to some as more severe than they actually are), understanding and removing barriers are key steps that organisations must take to achieve AI breakthroughs.

## Barriers to adoption inherent in AI technology



The most significant concern respondents had regarding AI tools for AFC and compliance purposes concerned reliability and accuracy. Given the serious and highly sensitive nature of many AFC processes, ensuring rigorous consistency in AI reasoning is a crucial issue. **Organisations need to be able to implement AI with full trust in its outputs, but the process of building confidence may not be straightforward;** as one respondent stated, some organisations have fears around “rapidly becoming reliant on something that may give us a false sense of security”.

Very closely linked to this were concerns over privacy and security, with data privacy and robust security measures highlighted by several respondents as critical requirements for any AI implementation in AFC and compliance. Concerns around security and privacy are unsurprising when discussing AI in AFC; whether an organisation is involved in handling sensitive personally identifiable information, building a chain of evidence in a criminal investigation, or transferring intelligence (e.g. through suspicious activity reporting), secure and confidential processes are essential.

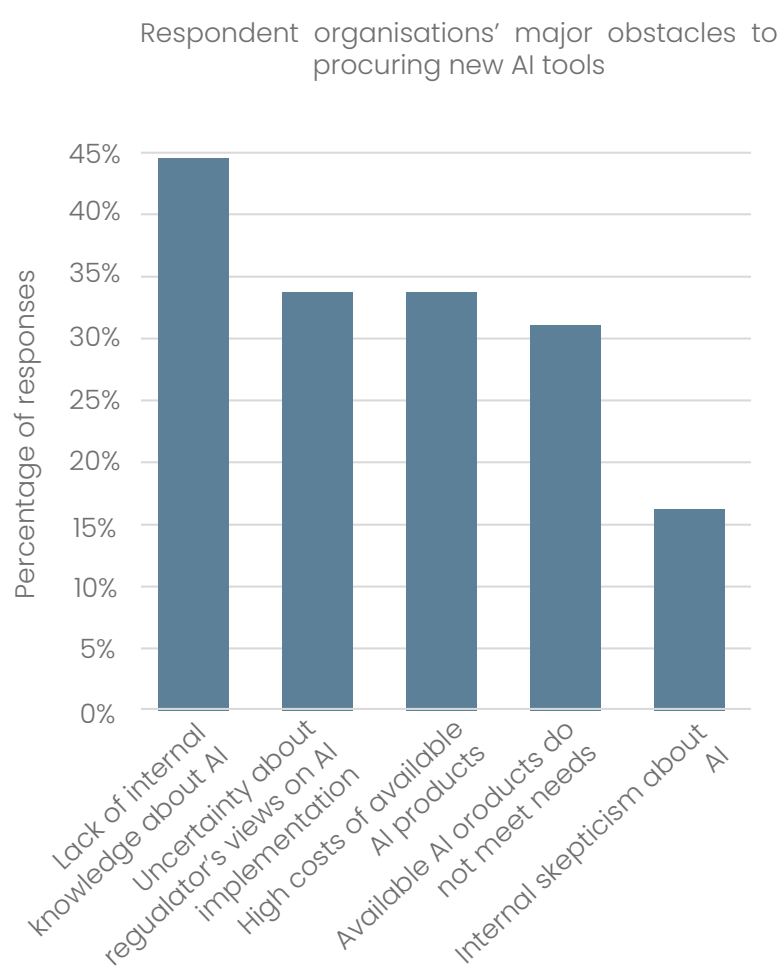
The second most significant concern raised by survey respondents was the perception that

AI applications in AFC will entail high costs for their organisation; high costs were also seen by a third of participants as a major obstacle to their procurement of new AI. Some respondents expressed doubts that the costs of new AI technology would be justified by the benefits; one individual asked the question whether AI in AFC would be a “costly sledgehammer to crack a nut”. It must be noted that this contrasts with much research, such as [a 2024 white paper published by academics at the University of Strathclyde](#), that has found that AI can deliver “greater efficiency at reduced costs” for organisations’ financial crime risk management.



The corollary of concerns about costs was the perception that current AI technologies do not present sufficient specific use cases to organisations. Over 30% of survey respondents said that the unavailability of suitable products was an obstacle to adopting AI technology. This suggests that the **respondents would consider using AI if they knew that the products available were suited to their specific organisational needs**, an idea reinforced by data showing that **more than two-thirds of these respondents were prepared to adopt AI in less than five years**.

## Barriers to adoption within organisations



One of the most significant barriers to the adoption of AI within organisations was perceived to be a lack of internal knowledge, with 45% of respondents highlighting this as a major obstacle to their procurement of new AI technology. This issue is notably far more pronounced than that of internal scepticism, which was identified by only 16% of respondents as a major obstacle, indicating that **while organisations may recognise the potential benefits of AI, they may lack the expertise to identify, implement and manage these technologies effectively**. This gap in knowledge can impede the integration of AI into AFC practices, limiting the technology's potential to enhance compliance and risk management processes.

Knowledge gaps play into another significant concern highlighted by the survey, namely the potential for **over-reliance** on AI. While AI can greatly enhance AFC processes, respondents identified a risk that organisations may become too dependent on automated systems, neglecting the critical role of human judgement and oversight. Over-reliance on AI can lead to complacency, where the outputs of AI systems are accepted without sufficient scrutiny. This can be particularly problematic in AFC, where the stakes are high, and the consequences of errors can be severe.

Both successful adoption and implementation of AI in AFC are limited by knowledge deficiencies. One respondent summarised this in their concern about “poor understanding and fear of employees to overrule automated decisions”. **A lack of technical understanding about AI can stall an organisation’s initial adoption of AI for AFC, but it also threatens to create unsafe working processes that can make an organisation more vulnerable to financial crime threats**, with users placing blind trust in systems they may not fully understand.

## Regulatory barriers to adoption

Concerns around regulation were one of the top potential barriers to the adoption of AI according to survey respondents, with over a third of respondents selecting ‘uncertainty about regulators’ views’ as a chief obstacle. Notably, this concern was shared by both those with high AI literacy and those with moderate to low understanding.

These concerns have some justification: regulatory frameworks for AI are still in their infancy, with many jurisdictions lacking comprehensive legislation to govern AI usage. The [EU AI Act](#), the world’s first comprehensive set of AI laws, has only recently come into force, with most provisions not set to be enforced until August 2026. Global divergence in regulatory approaches to AI poses further issues. The [Organisation for Economic Co-operation and Development \(OECD\)](#) has analysed different regulatory strategies across 49 jurisdictions, underlining the inconsistency in AI governance. These varied regulatory approaches make it difficult for multinational organisations to establish a cohesive AI compliance strategy.

This challenge is exacerbated by AI regulation’s susceptibility to politically driven change, as was seen in President Trump’s Executive Order on AI (passed 23rd January 2025), which, [according to the law firm Squire Patton Boggs](#), marked “a significant shift away from the Biden administration’s emphasis on oversight, risk mitigation and equity toward a framework centered on deregulation and the promotion of AI innovation as a means of maintaining US global dominance.”

Nevertheless, regulatory concerns do not necessarily present an insurmountable obstacle to the adoption of AI. **The principles of AI regulation have been articulated well and provide a good foundation for the development of a regulatory framework.** For example, the [UK regulatory principles](#) outline clearly the areas to be addressed: safety, security and robustness; appropriate transparency and “explainability”; fairness; accountability and governance; and contestability and redress. As one survey respondent noted:

*“I believe AI will be regulated soon, and I think financial institutions are awaiting regulators’ take on AI. It’s only a matter of time before firms begin to adopt AI, as it is still in the testing stage.”*

Meanwhile, regulators like the FCA have driven forward [initiatives to propel the development and adoption of new AI tools](#), demonstrating clear encouragement for organisations to take a proactive approach to AI adoption. With at least 75% of respondents aiming to adopt AI within five years, there is large potential for uptake within a time when the regulatory landscape will be more developed and easier to navigate.

## Overcoming barriers to adoption

As the fast-changing regulatory landscape suggests, many of the barriers to the adoption of AI in are quickly being overcome. Some concerns expressed by participants, such as those regarding reliability, accuracy, and security, are long-term, universal issues in AI development. It is vital that these remain focusses of both AI developers and the organisations implementing new AI tools.

While some of the larger challenges to AI are, therefore, to be expected to remain for the long term, they should not be seen as fundamental barriers to adoption. **By building familiarity with existing and developing AI applications for AFC, organisations can position themselves to take advantage of new opportunities as soon as they emerge.** Moreover, through direct engagement with AI development initiatives, AFC practitioners can help shape the creation of the specific tools they require.

Processes of knowledge building and engagement around AI development will additionally help organisations overcome other barriers to adoption they face. **By investing in training and development programmes that build AI literacy among their staff, organisations can ensure that they have the necessary skills to leverage AI technologies effectively.**

Organisations should also focus on adopting a hybrid approach to AI procurement and implementation that combines the strengths of AI with human expertise. This ensures that AI systems are used as tools to augment, rather than replace, human decision-making in AFC. By maintaining a balance between automation and human oversight, organisations can leverage AI's capabilities for AFC while ensuring robust and effective compliance measures.



## Conclusion

While challenges remain, AI's transformative potential for anti-financial crime is fast becoming reality.

The survey findings reveal a promising future for AI adoption in both general operations and specific AFC practices. While current implementation levels remain modest, a significant surge in adoption is anticipated over the next one to three years. Organisations are increasingly recognising AI's potential to enhance operational efficiency, strengthen compliance processes, and improve risk management. To capitalise on this momentum, organisations must proactively address key barriers to adoption.



# Recommendations

## 1. Adopt End-to-End AI-Enabled AFC Platforms

### Recommendation

Respondents expressed a clear need for systems which use AI to integrate the diverse AFC processes they carry out. Organisations should seek end-to-end platforms that unify onboarding, screening, monitoring, and investigations to reduce fragmentation and improve oversight across AFC processes.

### How Can Themis Help

Themis offers a modular, AI-powered platform that combines screening, monitoring, investigations, and reporting in one place. Themis Search enables a single view of financial crime risk, reducing reliance on multiple systems and manual processes.

## 2. Leverage AI for Real-Time Risk Scoring and Monitoring

### Recommendation

Respondents highlighted a desire for AI tools that are real-time, adaptable, automated, and highly specified to their organisation's needs. To stay ahead of evolving threats, organisations should implement real-time risk scoring and continuous monitoring tools that dynamically adjust to new data and risk indicators.

### How Can Themis Help

Themis' Customer Risk Calculator provides automated, dynamic risk scoring with high-risk triggers and review frequency guidance. Its 24/7 monitoring system updates sanctions lists every six hours and flags changes in client risk profiles in real time.

## 3. Conduct an Internal Audit & Consider Specialist Support for Scalable Compliance

### Recommendation

Organisations should conduct a thorough audit of their existing AFC processes and technology stack to identify specific pain points and inefficiencies where AI can deliver significant improvements. Where internal capacity or expertise is limited, partnering with specialist providers can help scale compliance functions effectively and ensure alignment with regulatory expectations.

### How Can Themis Help

Themis offers both diagnostic and delivery support. Its Business Risk Assessment tool helps organisations visualise risk exposure across internal systems and third parties. For those needing additional capacity, Themis provides insourced and outsourced KYC, onboarding, and monitoring services delivered by ICA-qualified professionals. These services are scalable, tailored, and designed to integrate seamlessly with your existing compliance framework.



## 4. Integrate AI with Existing Systems via APIs

### Recommendation

To maximise efficiency and reduce duplication, organisations should acquire AI tools that integrate fully with their existing systems, such as CRMs and operational platforms. The use of secure, flexible APIs is a key method by which easy and effective integration can be achieved.

### How Can Themis Help

Themis offers a suite of RESTful APIs that integrate seamlessly with platforms like Salesforce, Microsoft, HubSpot, and others. This enables automated data exchange across onboarding, screening, and monitoring workflows.

## 5. Use Novel Data to Enhance Detection

### Recommendation

Respondents saw the potential of AI to leverage new data sources and give new anti-financial crime capabilities as a key driver of AI adoption. Organisations should therefore prioritise tools that go beyond standard watchlists, incorporating novel structured and unstructured data to uncover hidden financial crime risks.

### How Can Themis Help

Themis' Special Interest Lists and proprietary conviction data cover all predicate crimes to money laundering, including environmental crime, modern slavery, and corruption. This enhances detection of hidden or indirect links to criminal networks, reducing the ability of illicit actors to conceal their activities from investigators.

## 6. Invest in Training and Research to Build Internal Capability

### Recommendation

Successful AI integration depends not only on technology but also on people. Respondents highlighted a lack of internal knowledge as a major barrier to their adoption of new AI-enabled AFC tools. To ensure sustainable AI adoption, organisations should invest in training and research that builds internal understanding of financial crime typologies, AI risks, and regulatory trends.

### How Can Themis Help

Themis delivers bespoke training, toolkits, and strategic research, supporting government, regulators, law enforcement and businesses with anti-financial crime risk awareness and capacity building. From typology-specific training modules to jurisdictional risk reports and ESG-linked crime toolkits, Themis helps organisations build long-term resilience and awareness.

**The next one to three years present a critical window for organisations to embrace AI in AFC practices.** Those who act decisively, aligning AI adoption with strategic objectives and addressing potential challenges head-on, will unlock significant competitive advantages. By leveraging emerging regulatory clarity, capitalising on cost reductions, and adopting a human-AI hybrid approach, organisations can transform their AFC capabilities and position themselves at the forefront of innovation. **Now is the time to move from recognition to action** – ensuring readiness for the AI-driven future that lies ahead.

# How Themis Uses AI

Themis Search is a SaaS platform designed to support Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance by enabling clients to screen and monitor individuals and companies against a wide range of global watchlists and proprietary databases, and conduct investigations through a risk-mapping interface that has access to millions of corporate records and real crime data that cover even the hardest-to-reach jurisdictions.

The platform is built upon a foundation of cutting-edge AI and comprehensive financial crime data. This includes sanctions lists, politically exposed persons (PEPs) information, law enforcement data, adverse media, and special interest lists related to issues such as modern slavery and the illegal wildlife trade. The platform leverages AI extensively across its operations, particularly in data harvesting, screening, and monitoring.

AI plays a central role in data harvesting by filtering and summarising news content using natural language processing (NLP) techniques such as named entity recognition and sentiment analysis. Generative AI models are used to summarise text and assess semantic relevance, enhancing the quality and efficiency of data ingestion.

In the screening and monitoring phase, AI is used to match client-provided data with profiles in the system. These tools support multilingual and typo-tolerant searches across

over 40 languages. Post-processing steps refine the results by comparing name components and adjusting confidence scores based on mismatches or missing data. The final results are ranked and presented to users, who can review and act on them.

The platform also features an AI-powered chatbot that provides 24/7 support, instant responses, and personalised assistance. It connects users to human experts when needed and integrates with Themis' research and training resources to offer comprehensive support, combining the trustworthiness of human expertise with the ease of AI automation.

In 2024, Themis received a UK Research and Innovation grant to support a transformative project focused on the development of new AI capabilities for financial crime detection. The final product of this research has now entered the final stages of development; we look forward to sharing its capabilities with clients and partners soon.

# Themis UK Research and Innovation Grant Project

In 2024, Themis was selected as one of the few recipients of a highly competitive grant from UK Research and Innovation (UKRI). Themis' UKRI project leverages AI capabilities in combination with real crime information to unearth hidden data patterns and vastly increase an organisation's ability to detect/report suspicious activity.

It uses AI to look beyond the standard watchlists to reveal a subject's wider and potentially hidden relationships, discovering their degrees of separation from, and exposure to, financial crime, and identifying how parties may be using different routes to legitimise the proceeds of their illicit activities. Users will be able to fully integrate tailored AI investigations into their existing AFC workflows, incorporating novel data and capabilities into established systems.

The project demonstrates how AI offers, in the here and now, opportunities to revolutionise anti-financial crime processes which have historically been subject to limitations around data quality, technology inflexibility, and solution design that has not focused primarily on user needs. By combining the knowledge of human financial crime experts with groundbreaking artificial intelligence, Themis aims to shift paradigms in how organisations combat financial crime.

The UKRI grant was awarded following a rigorous selection process that evaluated numerous applications from leading businesses and academic institutions across the UK. Themis' project stood out due to its potential for impact, innovation, and contribution to the strategic goals of UKRI, exemplifying how public and private sector priorities for AI in AFC can be fully aligned.

[illegible]



# ABOUT THEMIS

Financial crime has evolved faster than traditional systems. Themis delivers a new AI-powered, end-to-end platform purpose-built to help businesses detect, prevent, and respond to threats in real time. A modular solution that fuses advanced analytics, automation, and proprietary intelligence to tackle risk at scale and fast. As financial crime becomes more complex, Themis delivers clarity, speed, and impact. This isn't an evolution. It's the platform the future demands — powered by data, powered by Themis.



## Our reports & services:

Whether you're expanding into new markets, confronting sanctions exposure, or addressing risks such as environmental crime or human trafficking, we deliver clear, actionable insight grounded in real-world experience—across a broad range of risks. We specialise in complex, strategic projects where financial crime risks are new, emerging, or poorly understood. Our experts help you assess and mitigate exposure, empowering your organisation to make informed, confident decisions.

Our mission is to reduce the global impacts of financial crime through technological innovation, research, and the dedicated engagement of our expert teams. We support the public and private sectors with financial crime prevention, helping build safe, thriving businesses, preserving trust, and safeguarding reputations. We use a combination of the latest AI technology and human intelligence to support our clients and partners and ceaselessly drive new standards for anti-financial crime.

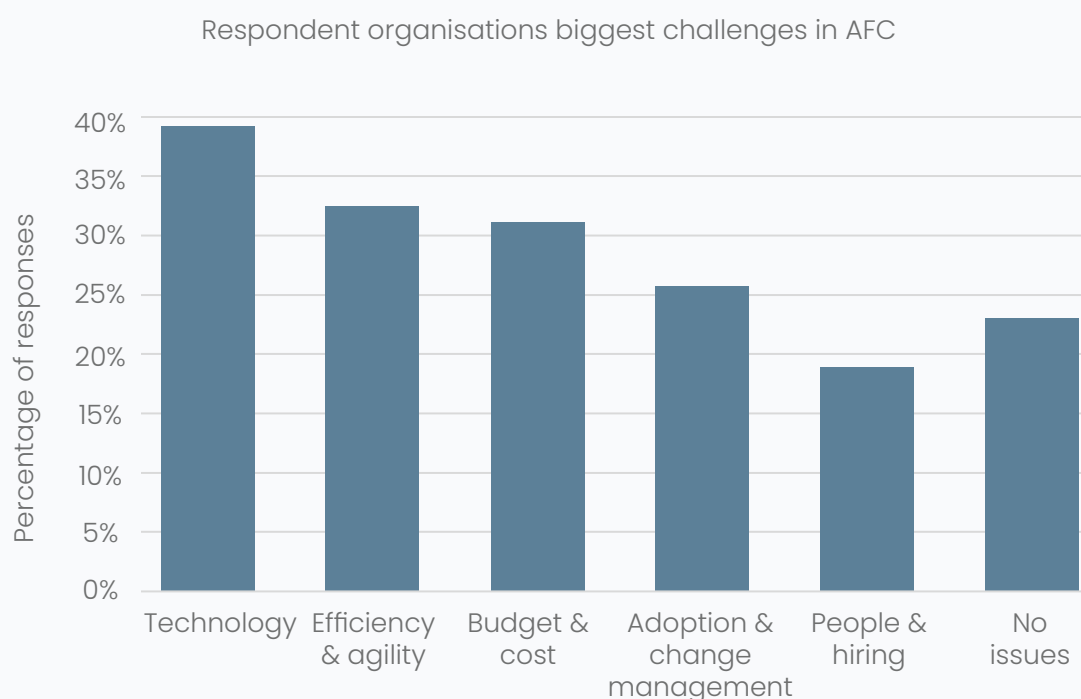




# Appendix

## Overview of Results

Question 1 – What are the major challenges your organisation faces in its anti-financial crime and compliance practice?

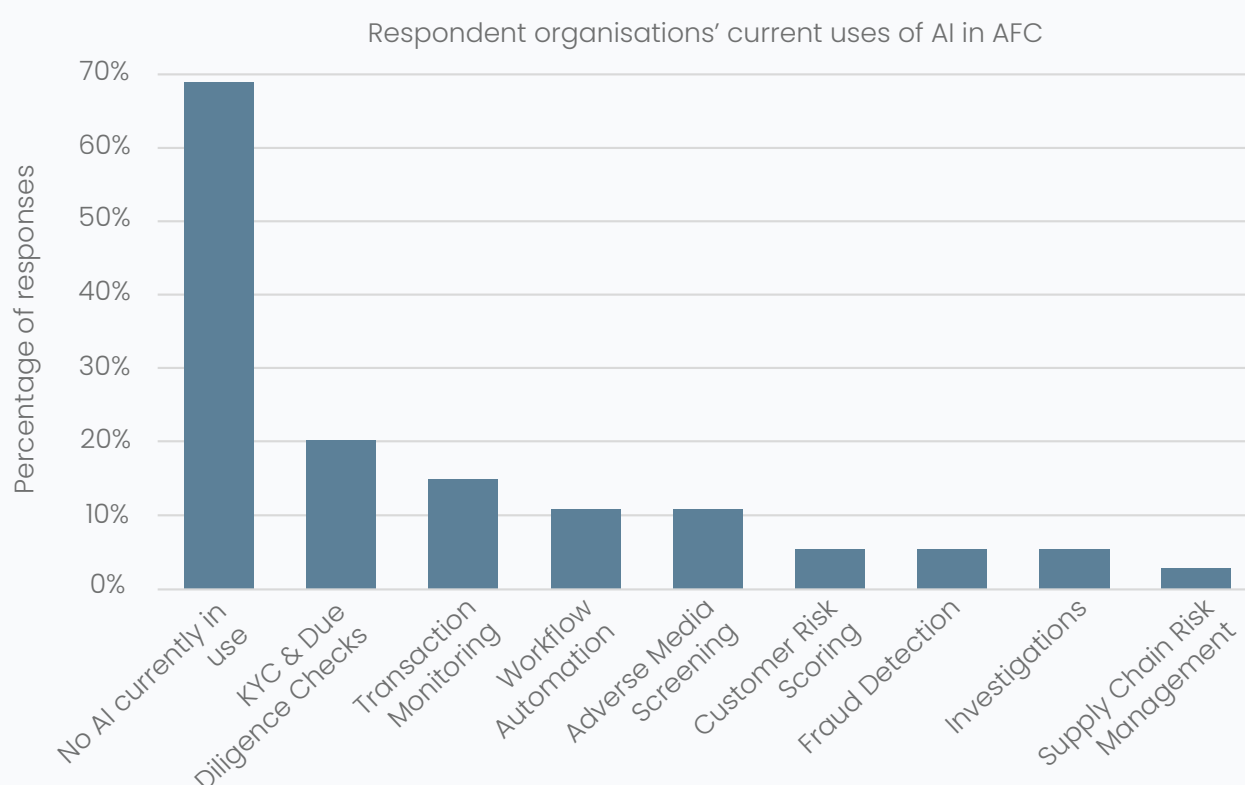


According to respondents, the biggest single challenge they face in their AFC and compliance is technology. This striking result is explored further in the Key Insights section above.

'Other' responses highlighted issues with changing and unclear regulation, other issues around technology (e.g. 'Selecting the right service providers'), fraud risks, and other issues relating to costs and cashflow.

23% of respondents stated that they faced no issues in their AFC and compliance activity.

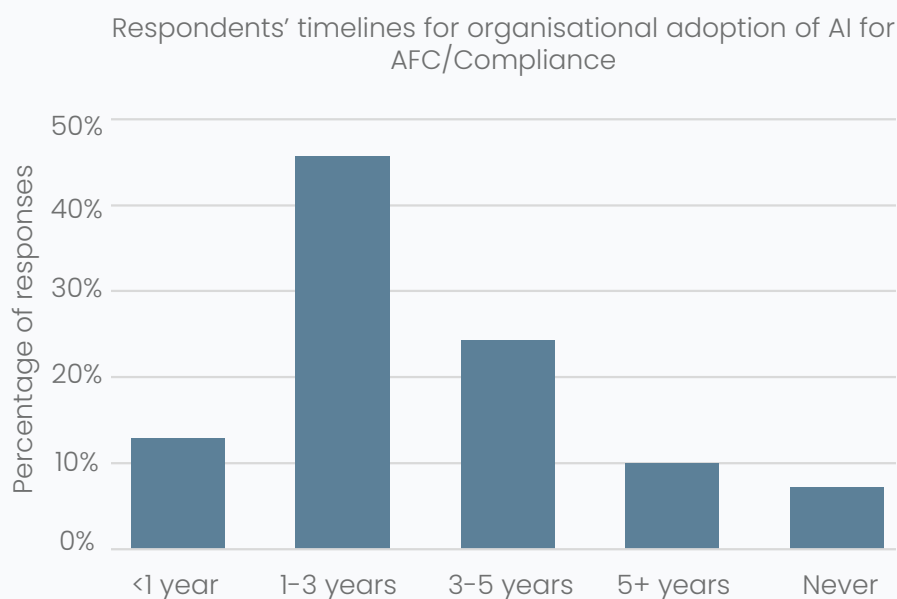
## Question 2 – For what purposes within anti-financial crime and compliance practice does your organisation currently use AI technology?



By far the most frequently given response was that surveyed organisations currently use no AI in their AFC and compliance activity; 69% of respondents stated this.

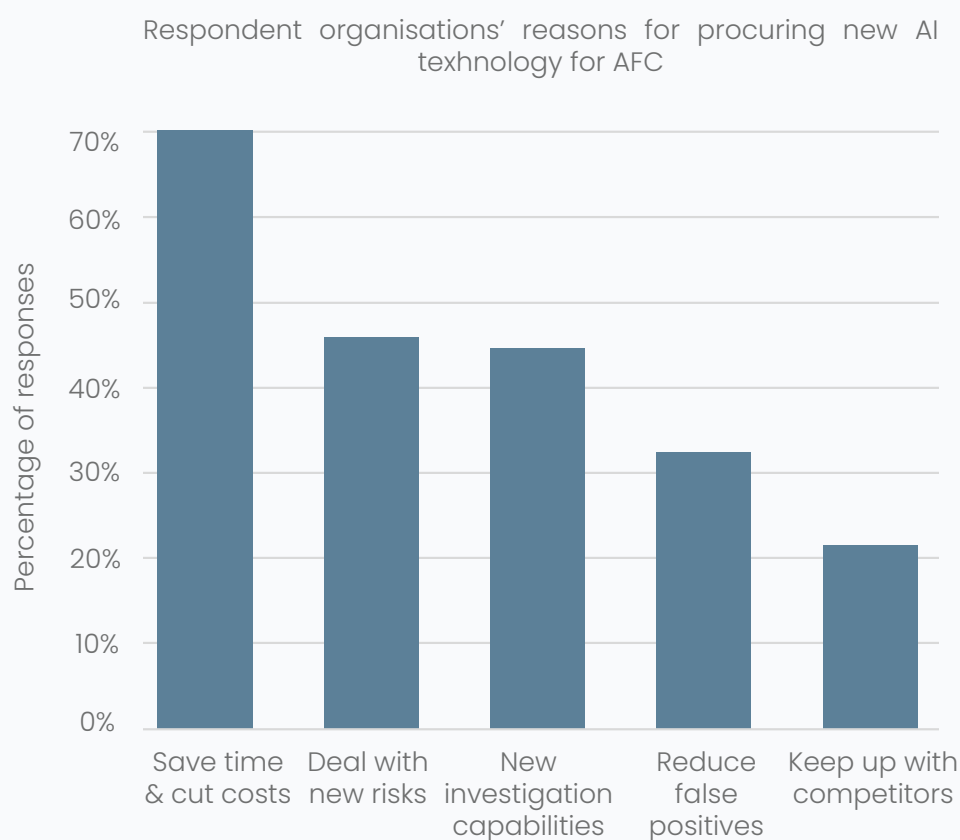
'Other' responses included usage of AI for operations and communications functions, as well as other document analysis and research purposes. One response also highlighted the use of 'external service providers'.

### Question 3 – In what timeframe do you think your organisation is likely to acquire new AI technology in anti-financial crime and compliance?



59% of respondents considered that their organisation would likely acquire new AI technology for AFC and compliance 'very soon' (in under a year) or 'soon' (in one to three years' times). Only 8% of respondents could not foresee their organisation acquiring new AI for these purposes (these are classed as 'Never' in the chart above).

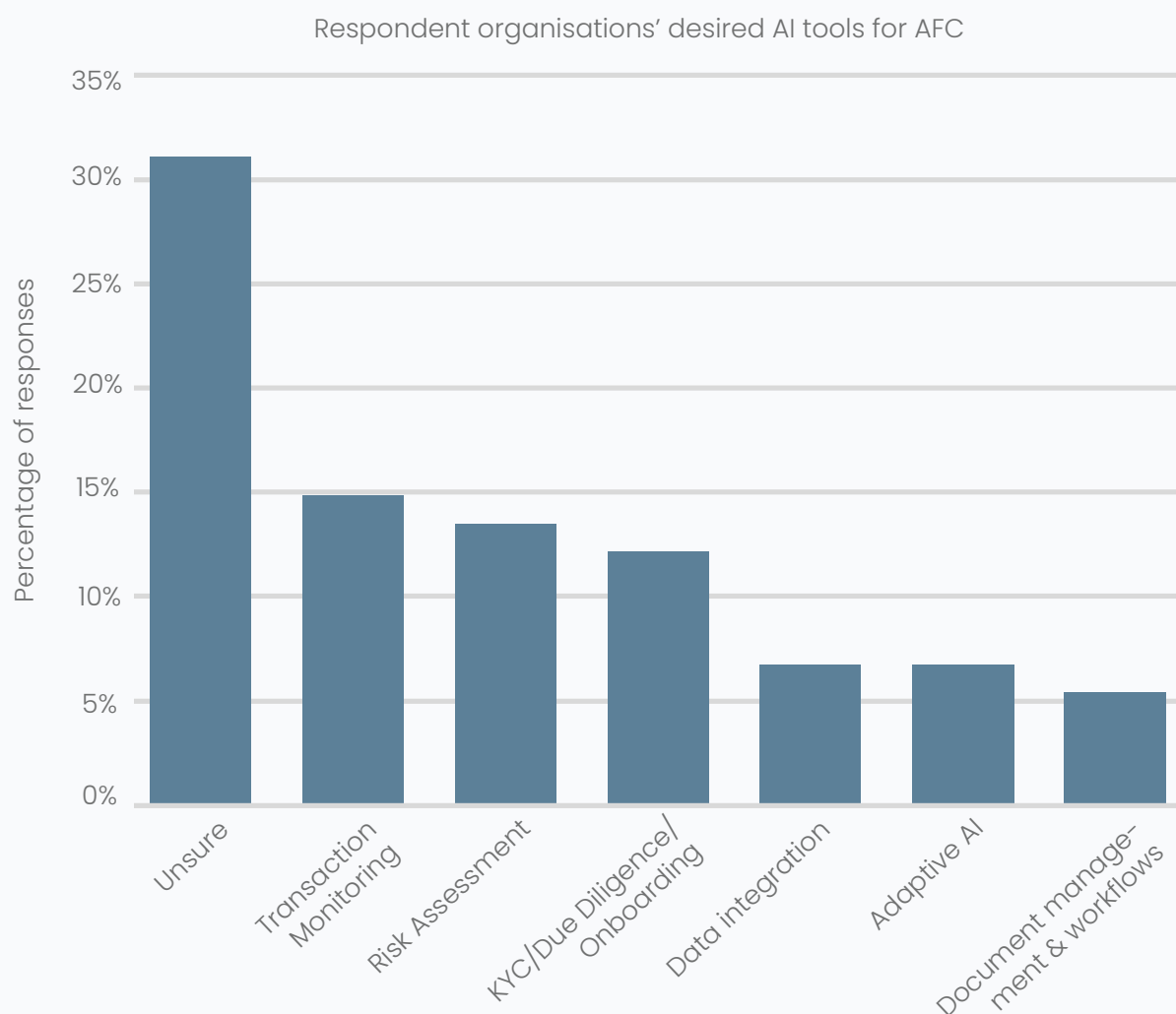
## Question 4 – What are the major reasons you would consider procuring new AI technology for your organisation’s anti-financial crime and compliance practice?



The most frequently given response, by a significant margin, for why organisations would procure new AI technology was to save time and cut costs in AFC and compliance activity, with over 70% of respondents giving this response. The next most common responses (each given by around 45% of respondents) focused on organisations’ desire to gain new capabilities in order to adapt to evolving types of risk.

‘Other’ responses included procurement of AI to enhance regulatory compliance and improve knowledge management, while one participant stated that they would procure AI “if it becomes a regulatory expectation or industry good practice”. Two participants stated that they would have no reason to procure new AI for AFC and compliance uses.

## Question 5 – If you could commission a bespoke AI product to help your anti-financial crime and compliance practice, what would you request?



While respondents were asked to provide open-ended text responses to this question, the intention being that each response reflect an individual organisation's unique requirements, some clear thematic groupings emerged, albeit with some elements of overlap between them. These are set out below, with indicative responses for each included.

The distribution of responses across each thematic grouping is illustrated. ►

## Uncertain/Not Sure (31% of responses)

Many respondents indicated uncertainty or lack of clarity about the specific AI product their organisation might commission. Some respondents alluded to a lack of knowledge about how AI could theoretically assist their organisation's AI/AFC practice, while others suggested that their organisation had no need for new AI technology.

"Not sure yet, need to research it more."

"I cannot see that we would need anything."

"N/A as too small a practice to develop a bespoke AI product"

## Transaction Monitoring (15% of responses)

Some responses focussed on tools and systems for enhancing the monitoring of transactions. Respondents identified the ability to conduct monitoring of transactional behaviour in real time as key requirements for an ideal AI system.

"AI product to identify and suspicious trades"

"Abnormal transactional behaviour of the customers, trend analysis, finetuning TMS alerts, etc."

"An AI tool for real-time transaction monitoring and automated client risk scoring using advanced analytics."

## Risk Assessment (14% of responses)

Responses in this category emphasised the importance of tools for assessing risks, scoring risks, mapping risks, and providing comprehensive risk assessments. Respondents focussed on user-friendly tools that can convert a variety of inputs into coherent risk assessments and reports.

"The ability to identify risks from a diverse set of sources, files, emails within a client file and consolidate into a risk assessment"

"One that could truly assess the reputational risks and behavioural risks in clients that are only evidenced by very soft or weak signals across markets, blending together what is on what is on the internet with what people say and market context"



## KYC/Due Diligence/Onboarding (12% of responses)

This category includes responses that focus on Know Your Customer (KYC) and Customer Due Diligence (CDD) processes. Respondents highlighted the need for better automation, end-to-end onboarding, and tools to increase the efficiency of compliance with KYC regulations.

"KYC assessments [with] better automation"

"End to end onboarding (KYC/CRA)"

"For first time buyers to pass a quick, but thorough process"

## Other Uses (8% of responses)

Some respondents highlighted very specific use cases for new AI tools. The responses highlight the need for tools tailored to specific tasks and challenges faced by individual organisations.

"Track illegal logging"

"Identify training needs and analyse the results, so that the right training can be provided to the whole entity across different business areas."

## Adaptive AI (7% of responses)

This category of responses focused on developing adaptive AI tools that are highly customisable to fit with and enhance existing processes. Respondents highlighted the need for products that can be customised to meet changing needs and regulatory demands.

"We initially need to investigate how AI can be best used within the existing processes of a Registration and Licensing Authority"

"Clear audit trail of all machine-learned decision making"

"A product that is constantly updated so as to give latest positions, a product that can be easily customised to meet changing needs of the users and regulatory demands"

## Data Integration (7% of responses)

This category includes responses that focus on integrating multiple systems, accessing data repositories, and bridging regulatory data with commercial opportunities. The responses highlight the need for tools that can handle structured and unstructured data and provide comprehensive data integration.

"Tools to identify risk across structured and unstructured data sets"

"The ability to integrate multiple systems"

"Data reporting output there is too much tech but limited assimilation of cross regulatory data."

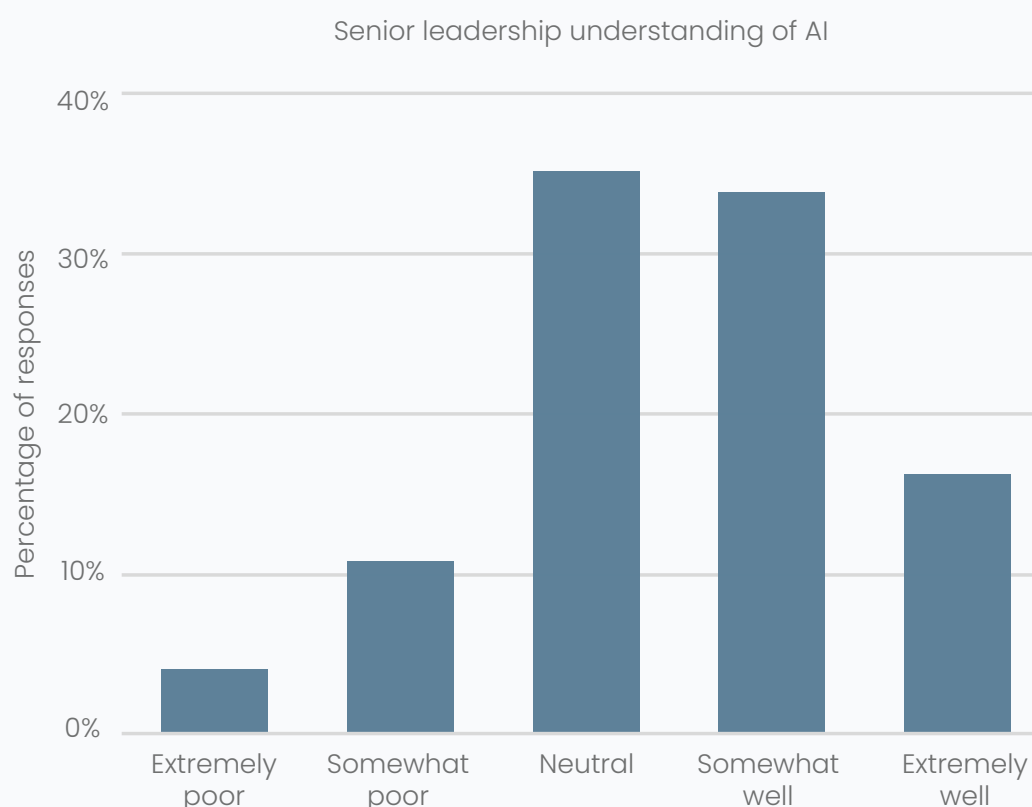
## Document Management and Workflows (5% of responses)

Some respondent focussed on AI tools to assist with processes in their AFC/compliance activity, particularly regarding document management and workflows. Automated drafting of reports (e.g. regulatory reports or suspicious activity/transaction reports) was highlighted as a particular use case of value.

"Document management"

"Report drafting"

## Question 6 – How well does your organisation’s senior leadership understand the risks and opportunities that AI might bring for your anti-financial crime and compliance practice?



Exactly 50% of respondents considered that their organisation’s senior leadership understood the risks and opportunities of AI presents for AFC either somewhat or extremely well.

Of the remaining respondents, 35% stated that their organisation’s senior leadership’s understanding was ‘neutral’, with only 15% of participants responding that leaders in their organisation had a somewhat or extremely poor understanding.

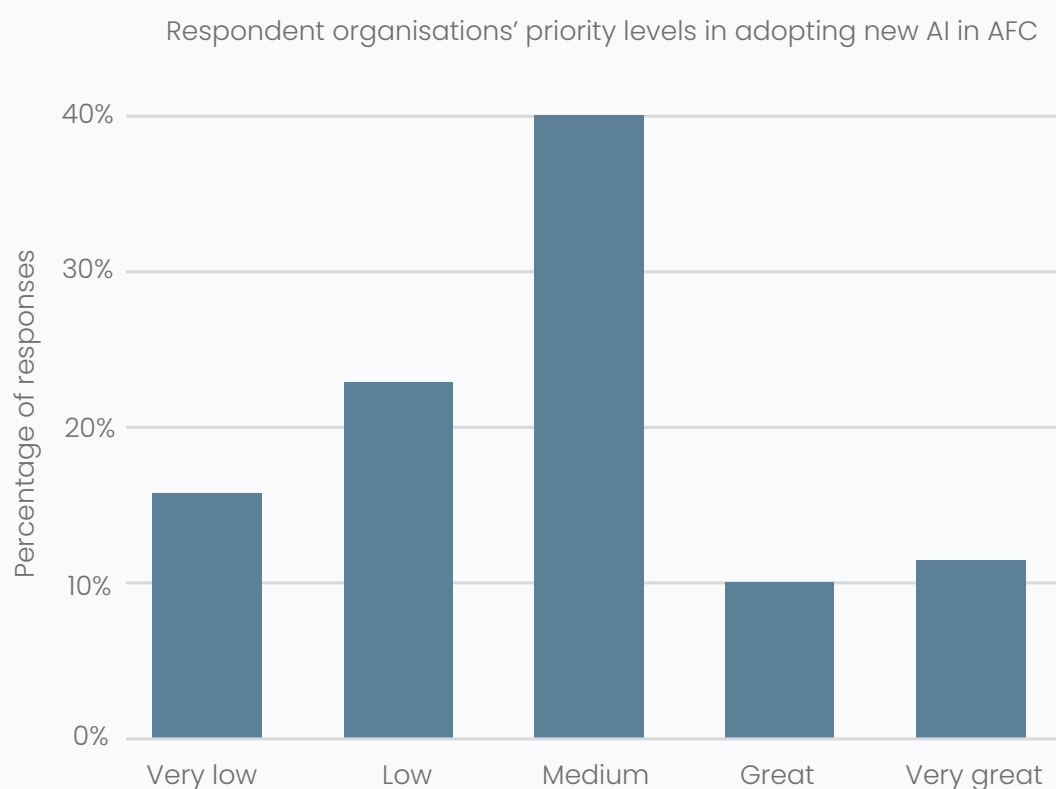
## Question 7 – What are the major obstacles to you procuring new AI technology for your organisation’s anti-financial crime and compliance practice?



The most common obstacle to procuring new AI for AFC and compliance that respondents faced was a lack of internal knowledge about AI, with nearly 45% of respondents describing this as a major obstacle. Notably, the sentiment that internal scepticism presents an obstacle was much less widespread, with only 16% of participants stating that this was an issue.

‘Other’ responses included some statements that no obstacles are faced, with AI procurement, or at least a strategy for AI procurement, an active work in progress. Several respondents highlighted other staff-related issues as impediments, including internal resistance to adopting technological change more generally, and problems with employee capacity and capability to adopt new technology, especially “if staff are not correctly trained”.

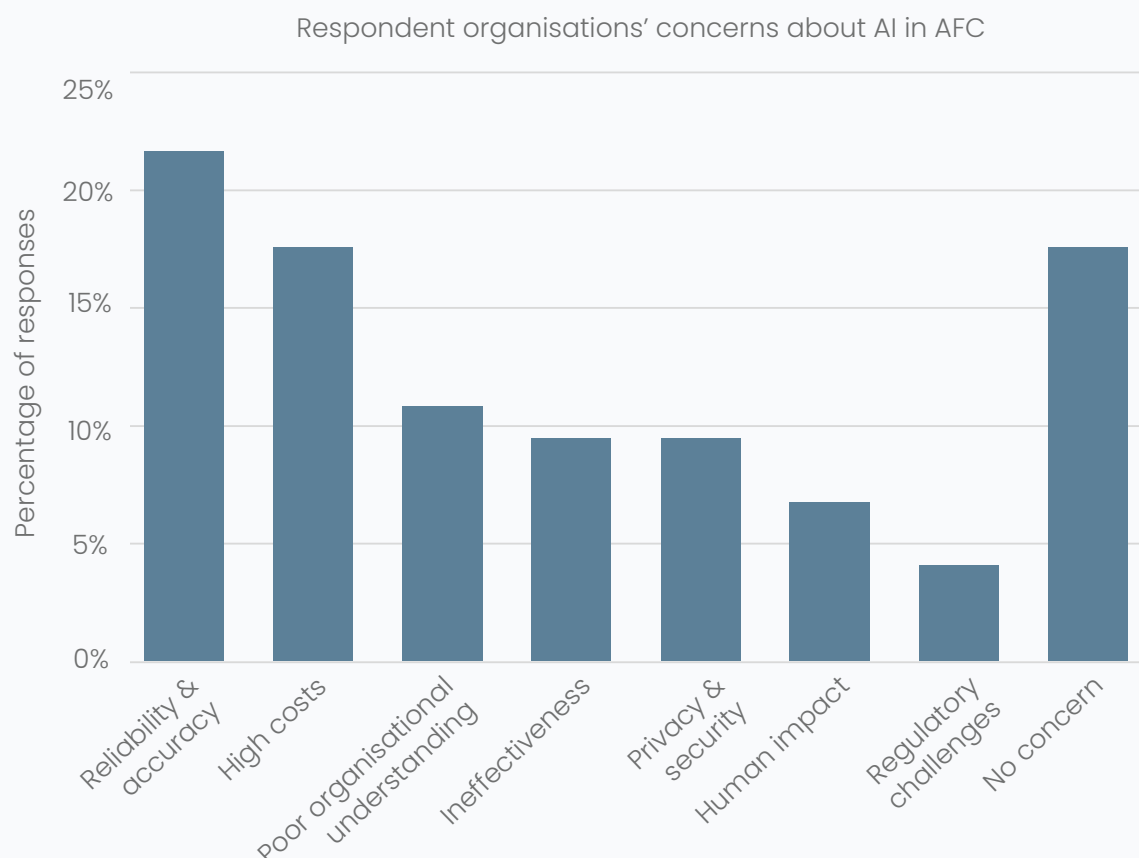
## Question 8 – How great a priority is the acquisition of new AI technology for your anti-financial crime and compliance practice?



By a significant margin, the most common response to this question was that the acquisition of new AI technology for AFC and compliance is a medium priority, with 38% of respondents stating this view. Almost the same number of respondents (39%) considered the acquisition of new AI to be a low or very low priority, with significantly fewer (23%) deeming it a great or very great priority.

It is notable that, among respondents who saw the acquisition of new AI to be a low or very low priority, a majority still believed their organisation would acquire new AI for AFC within five years (34% thought their organisation would acquire new AI technology within the next three years, with a further 28% expecting new AI acquisition in three to five years).

## Question 9 – What are your greatest concerns around implementing AI in your anti-financial crime and compliance practice?



While respondents were asked to provide open-ended text responses to this question, the intention being that each response reflect an individual organisation's unique requirements, some clear thematic groupings emerged, albeit with some elements of overlap between them. These are set out below, with indicative responses for each included.

The distribution of responses across each thematic grouping is illustrated below ▼



## Reliability and accuracy (22%)

Reliability was a key concern for many respondents. They were worried about the accuracy of AI outputs and the potential for mistakes in automated interpretation. Ensuring that AI systems do not lead to over-reliance on automated decisions was seen as crucial for maintaining trust and effectiveness. Respondents were concerned about the precision of AI systems in detecting and analysing financial crime, and emphasised the need for AI to provide accurate results to avoid false positives and negatives.

"Wrong outcomes from the AI"

"Mistakes in interpretation or analysis, missing pertinent details"

"Rapidly becoming reliant on something that may give us a false sense of security."

## High costs (18%)

Cost-related concerns were highlighted by many respondents, in particular high costs associated with implementing AI systems, including initial setup, ongoing maintenance, and training. They questioned whether the benefits of AI would justify the expenses and highlighted the need for cost-effective solutions.

"We experimented with [an AI compliance tool] but the costs were prohibitive on a group scale"

"Is it a costly sledgehammer to crack a nut?"

"High costs which might make it difficult for compliance to get buy-in from senior management"

## Poor understanding in organisation (11%)

A significant number of responses highlighted a lack of knowledge and understanding of AI among staff as a significant concern. Respondents expressed the need for proper training and education to ensure that AI systems are used effectively.

"Buy in from the executive and board"

"Lack of understanding by business of AI"

"Lack of knowledge and understanding/ lack of a need until its too late"

## Ineffectiveness (10%)

Some responses focused on concerns around the practical effectiveness of AI tools. Respondents identified the need for AI systems to be fit for purpose and provide tangible benefits to their AFC efforts.

"Effectiveness and sustainability of tools."

"To convince ourselves and the Regulators that AI works well."

"Ensuring it is fit for purpose and is of benefit to the company."

## Privacy and security (10%)

Several responses highlighted concerns around data privacy and security. Respondents emphasised the importance of protecting sensitive information and ensuring that AI systems comply with privacy regulations. Respondents were worried about the security of AI systems, including the accuracy and protection of data. They identified data privacy and robust security measures as a critical requirement for any AI implementation in AFC and compliance.

"Data Protection & Anti-breach & hacking attempts"

"Security of data"

## Human impact (7%)

Some responses addressed the impact of AI on human resources. Respondents were concerned about the potential loss of jobs and the need for human expertise in areas where AI might fall short. They emphasised the importance of balancing AI capabilities with human judgment and experience.

"How accurate it will be and the impact on the staff who might lose their job."

"Lack of personal judgements based on experience."

"Poor Understanding and fear of Employees to Overrule Automated decisions."

## Regulatory challenges (4%)

Several responses focused on regulatory and compliance challenges. Respondents identified the need for AI systems to meet regulatory requirements and maintain full explainability. They highlighted the importance of developing AI solutions that align with their specific regulatory environment.

"Our primary concerns about implementing AI in anti-financial crime and compliance centre on five critical challenges: ensuring data quality and representativeness for our unique [regional] context, maintaining full explainability to meet regulatory compliance requirements, addressing cybersecurity and data protection vulnerabilities, overcoming technological infrastructure limitations, and mitigating potential algorithmic biases."

"I believe AI will be regulated soon, and I think financial institutions are awaiting regulators' take on AI. It's only a matter of time before firms begin to adopt AI, as it is still in the testing stage."

## Other (1%)

1% of respondents stated that "**Fake identity**" was their greatest concern about the use of AI in AFC and compliance. Although not further clarified, this may refer to the use of AI to create fraudulent identity documentation, or to concerns around the ability of AI ID verification tools to detect fakes (both topics are explored further in the [Themis AI in Anti-Financial Crime Briefing Note](#)).

## No Concerns (18%)

Many respondents had no specific concerns, or did not have enough information to provide a meaningful answer. Some respondents considered it too early to tell what potentially concerning implications there are associated with AI usage in AFC/compliance.

"Not Clear yet"

"No concerns really"

"TBC"

# Get in Touch

If you would like to talk to us about any of the themes or updates covered in this report, please let us know.



**Nadia O'Shaughnessy**  
Head of Insight, Themis  
nos@wearethemis.com



**David Hodgson**  
Head of Business Development, Themis  
dh@wearethemis.com

Author:



**Henry Wyard**  
Senior Policy Analyst, Themis  
hw@wearethemis.com

## Looking for something specific?

Contact us to commission a bespoke report tailored to your priorities.



UAE: +971 (0) 58 526 8765 | UK: +44 (0) 20 8064 1724



info@wearethemis.com



www.wearethemis.com

© Copyright 2025. Themis International Services Ltd. All rights reserved.

