PwC EMEA AML Survey 2024

UK Insights on Effectiveness

November 2024

Contents

Executive Summary **2**
Introduction **4**
Methodology **5**
Regulations: Striking the Right Balance **7**
Current Perspectives 9
A Challenging Environment 11
Increasing Costs and Investments 13
Operations: Crafting an Effective AML Blueprint **17**
AML Control Effectiveness 18
Staffing Challenges: Talent and Recruitment 19
Data Collection 23
Customer Due Diligence 25
Technology: Embracing Digital Tools **29**
The Focus is on AI 31
Digital Tools: Enhancing Efficiency 35
Transaction Monitoring: A Closer Look 38
Conclusion **44**
Contact us **47**

Executive Summary

Earlier this year, PwC produced the first ever AML survey covering the Europe, Middle East, and Africa (EMEA) regions. This groundbreaking survey reveals how financial institutions in these areas are assessing and improving their Anti-Money Laundering (AML) measures, with the goal of enhancing their efficacy in the future.

Building on the insights from this survey, we performed a detailed analysis of the responses specifically from UK-based financial institutions. Our objective was to gain a deeper understanding of the effectiveness of AML regulations, operations, and technology within the UK context. We are now pleased to present the UK edition of this survey, which provides a comprehensive overview of the current state of AML/CTF measures in the UK financial sector.

Regulation	Over half (51%) of all UK respondents are optimistic about the current Anti-Money Laundering (AML) / Counter Terrorist Financing (CTF) rules, and think that they are helpful. However, perspectives on the effectiveness of current rules vary among different types of financial institutions, with only 36% of banks sharing this view, compared to 61% of payment institutions and 50% of asset managers.
	Additionally, 11% of all respondents cite a lack of uniformity in rules across countries and industries as a challenge. The debate continues between having a 'one size fits all' approach versus more tailored regulations, with uniformity being desirable in principle, but often requiring nuanced application to accommodate the diverse landscape of global finance and criminal activity.
	The survey also highlights the significant challenges faced by UK financial institutions in complying with AML/CTF regulations. The most pressing issue reported by 44% of all financial institutions is regulation complicating operational processes. Other challenges include the constant need to update KYC documentation and increasing regulatory pressures. These challenges are also compounded by budgetary limitations as cited by 29% of the respondents, most likely reflecting the UK's macroeconomic environment over the preceding 18 to 24 months, particularly in the aftermath of the COVID-19 pandemic.
	UK financial institutions have seen a significant rise in AML/CTF compliance costs, with 65% reporting increased spending over the past 24 months. This increase in costs is likely to be driven in part by evolving regulations, particularly post-Brexit, as the UK establishes its own regulatory framework. Banks are notably impacted, with 40% experiencing cost increases over 30%. Investments in AI and digital tools are also contributing factors.
Operations	The majority of UK respondents recognise the need to update their Target Operating Model ('TOM') to ensure that AML/CTF operations are efficient, compliant, and adapting to changing regulations and financial crime risks. 68% of respondents reported that they have updated their TOM within the last 12 months.
	Staff training is considered the most effective control in combating money laundering within financial institutions (identified by 39% of respondents). However, despite this, investment in training remains minimal in the UK, with only 22% of payment institutions planning to prioritise it over the next two years.
	Nearly 72% of UK respondents plan to increase their AML/CTF staff in control functions by at least 10%, reflecting the need to expand teams potentially in response to heightened regulatory pressures. Interestingly, only 12% of respondents identified recruiting skilled resources as their biggest challenge, suggesting that while many financial institutions are preparing for stringent regulatory demands, talent acquisition is not seen as a significant obstacle. However, retaining talent remains a concern in the UK, with 38% citing compensation as the primary issue.
	'Keeping KYC documentation up to date' is reported as one of the top challenges for respondents. Customer due diligence (CDD) serves as both an entry point for onboarding customers and an ongoing risk management measure through periodic reviews. Despite its importance, 33% of UK's respondents consider CDD onboarding to be the second weakest control, and 39% view periodic reviews as the weakest control. This may also have led to the high implementation of digital tools in CDD processes over the last two years.
	In the UK, there is a shift towards outsourcing AML/CTF activities such as KYC onboarding and periodic customer reviews, to manage complexities and enhance efficiency. Outsourcing provides UK financial institutions with increased capacity, cost savings, specialised knowledge, and advanced

	technological solutions like Artificial Intelligence (AI) and Generative AI (GenAI), which may exceed an institution's current investment scope or operational capacity.
Technology	UK financial institutions face significant challenges in adopting new technologies, including regulatory concerns, data quality issues, and budget constraints. Despite these hurdles, the integration of AI and digital tools is transforming AML/CTF activities by automating routine tasks, improving transaction monitoring, and regulatory reporting. The majority of survey respondents recognise the potential benefits of AI, with 91% considering its implementation to enhance compliance processes.
	Regulatory uncertainty remains a primary barrier to the adoption of new technologies, as the rapid pace of technological advancement often outstrips the development of corresponding regulatory frameworks. Data privacy and security requirements further complicate the landscape, making institutions cautious about implementing new technology. Data quality is another significant concern, as strong data quality is fundamental to effective identification and verification (ID&V) and screening processes. The lack of skilled resources and budget constraints also pose substantial challenges, hindering both the adoption and seamless integration of advanced technological solutions.
	Despite these obstacles, there is a strong interest in investing in AI and digital tools over the next two years. A notable 97% of UK respondents plan to allocate a portion of their budget to these technologies, with a focus on transaction monitoring, customer risk assessment, and screening. However, the implementation of AI and digital tools must be carefully managed to maintain data quality and ensure compliance with both data quality and regulatory standards.
	The survey also highlights the importance of regular testing and review of screening and transaction monitoring tools to ensure their effectiveness in detecting and preventing financial crimes. Nearly all UK respondents are using technology to monitor transactions, but challenges such as high volumes of false positive and alert backlogs persist. Addressing these issues requires a combination of advanced technological solutions and skilled resources. The report underscores the need for continuous improvement in AML/CTF processes to adapt to evolving financial crime risks and regulatory requirements.T

Introduction

Financial institutions in the UK are undergoing considerable changes in line with the shifting regulatory landscape, macroeconomic climate and post-Brexit developments. This is altering how they run their operations, interact with customers, and influence the choice of products and services they wish to provide. At the same time, criminals are also evolving, becoming more advanced in their methods to take advantage of customers and financial systems. Against a backdrop of sophisticated criminals, new regulations and emerging technologies, financial institutions must consider how they can best adapt to tackle AML processes in a smarter, more effective manner.

Methodology

This report provides a detailed analysis of, and insights from, the UK responses to the PwC 2024 EMEA AML survey. This wider survey had 396 respondents across 40 countries in total, 9% of which were from the UK.

Our approach ensured that the key players within each market contributed to our findings. We are confident that the insights garnered, particularly from the UK sector, are not only comprehensive, but also reflect the nuanced realities of the financial institutions operating within this jurisdiction. This report is based on data from 35 financial institutions based in the UK, the largest proportion being payments institutions, followed by banks, and then asset managers.

It should be noted that in order to gather robust data for our survey, we leveraged PwC's leading Anti-Financial Crime Network in the EMEA region. This was complemented by the expertise of a specialised survey firm, both of which were instrumental in identifying and engaging with pertinent stakeholders across the financial services landscape. Our focus was on securing participation from a broad spectrum of financial institutions, with an emphasis on prominent asset managers, leading banks, and key payment institutions. A significant portion of these entities were engaged through personal interviews, a method that allowed for in-depth discussions and nuanced feedback.

1 Regulations

Regulations: Striking the Right Balance

Financial institutions in the UK acknowledge the critical role of AML and CTF legislation in preserving the integrity of the financial system. The legislative framework is widely regarded as essential, yet financial institutions often highlight the burdensome nature of compliance, given its complexity and cost. The UK's AML/CTF framework, notably the Money Laundering Regulations 2017 (as amended) and the Proceeds of Crime Act 2002, is characterised by its rigour and thoroughness. Globally, AML/CTF standards are also tightening, with an increased focus on substance and effectiveness.

All financial institutions, irrespective of their scale or scope of operations, are expected to establish and maintain comprehensive AML/CTF frameworks. This includes senior management accountability, appropriate policies and procedures relating to customer due diligence, transaction monitoring, as well as the ability to detect and report suspicious activity. These measures are pivotal in the fight against money laundering and terrorist financing, but can also demand significant investment in advanced technology and employee training. This requirement poses a particular challenge for smaller entities within the financial sector.

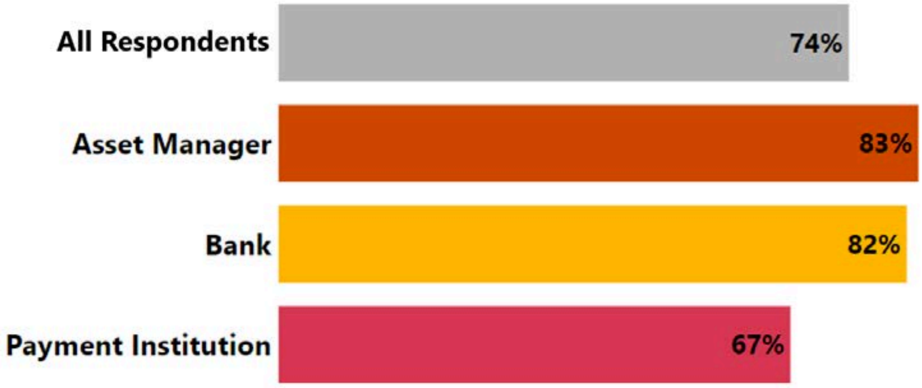
Despite the hurdles associated with regulatory compliance, there is widespread agreement among financial institutions around its necessity in protecting the financial system from the threats posed by illicit activities. The focus for financial institutions is on ensuring the right balance between stringent regulation and the practical application.

The Financial Conduct Authority (FCA), plays a pivotal role in enforcing AML/CTF standards, with the power to impose significant penalties for non-compliance. The FCA actively updates its own strategies to mirror the evolving nature of financial crime and the evolution of the financial services sector. It also offers guidance to firms on AML compliance and actively engages with the industry to gauge the impact of regulatory measures.

The FCA approach to supervision for payment institutions, banks and asset managers in the UK is based on a risk-based and outcomes-focused framework, that aims to ensure that these entities comply with the relevant AML/CTF regulations and standards, and mitigate the risks of money laundering, terrorist financing and other financial crimes. The FCA uses a combination of proactive and reactive tools and methods to supervise these entities, such as thematic reviews, inspections, audits, requests for data, taking enforcement actions and imposing sanctions on firms and individuals. Commitment 1 in the FCA business plan for 2024/25[1] is reducing and preventing financial crime.

[1] FCA Business Plan 2024/25

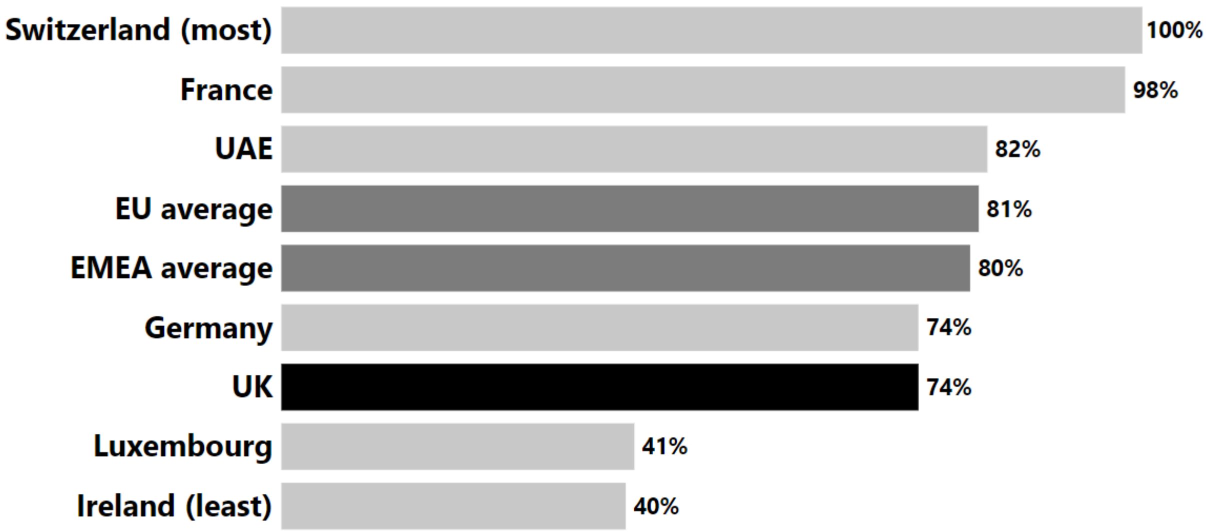
Exhibit 1: Respondents that were subject to any AML/CTF related regulatory inspection over the past 2 years



Source: PwC Global AWM & ESG Research Centre

Exhibit 1 shows that the majority of respondents (74%) reported being subject to some form of AML/CTF related inspection by the FCA over the last two years. This indicates how active the FCA remains as a Regulator, highlighting the increasing importance of understanding and complying effectively with applicable regulation and guidance. The 2022 to 2025 FCA Strategy[2] makes clear that a specific focus for the FCA during this period has always been to lessen and prevent serious harm, including reducing and preventing financial crime. The FCA's latest annual report[3] shows that the Regulator had 'opened' 613 financial crime supervision cases in 2022/23, an increase of 65% from the previous year, and an increase of 10% from their 2020/21 baseline figure of 548. According to Exhibit 1, the results indicate that the FCA's focus is shifting to include more asset managers and payment institutions, not just traditional banks.

Exhibit 2: Select countries that were subject to a regulatory inspection over the past 2 years



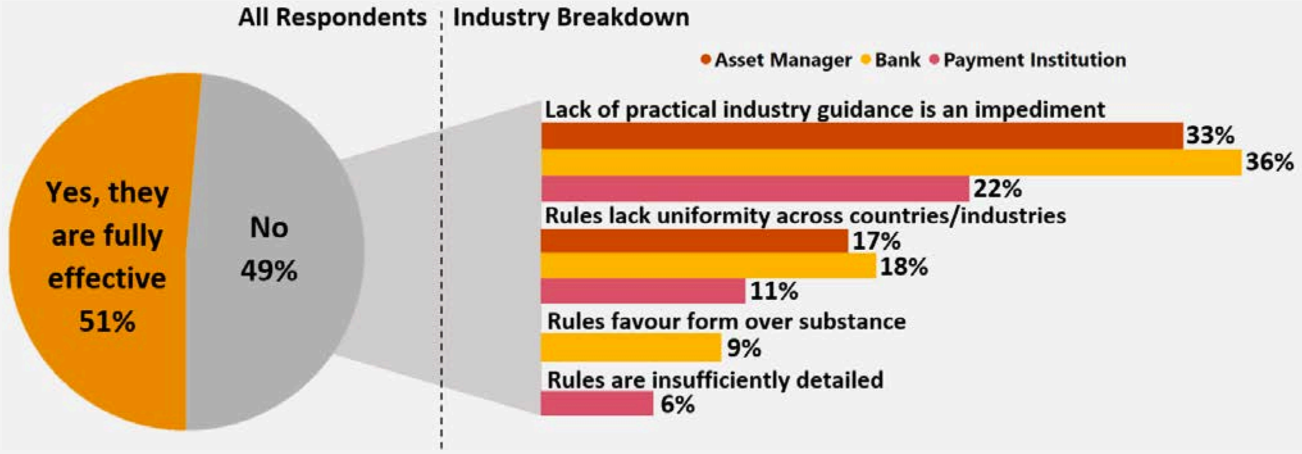
Source: PwC Global AWM and ESG Research Centre

We can see in Exhibit 2 above, that the UK regulatory inspection rate appears to be lower than the EU average (74% for the UK, compared to 81% for the EU), but is the same as reported by German counterparts.Whilst we cannot definitely determine the reasons for this, it should be noted that inspection rates will differ in countries for a number of causes such as the size of the financial sector, Regulator resources and strategic priorities.

[2] FCA: Our Strategy 2022 to 2025
[3] FCA: Annual Report and Accounts 2022/23

Current Perspectives

Exhibit 3: Are current AML rules helpful?



Note: Percentages may not add due to rounding.
Source: PwC Global AWM and ESG Research Centre

Just over half (51%) of all respondents answered that the current UK AML/CTF rules are helpful. But the industry views vary: 36% of banks believe the current rules are effective, compared to 61% of payment institutions and 50% of asset managers. This could in part be explained by the fact that banks have historically been the focus for the FCA, and faced significant penalties for AML/CTF non-compliance. This history of enforcement actions may contribute to a more critical view of the current legislation's effectiveness, as banks may feel that despite their best efforts, the legislation does not fully protect them from the reputational risks and financial costs associated with compliance failures.

Of the 49% who believe that improvement is necessary, most felt that there should be more practical industry guidance and examples to bring the regulations to life. Furthermore, 29% of those who answered 'No', cited a 'lack of uniformity in the rules across countries and industries' as a challenge. An industry breakdown can be seen in Exhibit 3. There are arguments on both sides for having a 'one size fits all' approach versus more tailored regulations. Uniformity is desirable in principle, but the application often requires a nuanced approach to accommodate the varied landscape of global finance, criminal activity and the type of institution.

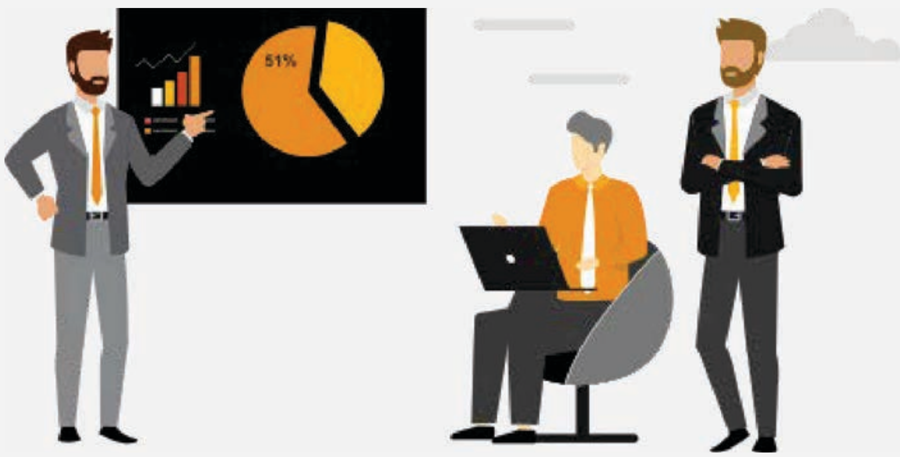
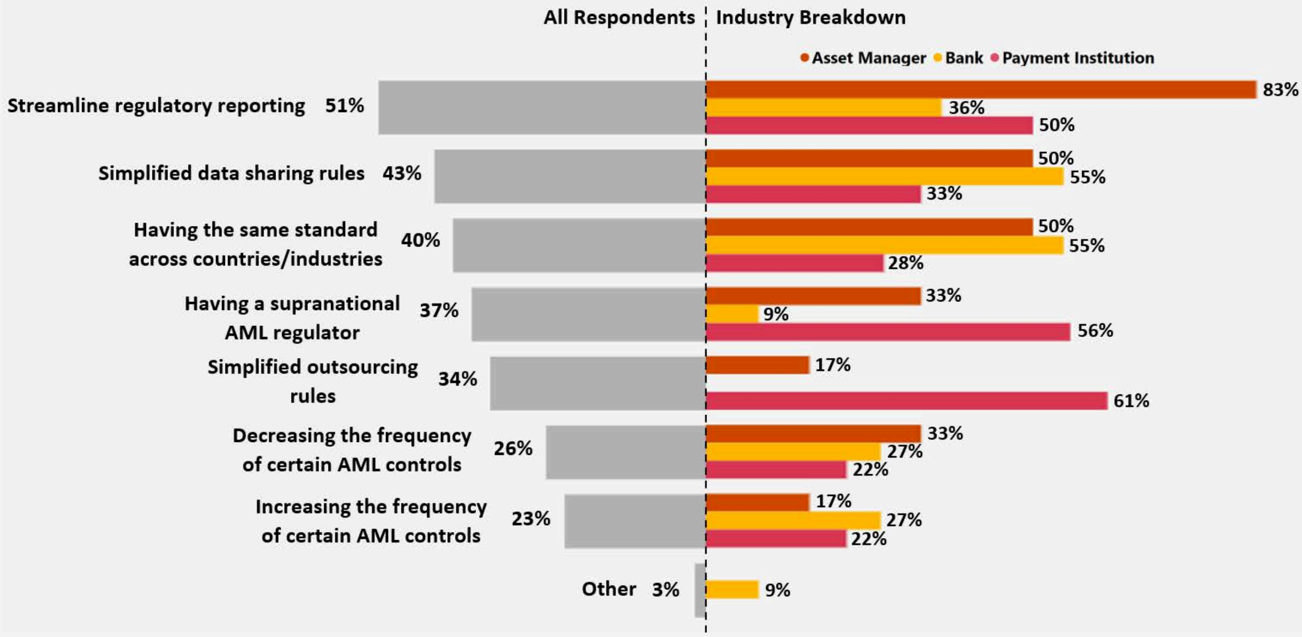


Exhibit 4: Which regulatory changes would significantly improve your AML/CTF effectiveness?



Note: Multiple choice question. Respondents were asked to select their top three answers.
Source: PwC Global AWM and ESG Research Centre

When questioned about what type of regulatory changes would significantly improve AML/CTF effectiveness, the most popular response was the 'streamlining of regulatory reporting' (Exhibit 4). In a difficult economic climate for financial institutions, there is a push to drive efficiencies and cut costs, including through reducing administrative burdens, allowing the focus to remain on financial crime prevention and detection. Asset managers were overwhelmingly in favour of streamlining regulatory reporting (83%), compared to banks and payment institutions.This could be to minimise administrative tasks, allowing a focus on core investment strategies.

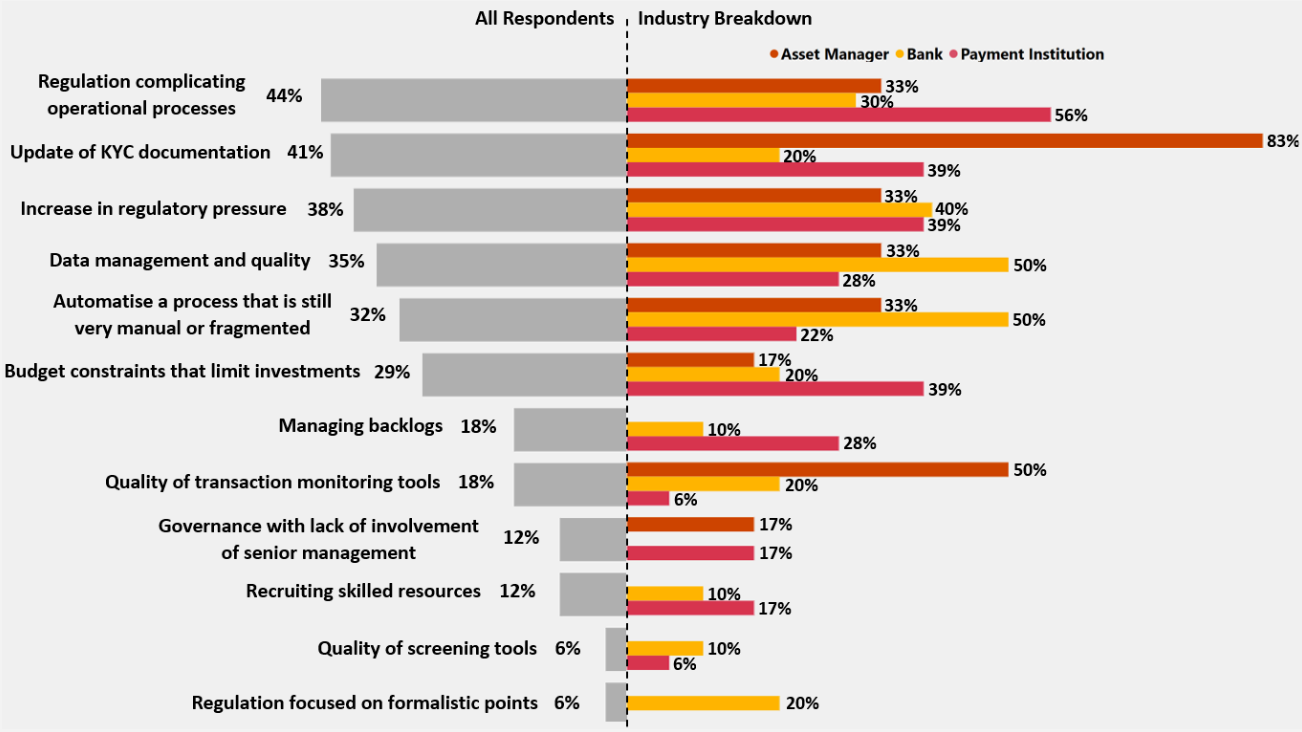
Interestingly, 34% of all respondents stated 'simplified outsourcing rules' would significantly improve their AML/CTF effectiveness, potentially supporting the wish to become more cost effective through outsourced models. However, none of the respondents were from banks, likely reflecting the maturity of their operational models already, as established users of outsourced models for their larger customer bases.

Three further prominent reasons were the 'simplification of data sharing rules', having the 'same standard across countries/industries', and, having a 'supranational AML regulator'. As institutions look to expand and diversify their products or services, it is no surprise that a 'standardisation and simplification' theme emerges. In particular, simplifying regulations would improve cooperation between different entities and jurisdictions, especially where the institution operates within multiple product lines and geographies. This would thereby improve tracking and prevention, and in turn allow financial institutions to focus on their core AML/CTF responsibilities.

The data also indicates a near equal amount of responses in relation to increasing or decreasing the frequency of certain AML controls to improve AML/CTF effectiveness. This indicates that AML/CTF requirements are regarded differently across the board: while some institutions feel a need to tighten controls, others could view them as a procedural burden which must be reduced. Asset managers were most in favour of decreasing the frequency of AML controls (33%).

A Challenging Environment

Exhibit 5: **What are your biggest AML/CTF challenges?**



Note: Multiple choice question. Respondents were asked to select their top three answers.
Source: PwC Global AWM & ESG Research Centre

The biggest AML/CTF challenge reported by respondents is 'regulations complicating operational processes', with 56% of payment institutions reporting this to be the case. This is hardly surprising given the complexity of AML regulations in the UK is a well-known factor contributing to this challenge. These regulations necessitate stringent compliance measures, which in turn introduce additional layers of complexity to the operational workflows of financial institutions.

Financial institutions are also challenged by the ever-changing landscape of local and international regulations, which can complicate operations and increase costs. Adapting to these changes often results in more time-consuming processes and slower transactions. A forward looking example is the introduction of the new EU AML package[4]. This may impact UK headquartered financial institutions with six or more branches in the EU, and branches of foreign financial institutions in the UK especially if they are deemed to be 'obliged entities'. Much is still unknown at this stage, but the implications for these financial institutions could include revising their operational processes to align with both UK and EU standards in some instances, leading to further operational complexities and costs.

The second largest challenge, highlighted by 41% of all respondents, is the 'update of KYC documentation'. Financial institutions face a constant challenge in keeping their KYC documentation up to date, in line with regulation and industry guidance. The task of updating information held on customers is essential in every financial institution, but can be very demanding, leading to increased operational costs, especially where high risk customers and products are involved. Nevertheless, it is an integral part of a financial institution's customer due diligence process and is mandated by UK regulations. Ongoing monitoring, screening and verification of customer data against changing regulatory requirements can be resource-intensive, depending on the risk profile of customers and the amount of automation employed.

When disaggregating by industry type, it is interesting to note that 'updating KYC documentation' seems to be a concern for 83% of asset managers, compared to banks (20%) and payment institutions (39%) providers. This likely reflects the complexity and sophistication of the customer base at asset managers (e.g. hedge funds, private equity, and trusts), and the associated time and cost of completing KYC.

Asset managers also frequently operate across borders, dealing with international clients and investments. This adds an additional layer of complexity due to varying international regulations and the need to understand and comply with multiple jurisdictional requirements

[4] Source: Anti-money laundering: Council adopts package of rules

The third ranked most challenging issue faced by UK financial institutions is the 'increase in regulatory pressure' with 38% of all respondents stating this was the case. It is worth noting that in the wider PwC EMEA AML Survey, regulatory pressure is cited as the number 1 challenge faced by institutions. There are likely to be a number of reasons for the prevalence of this in the UK including the FCA 'Dear CEO' letters that were issued to wealth management and stockbroking firms[5], as well as payments firms[6] in 2023. These highlighted the FCA's concerns, supervisory priorities and expectations in relation to financial crime prevention. It further signalled a shift in focus of the Regulator, away from traditional banking, towards asset managers and payments institutions.

Additionally, the 'debanking' controversy in the summer of 2023 required a number of banks, buildings societies and payment firms to provide data[7] to the FCA in relation to account closures between July 2022 and June 2023, to better understand whether customers' accounts were closed because of their lawfully expressed political views or beliefs. This led financial institutions to increase activity in reassessing their customer due diligence processes and customer records for politically exposed persons (PEPs), as well as the need to respond to increased data subject access requests from individuals under data protection legislation.

The controversy also prompted an amendment to the UK Money Laundering Regulations[8] which took effect in January 2024, and stated that domestic PEPs must still be subject to enhanced due diligence (EDD), but must be treated as lower risk than overseas PEPs. An FCA multi firm review[9] followed on the treatment of PEPs, and whether the current FCA guidance (from 2017) remains appropriate. A consultation[10] has since been launched on targeted clarifications to the FCA PEP guidance, which closed in October 2024. This has necessitated financial institutions to adjust their PEP risk assessments and customer onboarding process accordingly, which is likely to have had an impact on the perception of 'increasing regulatory pressures' and 'regulations complicating operational processes'.

The survey findings reveal that budgetary limitations are a significant challenge by approximately 29% of the respondents. This observation aligns with expectations when considered within the context of the UK's macroeconomic environment over the preceding 18 to 24 months, particularly in the aftermath of the COVID-19 pandemic. The economic repercussions during this period have undeniably exerted pressure on financial resources, thereby impacting the allocation and management of funds dedicated to AML/ CTF controls within these institutions.

[5] Source: FCA expectations for wealth management and stockbroking firms 8 November 2023

[6] Source: FCA priorities for payment firms 16 March 2023

[7] Source: FCA sets out initial findings on bank account access and closures

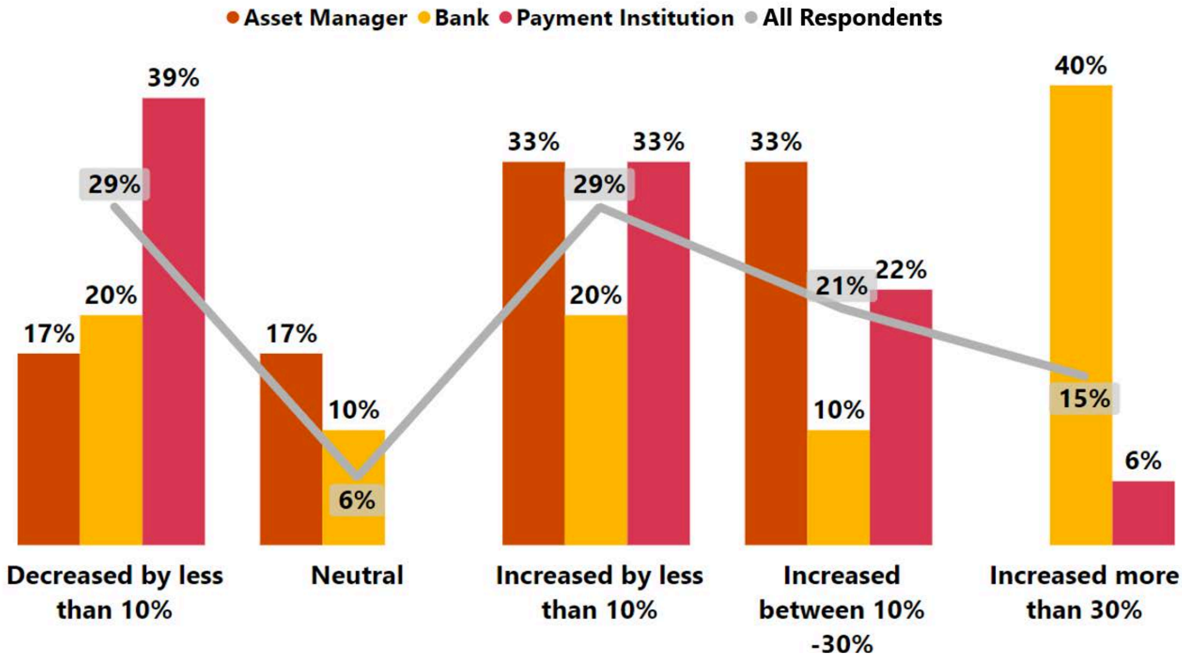
[8] Source: The Money Laundering and Terrorist Financing (Amendment) Regulations 2023

[9] Source: Multi Firm Review: The treatment of politically exposed persons

[10] Source: GC24/4: Proposed amendments to Guidance on the treatment of politically exposed persons

Increasing Costs and Investments

Exhibit 6: How much have your costs in relation to AML/CTF compliance changed over the last 24 months?



Note: Percentages may not add due to rounding.
Source: PwC Global AWM and ESG Research Center

According to a report by data analytics company LexisNexis[11], UK financial institutions spent £38.3bn on financial crime compliance in 2023. This is up 12% on the previous year, and up 32% since 2021. Our survey results echo this, showing that the majority of respondents (65%) experienced an increase in their spending for AML/CTF compliance over the last 24 months. Within this group, 15% of respondents reported their costs 'increased by more than 30%'. Interestingly, 6% of respondents reported no change in compliance costs, whereas 29% reported a 'decrease in costs by less than 10%' – this may be due to the efficiencies in financial crime compliance processes that led to cost savings.

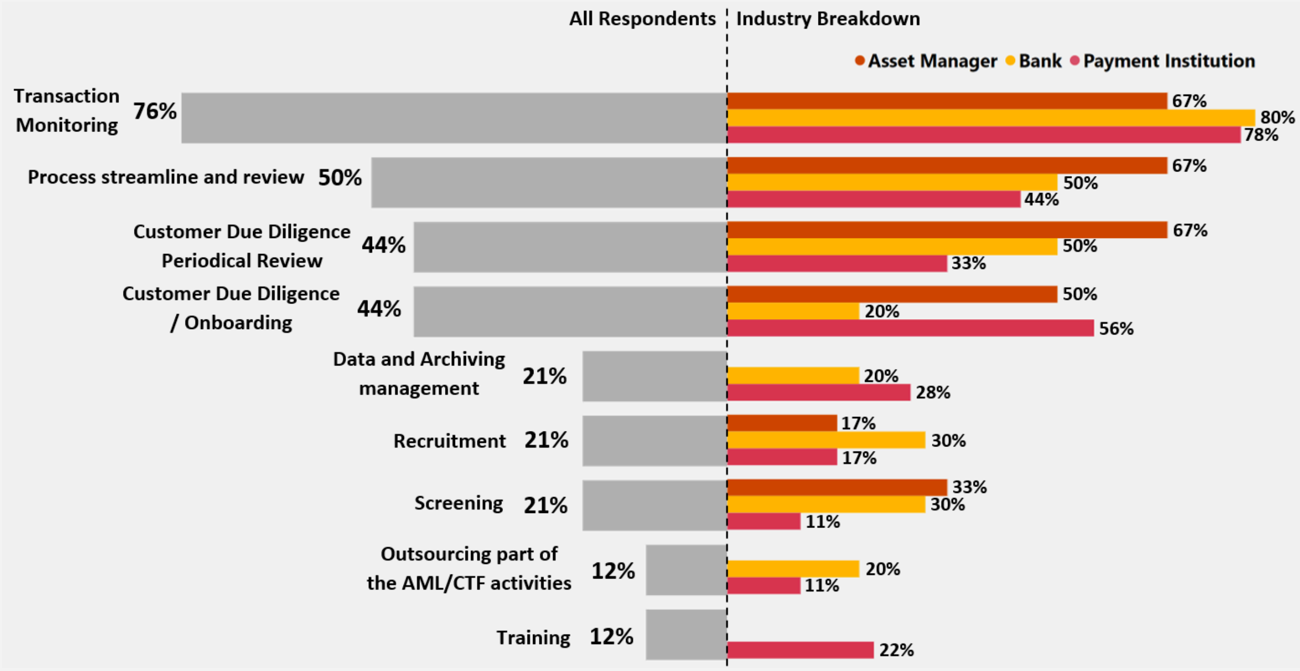
Analysis by industry type shows that banks seem to be the most heavily impacted, with 40% of banks reporting rises in cost of more than 30%. Overall, 70% of banks surveyed cited some level of increase, highlighting the strain on those financial institutions which are often at the forefront of AML/CTF efforts.

Another driver of increased compliance costs is likely to be the evolving regulatory environment. Since 2021, financial institutions have been adapting to new regulations and guidelines that demand more rigorous compliance measures. The UK, post-Brexit, has been keen to evolve its own regulatory framework that aligns with global standards, while also demonstrating its local commitment to preventing financial crime. This has led to the implementation of new laws and the update of existing ones, which in turn require institutions to invest in understanding, integrating, and maintaining compliance with these regulations. Other cost drivers are likely to be the increasing staff numbers in control functions and investments into AI and new digital tools, which are covered in more detail in following chapters of this report.

The responses demonstrate a correlation between the respondents who were subjected to regulatory inspection and increases in operational costs. An inspection by the FCA can have a significant impact on the costs of these financial institutions in many ways, especially where the inspection uncovers any gaps or deficiencies in the financial institution's AML systems and controls.

[11] Source: True Cost of Compliance 2023 Report – LexisNexis

Exhibit 7: **Which AML/CTF topic will you prioritise your investment in over the next 24 months?**



Note: Multiple choice question. Respondents were asked to select their top three answers.
Source: PwC Global AWM and ESG Research Centre

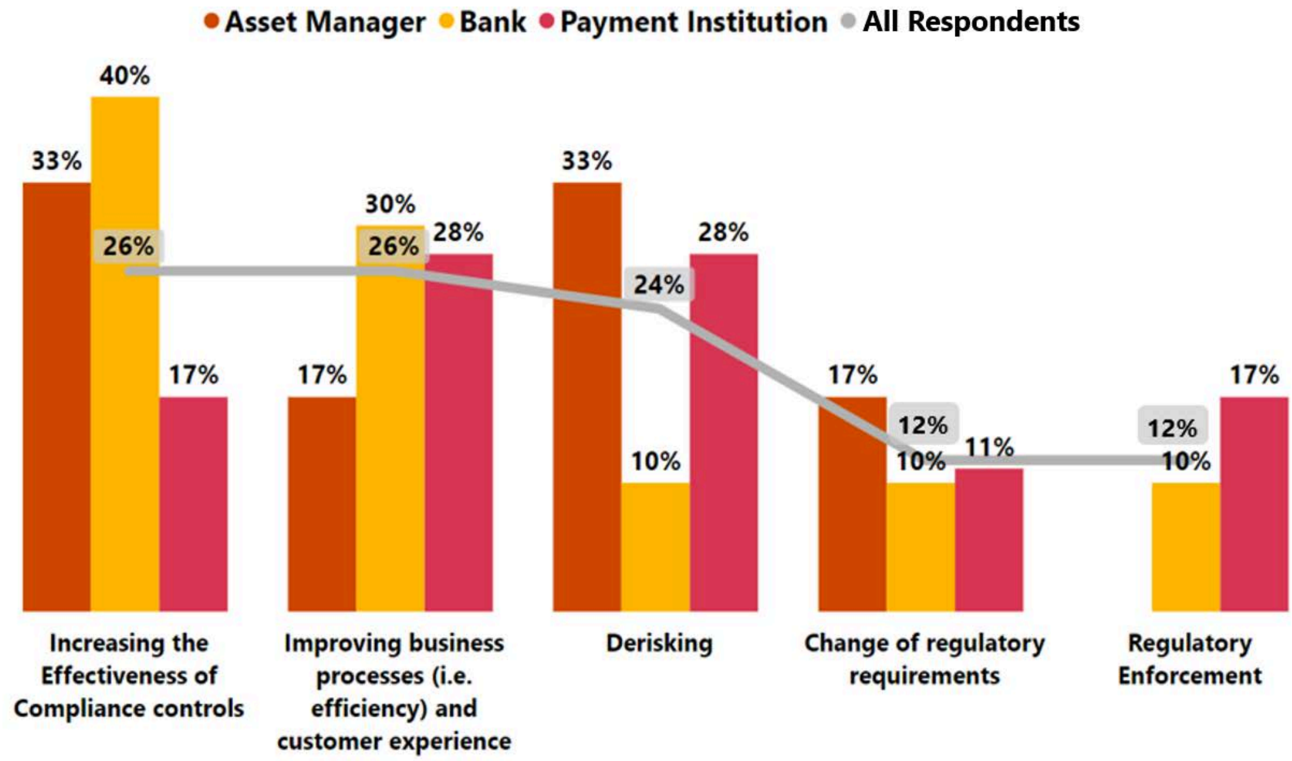
Transaction monitoring emerged as the most important AML/CTF investment priority for respondents over the next two years, as Exhibit 7 indicates (76% of respondents). Additionally, the UK results mirror the findings across the EMEA region, with almost two-thirds of respondents prioritising investment in transaction monitoring, acknowledging the role and significance of transaction monitoring in preventing and detecting AML/CTF.

An industry breakdown shows that 80% of bank respondents will prioritise investment in transaction monitoring. This is likely to reflect the larger volumes of transactions banks handle, and the scale of transaction monitoring systems required for those volumes. With enhanced transaction monitoring tools which increasingly include the use of AI, financial institutions can more effectively manage financial crime risk. This can be through being able to detect unusual customer activity earlier by creating a more holistic view of customer behaviour, being able to predict future trends, and identifying new risks before they become widespread. Machine learning techniques can reduce the number of false positives by better distinguishing between true matches and coincidental similarities, improving operational effectiveness. Technology and its impacts are covered in more detail in the 'Technology' section of this report.

The next areas prioritised for investment are 'process stream line and review', 'customer due diligence (CDD) periodical review' and 'CDD / onboarding' (50%, 44% and 44% respectively). Asset managers were overwhelmingly in favour of prioritising spend in 'process stream line and review' and 'customer due diligence (CDD) periodical review' when compared to banks and payment institutions. This appears to mirror their desire to 'streamline regulatory reporting' to improve effectiveness (as seen in Exhibit 4). In general, the prioritisation of these areas shows that financial institutions understand that CDD is a crucial task and are trying to balance risk management with cost reduction through improved efficiency.

As you will see later in this report (Exhibit 10), transaction monitoring was identified as the third strongest AML control in preventing financial crime which may also contribute to the reason for it being an investment priority. Interestingly, areas such as 'CDD periodical review' and 'CDD / onboarding' were rated as the weakest and second weakest controls in preventing financial crime, respectively. The investment in CDD processes by financial institutions indicates a growing recognition of its importance in preventing financial crime and ensuring regulatory compliance. This reflects a broader understanding that getting CDD right from the outset is crucial for effective AML effort.

Exhibit 8: **Key driver for investments**



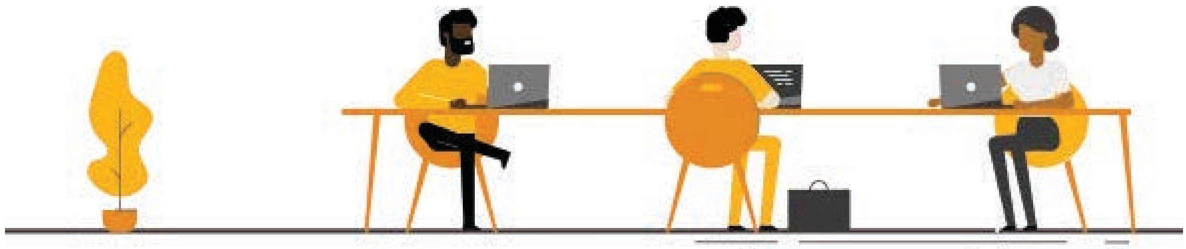
Note: Percentages may not add due to rounding.
Source: PwC Global AWM and ESG Research Centre

Investment decisions across the industries appear to be influenced by a common set of priorities. The primary drivers are centred around effectiveness, efficiency and risk management. 26% of all respondents selected ‘increasing the effectiveness of compliance controls’, while another 26% selected ‘improving business processes and customer experience’ as the key driver for their investments. 24% of respondents indicated that ‘derisking’ was a key driver, signalling an inclination towards mitigating potential risks before they materialise.

Payment institutions have become an increasing focus for the FCA over the last few years due to their rapid expansion.The results also show that banks, who have been under FCA scrutiny for a longer number of years, understand the importance of investing in and improving their compliance controls and business processes.

Changes in regulatory requirements and regulatory enforcement are perceived as less influential in terms of attracting investment, with each drawing 12% of responses. While these areas are still important and represent an actual challenge for respondents (as discussed earlier in this section), the responses demonstrate that financial institutions’ key drivers for investment lie elsewhere.

These results deviate slightly from the wider EMEA AML survey results. While the top two drivers for investment remain the same across the board, interestingly, no UK respondents selected ‘reducing AML/CTF compliance costs’ as a key driver for investment, whereas 7% of respondents in the EMEA survey cited this as a key driver. This is perhaps because cutting compliance costs is a by-product of ‘increasing the effectiveness of compliance controls’ and ‘improving business processes’: by increasing effectiveness and efficiency, compliance costs will likely fall as a result. Therefore, respondents were more inclined to select these answers as they are more representative of the entire investment programme. Either way reducing compliance costs is unlikely to be a sole driver for investment decisions.



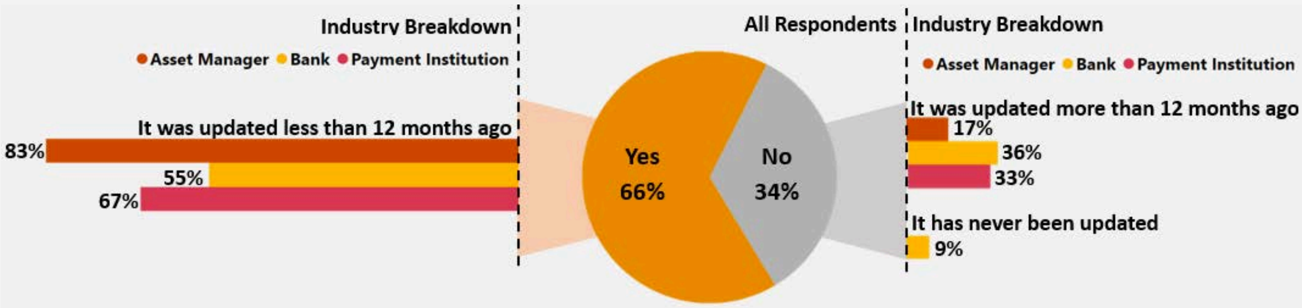
2 Operations

Operations: Crafting an Effective AML Blueprint

Effective operations within a financial institution are essential for mitigating money laundering and terrorist financing risks. They require a holistic approach that combines strong leadership, a culture of compliance, comprehensive policies, continuous training, advanced technology, independent testing, and adherence to regulatory requirements. Together, they form a cohesive framework that is designed to detect, prevent, and report unusual activities.The effectiveness of these operations is reflected in the financial institution's ability to adapt to evolving risks and regulatory requirements, helping to protect themselves and their customers from being exploited for illicit purposes.

A Target Operating Model (TOM) serves as a blueprint for an organisation, outlining how it should operate to effectively achieve its business objectives while adhering to regulatory requirements. An appropriately designed TOM ensures that AML operations are efficient, compliant, and adaptable to changing regulations and threats.

Exhibit 9: Have you updated your AML Target Operating Model in the last 12 months?



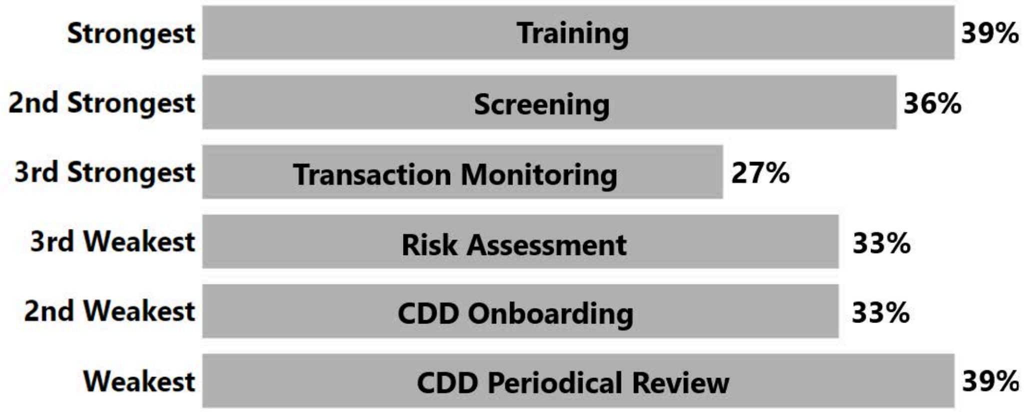
Note: Percentages may not add due to rounding.
Source: PwC Global AWM and ESG Research Centre

Per Exhibit 9, 66% of all respondents have updated their TOM within the last 12 months. Conversely, out of the 34% who reported ‘No’ to updating their TOM within the last year, 29% updated their TOM more than a year ago. However 9% have never updated it. A deeper dive into the survey data shows that 83% of asset managers updated their TOM within the last 12 months, followed by payment institutions (67%) and then banks (55%). For asset managers, outside of operational efficiency and cost management reasons, a key reason for this could be due to an increased focus on ESG (Environmental, Social, and Governance) factors.

There is a growing emphasis on integrating ESG into investment strategies. Asset managers are updating their operating models to include comprehensive ESG criteria, which also encompass AML/CTF considerations. This integration requires significant adjustments to existing processes and systems to ensure that investments are not only profitable, but also ethically sound and compliant with AML/CTF regulations.

AML Control Effectiveness

Exhibit 10: **Most common answer when respondents ranked AML controls by their level of effectiveness**



Note: Respondents were asked to rank controls from strongest to weakest. These are the most common answers for each rank.
Source: PwC Global AWM and ESG Research Centre

As shown in Exhibit 10, 39% of respondents identified 'training' as the most effective AML/CTF control measure. While automation and technical tools support a base level of AML compliance, skilled staff are critical to decision-making in areas such as suspicious activity reports (SARs) and enhanced due diligence (EDD), where AML rules are complex and subject to interpretation. Exhibit 5 of our survey outlines regulation and rules becoming inherently difficult and more guidance being required, so continuous and up-to-date training is crucial to keep up with these changes.

Exploring the data further reveals a paradox: while training is recognised as the most effective AML/CTF control, it tends to attract minimal investment from financial institutions (per Exhibit 7). Only payment institutions (22%) plan to prioritise investment in training over the next two years, prompting questions around the reluctance to invest in what is considered the most effective AML measure. With training identified as the most effective control, it begs the question why training is attracting minimal investment, and if there is a need to switch the dial on the allocation and prioritisation of investment.

The consequences of inadequate training can be severe, and can contribute to substantial fines and reputational damage. For example, in January 2023 the FCA fined 2 banks approximately £4m[12] and £7m[13] respectively for failing to implement adequate AML controls, which included the lack of proper training, exacerbating failings. Therefore, it is critical for financial institutions to make sure that the AML training for their staff is comprehensive, up to date and most importantly, understood.

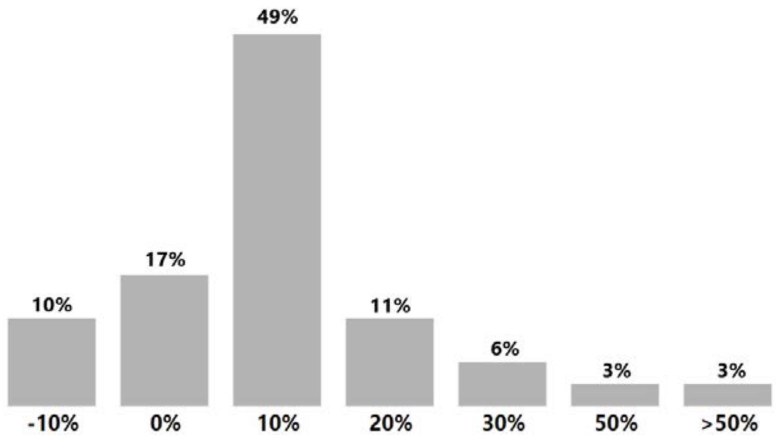
CDD is a key component of the AML/CTF framework within financial institutions. It serves not only as the entry point for onboarding customers, but also as an ongoing risk management measure by way of periodic reviews. Nevertheless, Exhibit 10 shows that 33% of respondents consider 'CDD onboarding' to be the second weakest control in ensuring AML effectiveness, while 39% view 'CDD periodic reviews' as the weakest control. Consequently, it is not surprising that CDD is one of the areas that has seen the highest implementation of digital tools over the past two years, as seen later in this report.

12 Source:https://www.fca.org.uk/publication/final-notices/al-rayan-bank-plc-2023.pdf

13 Source:https://www.fca.org.uk/publication/final-notices/guaranty-trust-bank-uk-limited-2023.pdf

Staffing Challenges: Talent and Recruitment

Exhibit 11: By what percentage do you plan to increase or decrease your staff in AML/CTF control functions?



Note: Percentages may not add up due to rounding.
Source: PwC Global AWM and ESG Research Centre

Our survey indicates that almost three quarters (72%) of respondents are currently considering increasing their staff in AML/CTF control functions by at least 10%, potentially reflecting the need to expand or restructure teams in light of a perceived increase in regulatory pressure as shown in Exhibit 5 earlier. Notably, the only reduction in staff (i.e. a reduction of up to 10%) is made up entirely of asset managers and payment institutions. This reflects a nuanced picture within the industry, with some industry types more likely to downsize staff in AML/CTF control functions.

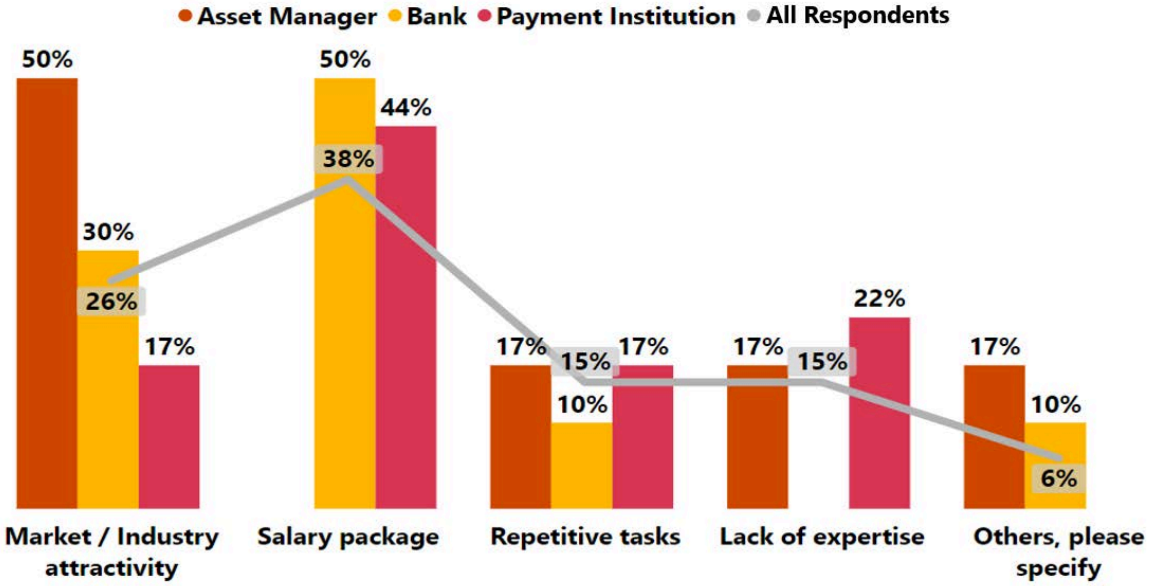
These results may also stem from the financial institutions' internal recruitment strategies: for example, any decrease in staffing may be as a result of outsourcing certain AML roles to third parties, or being able to more cost effectively scale up and down to manage peaks and troughs in the business.

In contrast, staffing increases may stem from the ever evolving regulatory environment. Stricter regulations can require more staff to monitor transactions; financial institutions need knowledgeable staff to adapt to evolving and sophisticated financial crimes. Expansion into new territories would also require additional staff to manage new products and services, with a knock on impact in staffing levels to monitor financial crime. Additionally, the evolving nature of due diligence, shaped by the recent COVID-19 pandemic and digital transformations, as well as the variety of products offered to customers, may necessitate an increased workforce to carry out thorough due diligence processes.

Interestingly, as shown in Exhibit 5 in relation to AML challenges, only 12% of respondents consider recruiting skilled staff as a challenge, with this being more of concern for payment institutions and banks. The skills and knowledge of these staff are greatly valued, given the critical role they play in ensuring AML/CTF effectiveness.

This echoes Exhibit 10 on the previous page, where training was viewed as the most effective control in combating money laundering. Financial institutions seem to recognise the critical importance of skilled AML/CTF staff to their success, with many planning to expand their teams and invest in training, reflecting a commitment to strengthening their AML/CTF capabilities.

Exhibit 12: **What is the most important blocking factor for retaining talents in your AML/CTF related activities?**



Note: Percentages may not add due to rounding.
Source: PwC Global AWM & ESG Research Centre

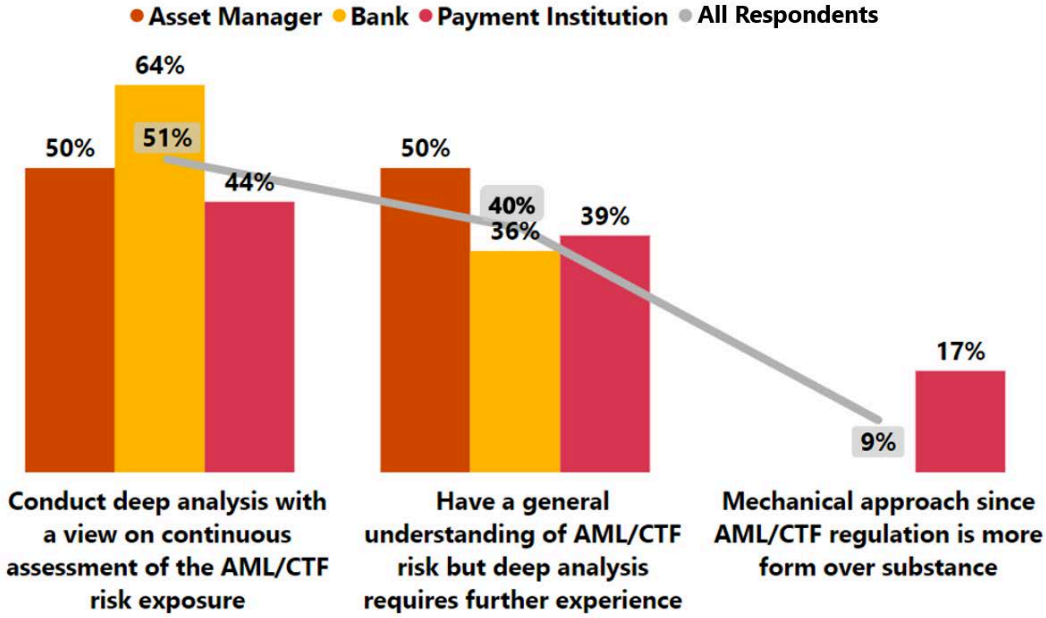
As seen in Exhibit 12 above, survey respondents have indicated the primary challenges they face in retaining talent within AML/CTF related activities. The predominant issue, cited by 38% of respondents, is the compensation offered.

A closer examination reveals that banks report the most difficulty in this area, with 50% attributing talent loss to salary packages, compared with 44% of payment institutions. Interestingly, asset managers do not consider compensation to be a concern. This variation may reflect differences in business models, regulatory pressures, or the availability of AML professionals across these sectors.

The limited attractiveness of the market/ industry was cited as the second most important blocking factor (26%). Additionally, 15% of respondents identified the lack of expertise and the monotony of tasks as contributing factors to talent attrition. It could be argued that employees are seeking more dynamic and varied roles in the industry. To address this issue, the introduction of automation in repetitive tasks could play a crucial role. By leveraging technology and automation, financial institutions can make roles within the AML/CTF sector more appealing and retain talent more effectively.

These findings are consistent with those from the broader EMEA survey, which highlighted similar concerns across various regions. The consensus suggests that these are not isolated issues, but rather widespread challenges within the industry.

Exhibit 13: **Which AML approach do most of your staff follow?**



Note: Percentages may not add due to rounding.
Source: PwC Global AWM and ESG Research Centre

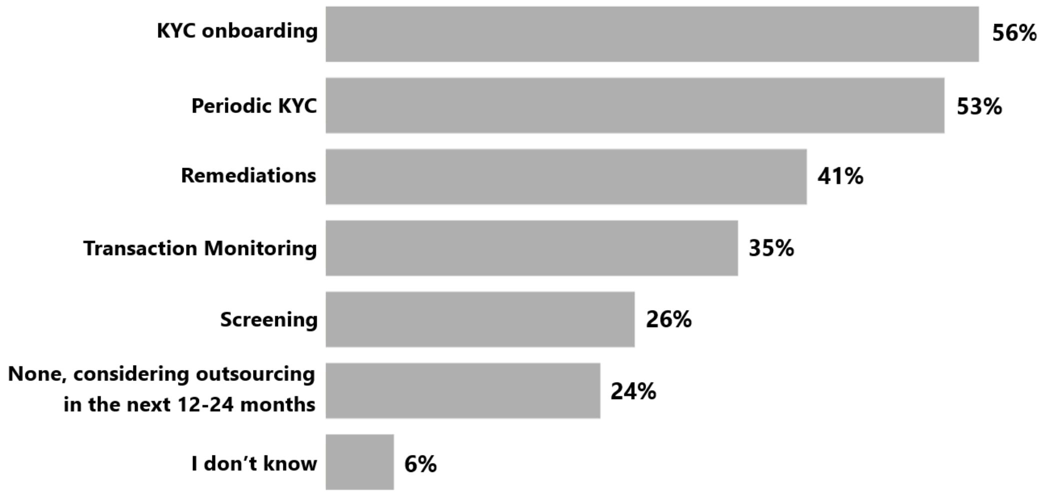
Exhibit 13 shows that the perception of how AML rules and regulations are applied by staff within financial institutions is largely positive. Only 9% of respondents believe that their AML staff follow a 'mechanical approach', while 51% believe that their staff 'conduct deep analysis'. Such a trend suggests a maturity in financial institutions, and that most employees are not just well-versed in essential AML principles, but are also adept at utilising their expertise in practical scenarios. This reflects a workforce that is both knowledgeable about the core AML regulations and is skilled in their application - factors conducive to a robust compliance environment.

However, some areas do require improvement.
For example, 40% of respondents believe that their staff have knowledge of AML/CTF risk exposure, but need more experience. This reinforces the importance of two key strategies highlighted in this report: the improved training of staff and the retention of qualified staff. These strategies will ensure that staff have the requisite skills to conduct deep analysis.

It is only payment institutions (17%) which state that their staff use a mechanical or checklist driven approach, in contrast to a more analytical approach, where decisions are made based on a deeper understanding of the risks involved and the application of professional judgement.

The inclination of payment institutions towards a mechanical approach to AML/CTF compliance could be attributed to a combination of regulatory expectations, the nature of their business model, compliance culture, technological capabilities, and risk appetite. It is important to recognise, however, that while a mechanical approach can offer certain benefits, such as consistency and efficiency, it may not always be as effective in identifying and mitigating complex money laundering or terrorist financing risks, which require a more nuanced and risk-based analysis.

Exhibit 14: **Which AML/CTF control activities are you outsourcing?**



Note: Multiple choice question. Respondents were asked to select their top three answers.
Source: PwC Global AWM and ESG Research Centre

Financial institutions are navigating a future that demands agility within its financial crime framework, whether through streamlining costs, focussing on essential operations, re-assessing risk appetites, or adapting to regulatory changes. These strategic choices can carry challenging operational and technological hurdles, sometimes too complex to tackle without additional support.

To navigate these complexities, many financial institutions are turning to outsourcing, particularly managed services, as a means to efficiently manage money laundering risks and meet regulatory obligations. This approach not only offers cost efficiency through a blend of onshore and offshore services, but can also integrate innovative technologies to enhance effectiveness. Among the most commonly outsourced AML/CTF activities are 'KYC onboarding' (56%) and 'periodic reviews' (53%).

The creation of KYC and periodic review outsourced solutions presents its own set of challenges for financial institutions. Institutions may be required to conduct client due diligence checks that vary across jurisdictions, manage a variety of data and workflows, and ensure efficient data processing systems to collect and assess risk relevant information. Complications can arise from non-standard interfaces and outdated legacy systems, which can significantly hinder processes, and the technical obstacles associated with improving these systems can demand substantial resources.

While custom solutions provide specificity, they come with their own risks and costs, such as ongoing maintenance and ensuring regulatory compliance. In light of these challenges, it is no surprise that financial institutions may choose to outsource KYC onboarding and periodic reviews as a beneficial strategy. It can offer financial institutions advantages such as:

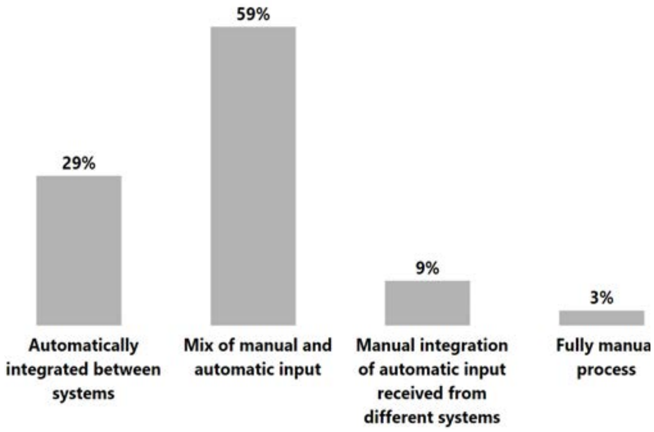
- additional capacity and cost savings through access to trained professionals and teams that can be scaled up and down;
- access to specialised knowledge; and
- access to advanced technological solutions including third party data integrations, analytics, AI and GenAI.

Any of these may be beyond the current investment scope or operational capacity of financial institutions.

24% of respondents indicated that they do not currently outsource their AML control activities, but have plans to pursue outsourcing within the next one to two years. Further examination uncovers industry differences as there seems to be a hesitance among asset managers to outsource AML control activities. A higher proportion of asset managers (33%) appear not to currently outsource their AML/CTF control activities, compared with 28% of payment institutions and 10% of banks. Various factors could contribute to this including, for example, the wish to maintain direct oversight and control over compliance processes by keeping things in-house to manage risk, or cost constraints. Outsourcing can introduce risks related to third-party management and data security, which they may find untenable.

Data Collection

Exhibit 15: How do you collect data for AML reporting, either for internal or regulatory purposes?



Note: Percentages may not add up due to rounding
Source: PwC Global AWM and ESG Research Centre

Data collection is an essential part of AML/CTF operations as it is needed to understand clients, perform analysis, and provide reports. As expected, the majority of data collection methods are a mix of manual and automatic input (59%).

Just over a quarter of respondents (29%) reported that they streamline data collection through automatic integration between their systems. However, a small proportion (9%) still rely on manual integration of automatic input received from different systems and an even smaller proportion (3%) still have fully manual processes. These results are in line with responses across the wider EMEA region. Manual data collection methods can have a number of negative operational impacts as they are inherently more time-consuming and more prone to user input error. Staff may spend considerable amounts of time gathering information, which can lead to delays in the analysis and reporting of suspicious activities. This inefficiency is exacerbated in the context of financial institutions where the volume of transactions and the breadth of data required for AML/CTF compliance can be substantial.

The time spent on manual data entry could be better utilised in analytical pursuits or more strategic tasks that add value to the AML/CTF framework. Manual data collection can also lead to data being siloed or stored in inconsistent formats, making it difficult to integrate and access information across different departments or systems. This lack of integration can impede comprehensive monitoring and analysis, as staff may not have a holistic view of the data necessary to identify patterns indicative of money laundering or terrorist financing.

Human error is another significant risk in manual data collection. Mistakes such as miskeying information, overlooking critical data, or misinterpreting complex transaction patterns can lead to inaccurate records and poor data quality. In the realm of AML/CTF, where precision is crucial for identifying and reporting suspicious activities, such errors can have serious consequences, including regulatory penalties, reputational damage, and the potential for illicit activities to go undetected.

It is worthwhile noting that banks are often hindered by legacy systems and organisational structures that impede swift digital adoption. This highlights the broader struggle within the banking industry to evolve digitally. Some banks may be wrestling with deep-rooted procedures and a culture that is less amenable to change. The contrast between their high-tech ambitions, the resistance from long-standing practices and the weight of technological 'debt' illustrates the intricate path banks must navigate in their digital transformation journey.

There are however noticeable disparities across Europe when it comes to data collection as highlighted in the wider EMEA survey. Financial institutions from the UK and Ireland are lagging behind, and the least likely to have such automatically integrated data between systems in place (16%), with respondents from France, the Nordics and Central and Eastern Europe (CEE) more likely (all over 30%) to have these systems in place.

Exhibit 16: Regional breakdown- respondents that selected 'Automatically integrated between systems'

Note: Percentages may not add due to rounding.
Source: PwC Global AWM and ESG Research Centre

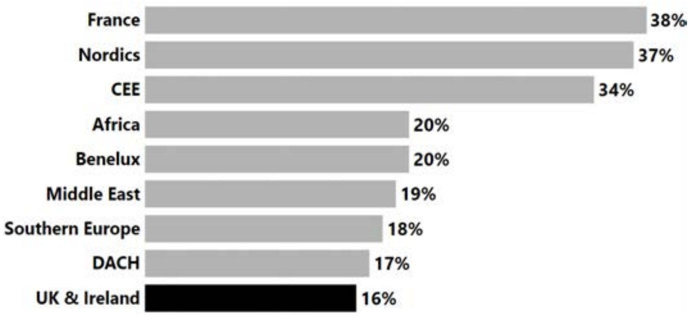
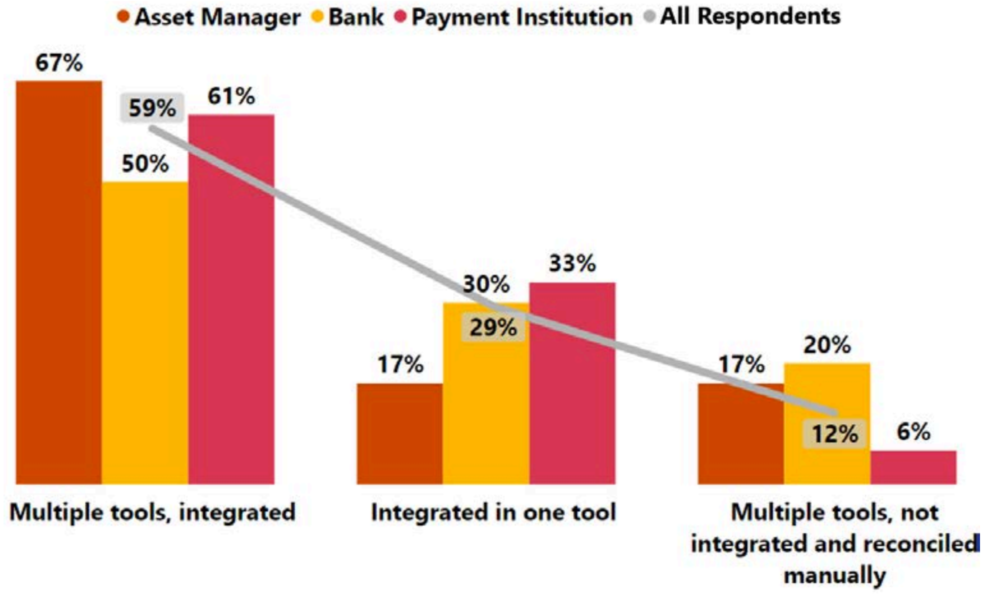


Exhibit 17: **How do you store the clients' KYC documentation that is regularly consulted for AML/CTF controls?**



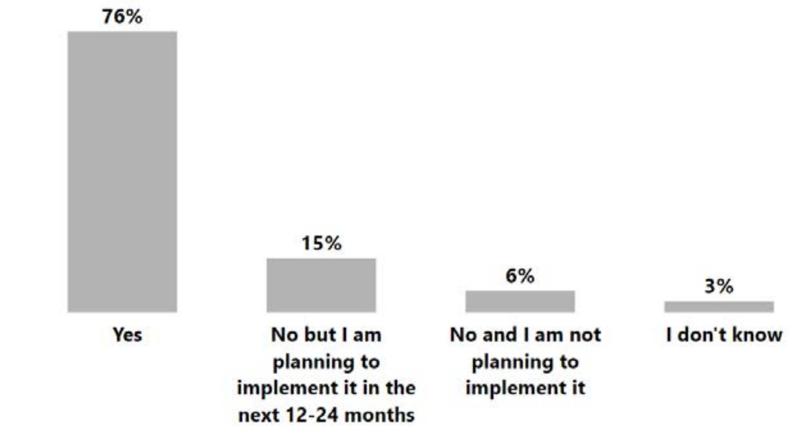
Note: Percentages may not add due to rounding.
Source: PwC Global AWM and ESG Research Centre

With regards to the storage of KYC documentation, the majority of respondents (59%) employ a variety of integrated tools to manage their KYC data. The integration of multiple tools allows users to leverage the strengths of various systems. Conversely, 29% of respondents prefer the use of one integrated tool. This is likely due to the benefits of having a centralised access point, a more holistic customer view in one tool, as well as the potential efficiency it brings to data management. However, a small proportion of respondents (12%) use multiple tools that are not integrated and are reconciled manually. Although this can provide opportunities for oversight and the flexibility to adapt to each situation, it may be deemed inefficient and brings an increased risk of human error.

Customer Due Diligence

Exhibit 18: Do you use any remote verification systems for customer due diligence purposes?

All respondents



Industry breakdown of respondents that responded with 'Yes'

Note: Percentages may not add due to rounding.
Source: PwC Global AWM and ESG Research Centre

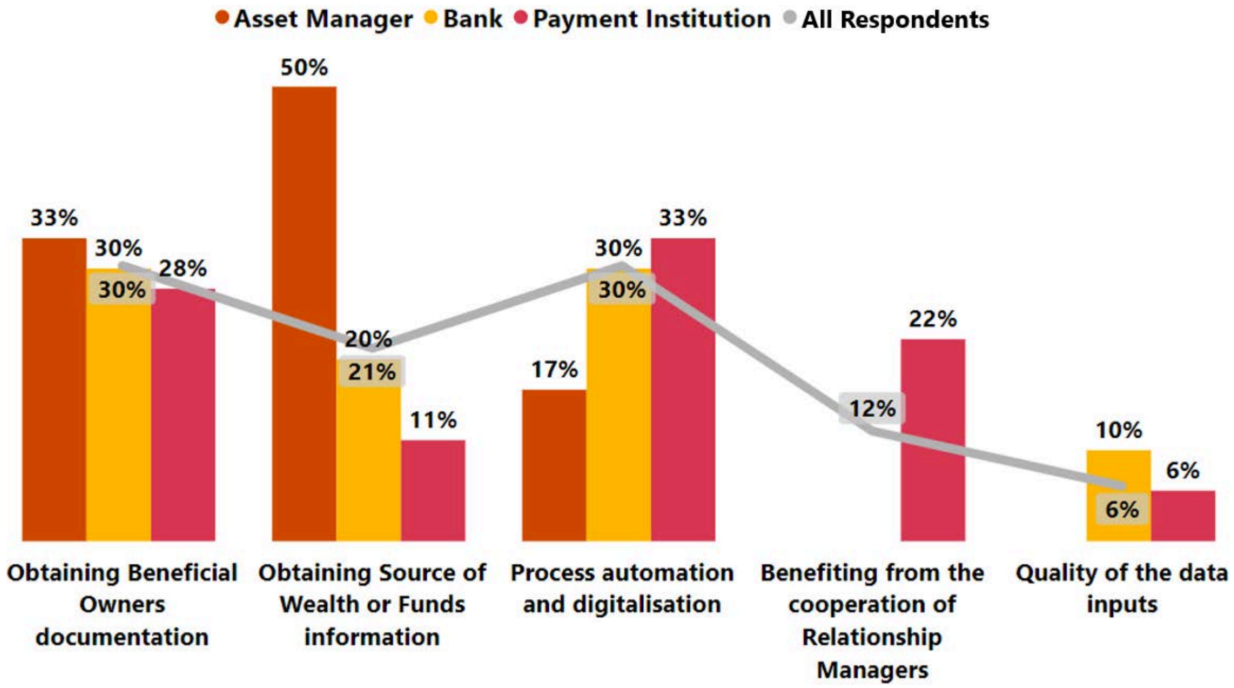
Remote verification systems for CDD can be highly beneficial for financial institutions. They offer convenience for customers, allowing them to complete the CDD process from anywhere without the need for a physical presence. They can enhance the speed, accuracy and efficiency of the verification process. Implementing and maintaining remote verification systems does, however, require significant investment in technology and training. Financial institutions must ensure that their staff are well-versed in these systems and are able to handle any exceptions or issues that arise, echoing the need for skilled staff raised in this report. Remote verification systems are, however, heavily dependent on the quality and availability of data. They typically use a combination of biometric verification, document verification, and data checks against various databases, and if the data sources are outdated, incomplete, or incorrect, the reliability of the verification process can be compromised.

It is not surprising that over three quarters (79%) of financial institutions included in this survey have adopted remote verification for CDD processes, potentially reflected in Exhibit 24 where customer due diligence was the second most common reason for implementing new digital tools to enhance AML/CTF activities. A closer look at the industry breakdown reveals that 72% of payment institutions, 80% of banks, and 83% of asset managers are utilising this verification approach.

Furthermore, 15% of all respondents in the survey expect to integrate these systems within the next two years, continuing the trend towards the automation of CDD processes. These institutions must ensure that the use of automation enhances efficiency without detracting from the attention that staff must maintain on CDD. CDD is a sophisticated process which, even when automated, still relies on the expertise of AML personnel.

As remote verification systems involve the collection, processing, and storage of sensitive personal data, this raises concerns about data security and privacy, particularly in the event of a data breach. This may help explain why ‘simplification of data sharing rules’ was highlighted as one the top regulatory changes required to improve AML/ CTF effectiveness earlier.

Exhibit 19: Which is the most critical factor in performing your customer due diligence process effectively?



Note: Percentages may not add due to rounding.
Source: PwC Global AWM and ESG Research Centre

As shown in Exhibit 19, 30% of respondents cite automation and digitisation of information as being the most important factor in performing CDD processes effectively. The same proportion (30%) believe that obtaining documentation on beneficial owners is the most critical. An industry breakdown shows that there isn't a significant variance between asset managers, banks and payment institutions, in 'obtaining beneficial ownership documentation' as a critical factor in performing their CDD processes effectively.

Obtaining beneficial ownership documentation is particularly crucial for asset managers due to the nature of their business, which often involves managing substantial sums of funds on behalf of their clients, who may be individuals, corporations, or other, more complex, legal entities. Asset managers are entrusted with the discretion to invest and manage these funds, which can include the acquisition of assets that could be used to conceal the true ownership and origins of illicit funds.

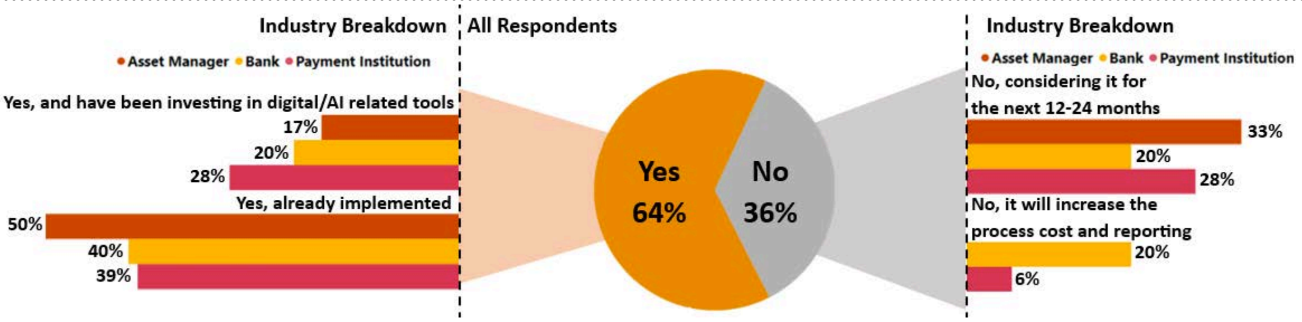
By obtaining and verifying beneficial ownership information, asset managers can ensure they are not unwittingly facilitating money laundering or terrorist financing activities. This level of due diligence is essential not only for legal compliance, but also for maintaining the integrity of their investment operations and protecting their reputation.

However, for asset managers, the identification of beneficial owners is a key component in understanding the risk profile of the funds they manage and ensuring that they are not exposed to potential financial crime risks associated with opaque ownership structures.

The nature of their customers, products and services are also likely to be why 50% of asset managers responded that obtaining source of funds or source of wealth was critical compared to banks (20%) and payment institutions (11%).

These results are in line with the wider EMEA survey and highlight the need for UK institutions to place a renewed focus on quality data collection. The tendency to approach CDD as a routine task leads to the initial collection of client data that is inadequate. This shortfall in comprehensive and accurate data collection at the outset of the client relationship hampers the integrity of other AML controls and as a result, financial institutions find themselves needing to gather further customer data at subsequent stages. This issue is particularly critical given that the efficacy of screening, transaction monitoring, and risk assessment is contingent upon the availability of accurate data. Therefore, maintaining high standards of data quality is essential for the robustness and reliability of the CDD process.

Exhibit 20: Are you considering moving to a perpetual KYC process?



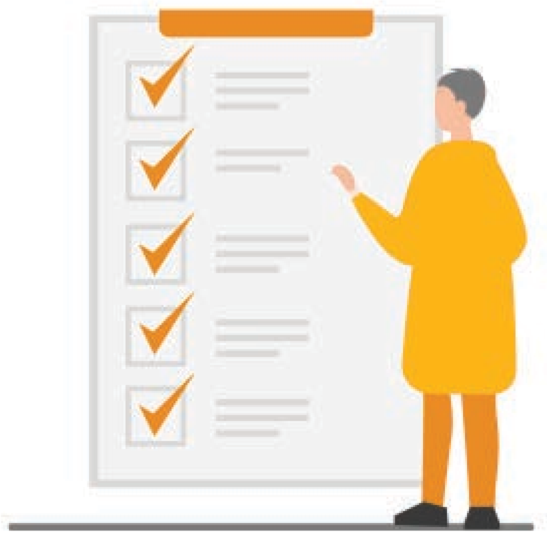
Note: Percentages may not add due to rounding.
Source: PwC Global AWM and ESG Research Centre

Perpetual KYC is a continuous method of customer due diligence that utilises technology and data analytics to constantly update and assess customer risk profiles. Unlike traditional KYC, which verifies customer information at the start of the relationship and reviews it periodically (e.g., every one, two, or five years based on risk category). Perpetual KYC is an ongoing process. It ensures customer data remains current and accurate by regularly monitoring and updating information based on events and changes in the customer's status, rather than at fixed intervals.

As shown in Exhibit 20, 64% of respondents are currently implementing perpetual KYC and a further 26% of all respondents who answered ‘No’ are considering transitioning to perpetual KYC in the next 12 to 24 months, with a third of asset managers reporting this to be the case. However, 9% of all respondents believe a move to perpetual KYC would be costly, preferring to follow more traditional KYC processes.

The adoption of perpetual KYC by financial institutions is a response to the increasing complexity and velocity of financial crime, as well as the need for more robust and proactive risk management practices. By maintaining an ongoing understanding of their customers, financial institutions can more effectively detect financial crimes, and apply more appropriate risk based customer treatments.

For AML/CTF professionals, the implementation of perpetual KYC represents a significant shift from periodic customer reviews to a more continuous and responsive model. The trend towards increasing usage of technology within the KYC process is mirrored in Exhibit 25, where 86% of respondents say they already use KYC digital tools, while 9% are planning to implement them within the next two years.



3 Technology

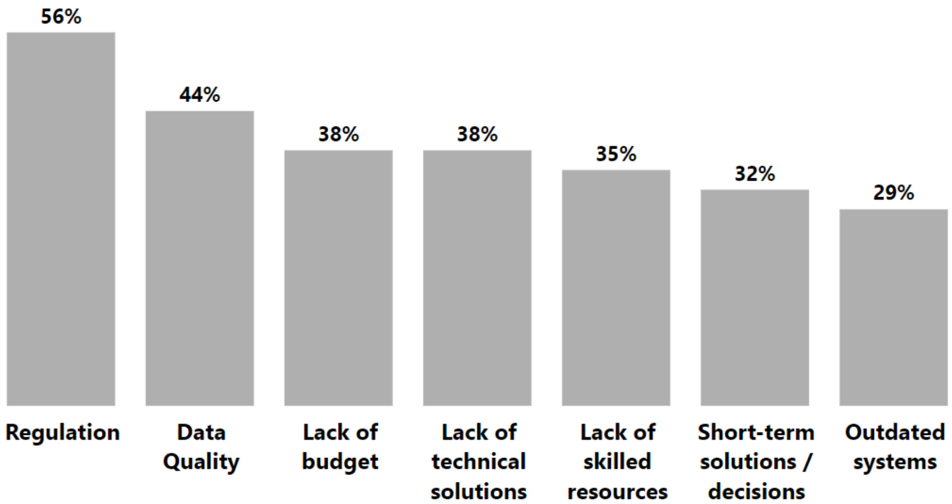
Technology: Embracing Digital Tools

Financial crime compliance can sometimes be classed as inefficient due to manual processes or because of the limited use of technology to help pinpoint financial crime risks. This, of course, will always be dependent on the strategy of the financial institution, its approach to risk management and appetite for investment in new technology (or technology upgrades).

In the evolving UK financial sector landscape, particularly in the post-Brexit era, technology has emerged as a pivotal force in fortifying financial institutions against the complex challenges of AML/CTF. As the UK redefines its financial system framework to maintain its global preeminence outside the EU, the adoption and integration of advanced technological solutions are not merely advantageous but essential. These innovations offer robust mechanisms for detecting and preventing financial crimes, ensuring compliance with ever-stringent regulatory demands, and fostering trust in the integrity of the UK's financial markets. Both AI and digital tools are helping to transform certain AML/CTF activities, with the majority of survey respondents already adopting them within their AML processes.

This survey seeks to explore the strategic role of technology in enhancing AML/CTF efforts, scrutinising its effectiveness, and anticipating future developments that will shape the resilience of financial institutions in the UK. Through this lens, we aim to understand how technology will underpin the security and prosperity of the financial sector in the years to come.

Exhibit 21: What are the blocking factors for increased use of new technologies in your financial institution?



Note: Multiple choice question. Respondents were asked to select their top three answers.
Source: PwC Global AWM and ESG Research Centre

The main blocking factor for the increased use of new technologies reported by respondents is ‘regulation’ (56%). The rapid pace of technological advancement often outstrips the development of corresponding regulatory frameworks. This creates a landscape of regulatory uncertainty where financial institutions may be hesitant to adopt new technologies due to the lack of clear guidelines and knowledge of how to navigate them, or potential future regulatory changes. The fear of non-compliance or the need for subsequent adjustments can deter institutions from investing in new technologies.

Data privacy and security requirements in the UK could be another regulatory issue making institutions nervous about implementing new technology. Financial institutions will want to ensure that any new technologies adopted are fully compliant with UK General Data Protection Regulation (UK GDPR), so that they do not expose themselves to the risk of fines or even reputational damage, which could result in the loss of customers.

Additionally, Exhibit 21 reveals that 44% of survey respondents identify data quality as another significant barrier to the adoption of new technologies. The customer onboarding process relies on strong data quality to ensure ID&V checks are accurate. If there are data quality gaps such as missing names or misspelling, this can impact the effectiveness of ID&V and subsequent screening checks. Therefore, navigating any data quality issues (i.e. how data is recorded at source, and how this is integrated with financial crime technology solutions) is understandably a key concern.

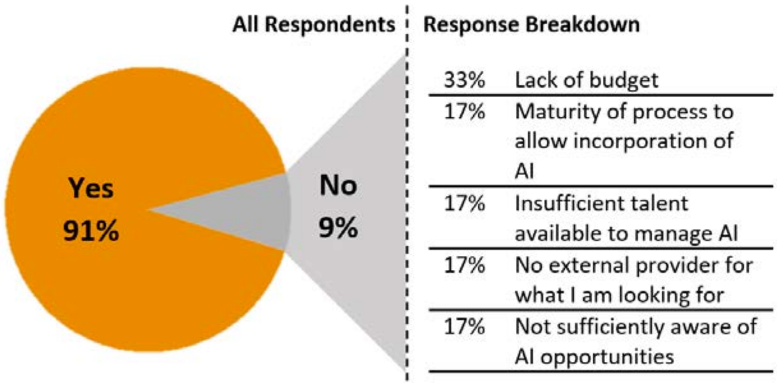
The implementation of new technologies requires thorough quality analysis and remediation of data inputs to ensure effective quality outputs. This blocking factor is closely followed by the lack of budget, and the lack of technical solutions. In contrast, respondents to the wider EMEA survey cited that 'data quality' was the number one blocker to the increased use of new technologies, followed by 'lack of budget', and then 'regulation'.

The lack of skilled resources is another prevalent issue that institutions have reported. Even when institutions are willing to invest in new technologies, the cost and time required to train existing staff or hire new experts can be prohibitive. Training programmes need to be comprehensive and ongoing to keep pace with the rapid evolution of technology. This can divert resources away from other critical areas, creating a bottleneck in the adoption process.

Many financial institutions operate on legacy systems that are not easily compatible with new technologies. Skilled professionals are required to bridge the gap between old and new systems, ensuring seamless integration. Without such expertise, institutions may face significant technical challenges that hinder the deployment of innovative AML/CTF solutions. Addressing this skills gap is essential for institutions to fully realise the potential of advanced technological solutions in combating financial crime. Investing in training and development, attracting top talent, and fostering a culture of continuous learning are critical steps towards overcoming this challenge.

The Focus is on AI

Exhibit 22: Are you considering the implementation of artificial intelligence (AI) into your processes/workflow? If No, why not?



Note: Percentages may not add due to rounding. Multiple choice question.
Source: PwC Global AWM and ESG Research Centre

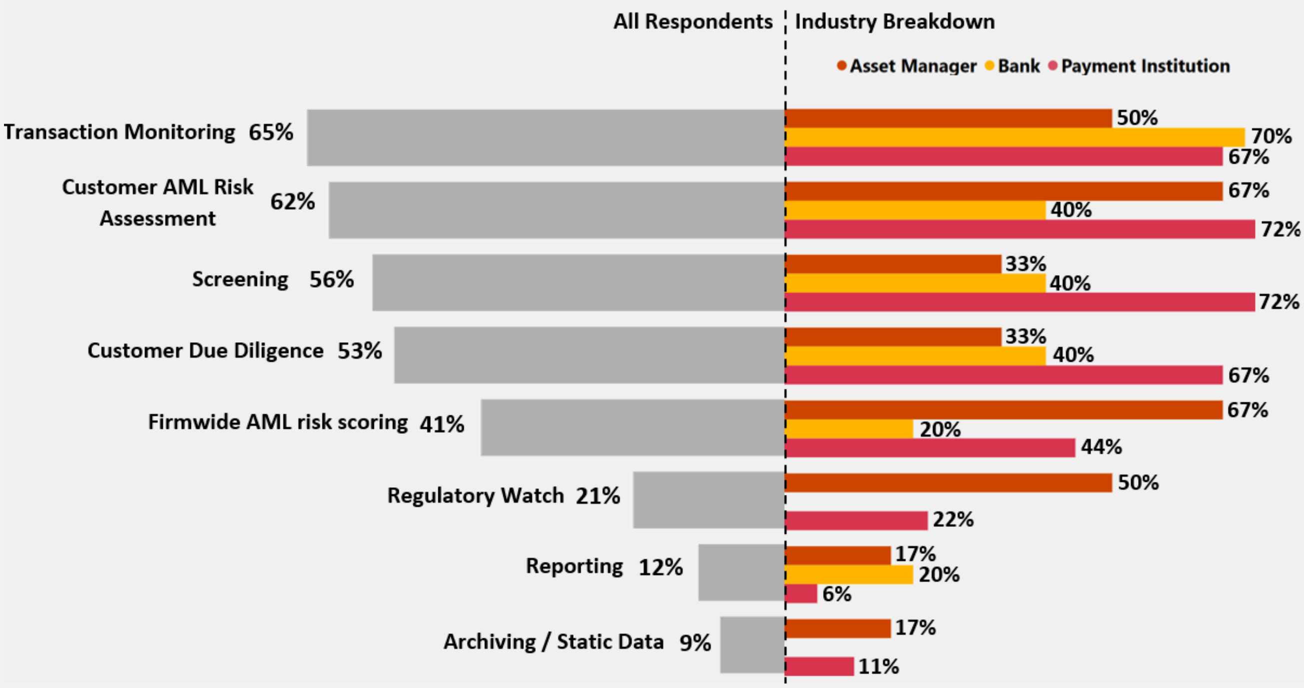
The considerable interest in implementing AI across AML/CTF processes is evident: 91% of respondents acknowledge its potential benefits. This sentiment is shared across industries (83% of asset managers, 90% of banks, and 94% of payment institutions), highlighting the growing recognition of AI's ability to improve AML processes. AI-driven solutions can automate many routine tasks involved in AML/CTF processes, such as transaction monitoring, customer due diligence, and regulatory reporting. This automation not only speeds up these processes, but also reduces the need for extensive manual intervention, leading to significant cost savings for financial institutions.

AI systems can analyse vast amounts of data at unprecedented speeds, identifying patterns and anomalies that may indicate suspicious activities. Machine learning algorithms can be trained to recognise complex money laundering and terrorist financing schemes that traditional rule-based systems might miss. One of the major challenges in AML/CTF compliance is the high rate of false positives generated by traditional monitoring systems. AI can significantly reduce these false positives by using advanced analytics and machine learning to better distinguish between legitimate transactions and those that warrant further investigation. This allows compliance teams to focus their efforts on genuine threats.

A minority of respondents (9%) said that they were not considering implementing AI. Exhibit 22 shows the reasons why some industries may be unable or unwilling to implement AI, with one third of respondents stating 'lack of budget' as a blocker. 'Insufficient talent available to manage AI' was also highlighted as a reason for not implementing AI. This is echoed in Exhibit 32 later in this report, where resourcing of skilled staff for transaction monitoring was highlighted as a challenge to transaction monitoring processes, despite it being the top area where firms are considering introducing AI (see Exhibit 23).

The benefits (and risks) of AI have come under the spotlight in recent years. In April 2024, the FCA detailed its approach to AI, noting that it is focused on how firms can responsibly adopt the technology, whilst ensuring that regulatory expectations are met. The FCA recognises that future regulation will likely need to adapt as a result of AI, noting that *'many risks related to AI are not necessarily unique to AI itself and can therefore be mitigated within existing legislative and/or regulatory frameworks'* and that institutions may need to change their approaches to firm risk management and governance. The FCA acknowledges, however, that they will need to continue to build an in-depth understanding of how AI is used by financial institutions before making any changes to regulation, to ensure changes are *'proportionate to the risks, whilst creating a framework for beneficial innovation.'*

Exhibit 23: **In which area do you consider introducing AI in your AML/CTF activities?**



Note: Multiple choice question.
Source: PwC Global AWM and ESG Research Centre

Exhibit 23 shows where financial institutions are considering adopting AI within the AML/CTF process. The main area of focus is 'transaction monitoring' (65% of respondents), closely followed by 'customer AML risk assessment' and 'screening' (62% and 56% respectively). This is reasonable, given these activities are time and resource intensive, therefore using AI to automate the process would reduce the administrative burden, free up much-needed resources and enable cost savings. However, consideration must be given to how data quality will be maintained as both an input and output (a key concern per Exhibit 21).

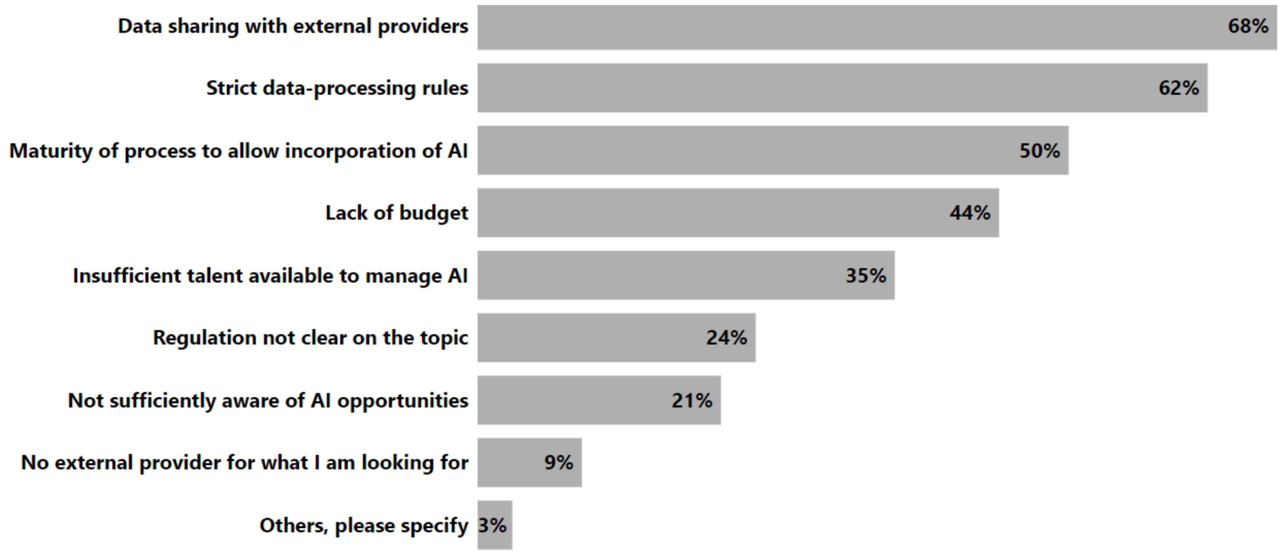
The focus on transaction monitoring and customer due diligence is consistent with investment priorities in Exhibit 7, showing again that they are high on the agenda, and that financial institutions are clearly leaning towards AI to make processes more effective and efficient. In comparison, despite 'screening' being cited as a key area for AI in Exhibit 23, it was ranked as one of the lower priorities for investment focus (as seen in Exhibit 7). The application of AI in the financial services industry has grown rapidly, offering opportunities for innovation, efficiency and improved customer outcomes.

However, the regulatory position on AI technology has remained in its infancy, leaving many financial institutions to manage AI applications and the related financial crime risks with uncertainty. One thing is clear from the FCA AI update[14]: a financial institution's decisions remain the responsibility of its management bodies, regardless of whether those decisions are taken by AI based tools, including scenarios where third-party AI technologies are utilised.

Payment institutions were the most inclined to introduce AI into a wide range of areas, with a high proportion indicating that they would consider AI in 'transaction monitoring', 'customer AML risk assessment', 'screening' and 'CDD'. Payment institutions, often being newer and more technologically agile than traditional banks and asset managers, are more inclined to integrate cutting-edge technologies like AI. These institutions typically have less legacy infrastructure, which allows for easier and faster implementation of new technologies. The ability to quickly adapt and innovate is crucial in the fast-paced financial technology landscape.

[14] Source: FCA AI Update, published 22 April 2024

Exhibit 24: **Which type of constraints do you see in applying AI tools to your AML/CTF activities?**



Note: Multiple choice question.
Source: PwC Global AWM and ESG Research Centre

Exhibit 24 shows that 68% of respondents identified data sharing with external providers as the primary challenge in integrating AI tools into their AML/CTF activities. This concern likely links to regulation being the key blocking factor for new technologies (in Exhibit 21), and highlights the sensitivity and risk associated with the handling of data in the context of AML/CTF activities. Any violation of UK GDPR may lead to potential fines or severe reputational damage, resulting in customers moving their business elsewhere as they lose trust in their financial institutions and their ability to adequately protect customer data. It is therefore logical that 'strict data processing rules' are cited as another constraint in implementing AI into AML/CTF activities (62%). Protection of, and fairness for, data subjects is also referenced through the FCA's AI update.

The recurring themes of limited budgets, insufficiently skilled staff, and a lack of suitable providers resurface as obstacles to applying AI, and are also echoed in Exhibit 22 above. Moreover, 50% of all respondents indicated that their processes are currently not mature enough to permit effective AI implementation into AML/CTF activities, suggesting that investment needs to be made into upgrading these systems before AI can be considered.

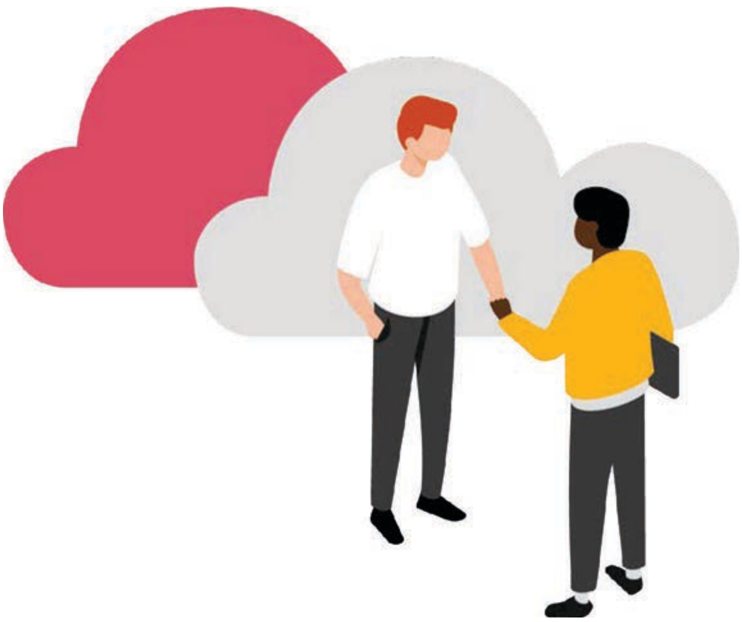
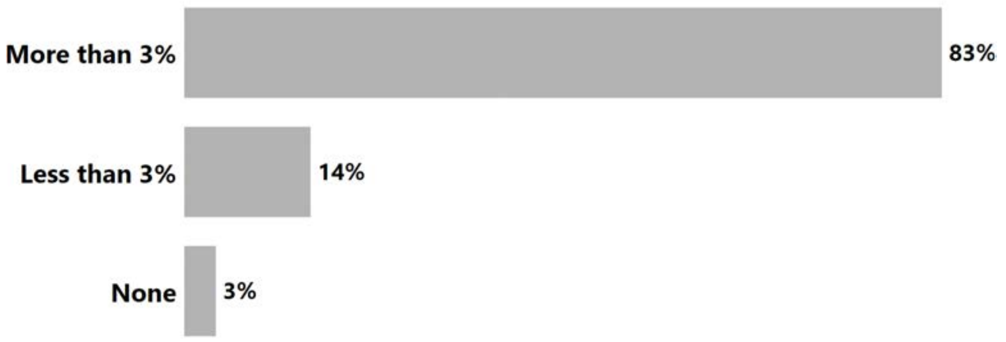


Exhibit 25: **What portion of your AML/CTF budget do you plan on investing in AI tools over the next 24 months?**

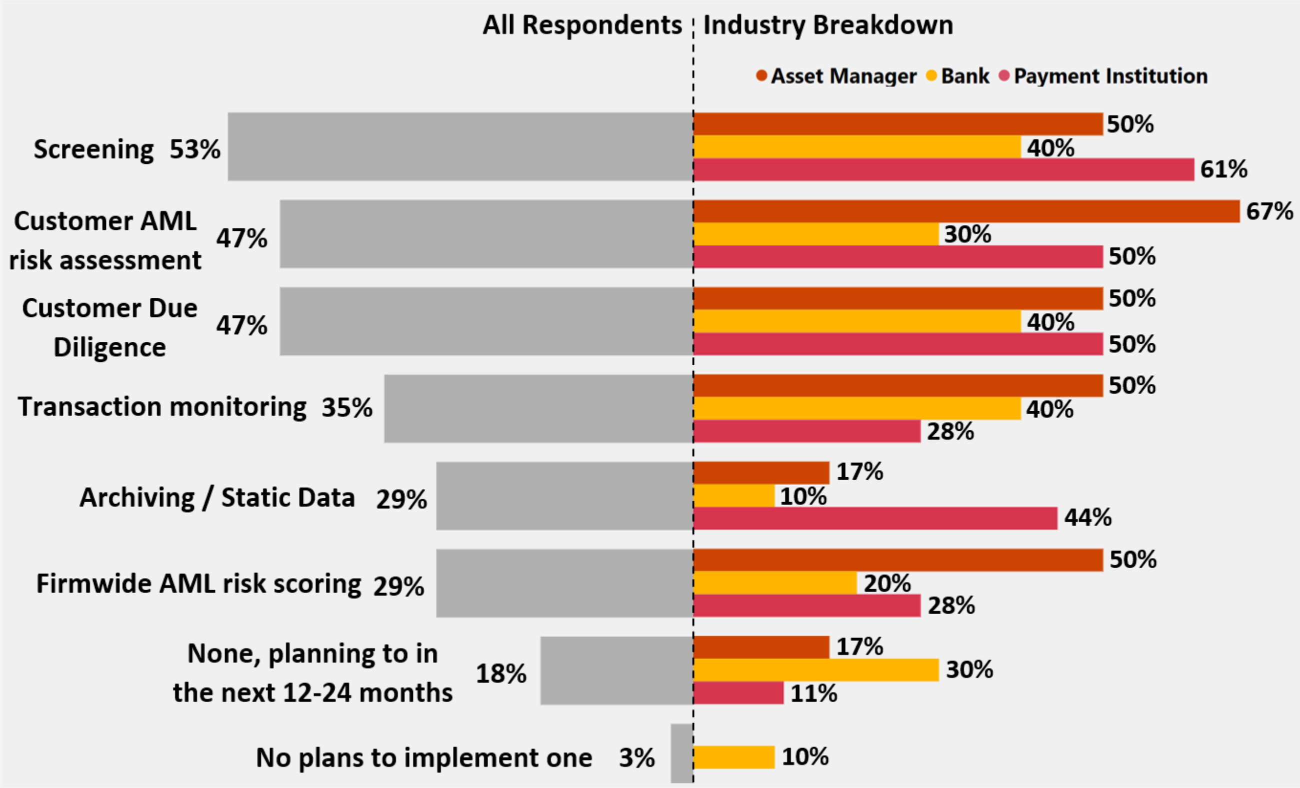


Note: Percentages may not add due to rounding.
Source: PwC Global AWM & ESG Research Centre

Given the potential of AI, it is not surprising that 91% of respondents are contemplating its implementation as seen earlier in this section. Despite being cognisant of the constraints that may accompany AI usage, an impressive 97% still intend to invest in it within the next two years, as illustrated in Exhibit 25. A notable 83% of respondents plan to spend more than 3% of their budget over the next two years on AI investment. Such investment is indicative of AI's potential to enhance processes and improve accuracy and efficiency across AML. It will be interesting to observe how this materialises in practice over the next few years. Lack of budget has consistently been cited as a blocking factor to adopting new technologies, and so it remains to be seen whether financial institutions will follow through on their intentions.

Digital Tools: Enhancing Efficiency

Exhibit 26: **In which area did you implement a new digital tool to enhance your AML/CTF activities in the last 24 months?**



Note: Multiple choice question.
Source: PwC Global AWM and ESG Research Centre

Transaction monitoring is a cornerstone of AML and is seen as a key focus, as demonstrated by Exhibit 7 (investment priorities), Exhibit 23 (AI integration) and Exhibit 10 (strong controls). Despite this, it only ranks fourth among the areas in which respondents have implemented a new digital tool in the last two years. This could suggest that some respondents are focusing on relying on existing transaction monitoring tools and enhancing these, rather than implementing new systems, with new suppliers.

'Screening' (53%), 'customer AML risk assessment' (47%) and 'CDD' (47%) are the areas which have seen the highest implementation of digital tools over the past two years. These categories were also identified as likely candidates for AI integration in Exhibit 23, suggesting that technology usage in these areas has already been successful and respondents are keen to benefit further from advanced technologies such as AI.

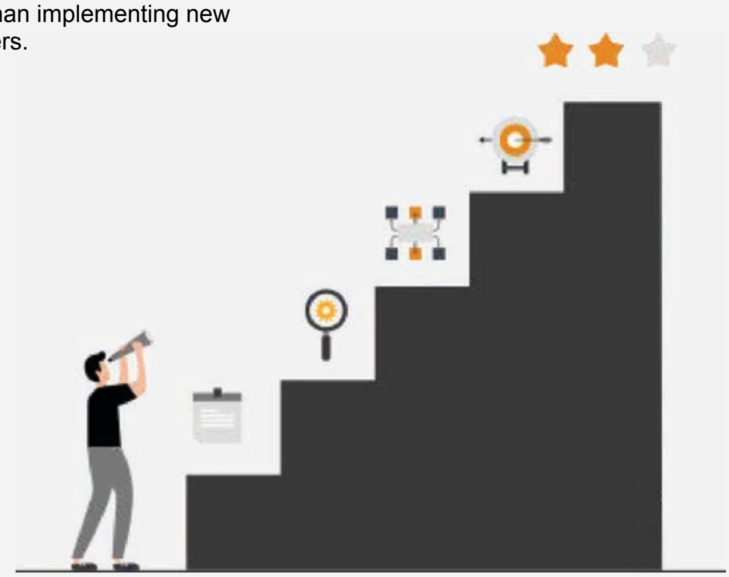
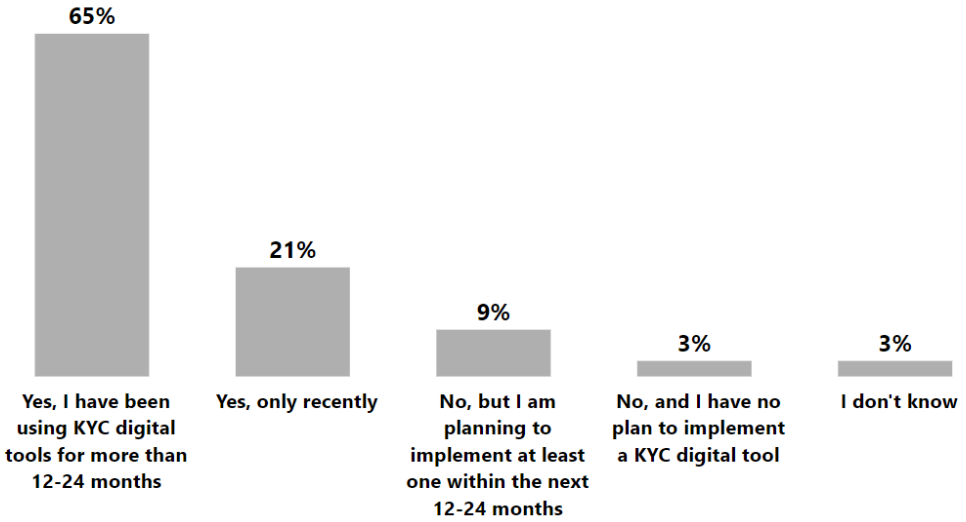


Exhibit 27: Have you implemented any KYC digital tool to facilitate your KYC process?

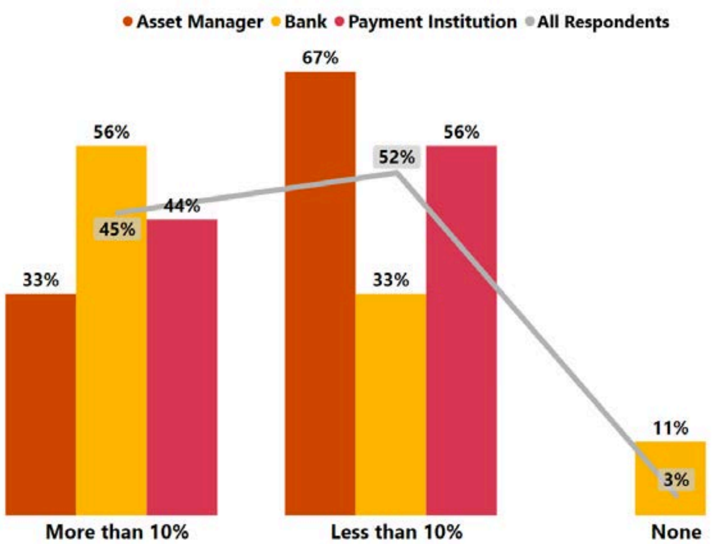


Note: Percentages may not add due to rounding.
Source: PwC Global AWM and ESG Research Centre

Per Exhibit 27, the majority (65%) of respondents have been leveraging digital tools (such as electronic identification via video selfies) to enhance the KYC process for at least one year. The fact that 21% have also recently started to implement these tools, with a further 9% planning on doing so, shows the recognition within the industry of the efficiency that digital tools permit.

It is likely that one reason for the popularity of these digital tools is their ability to streamline the KYC process, which links to our earlier finding, where one of the main challenges faced by institutions was the updating of KYC documentation. The use of digital tools may also help to alleviate the repetitiveness of some KYC processes, which may in turn help with staff retention (see Exhibit 12, where repetitive tasks were cited as a key driver of attrition), and allow staff to concentrate their efforts on more challenging and complex areas.

Exhibit 28: What percentage of your AML/CTF budget do you expect to invest in digital tools in the next 24 months?

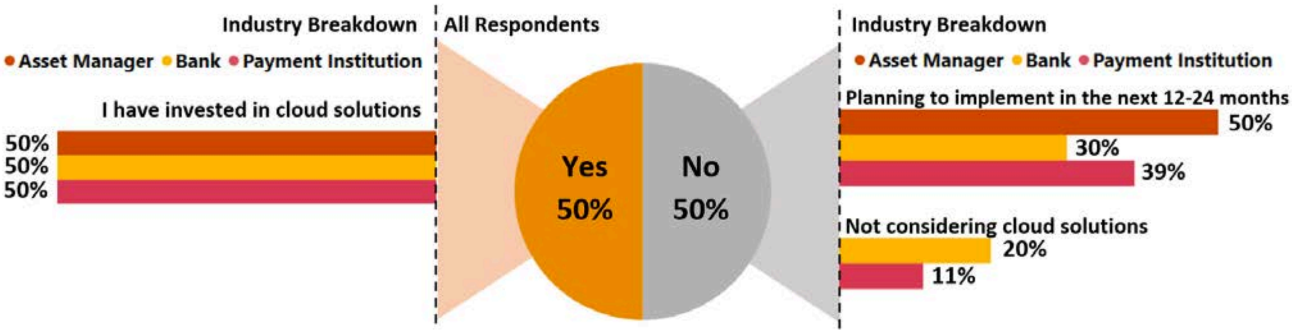


Note: Percentages may not add due to rounding.
Source: PwC Global AWM and ESG Research Centre

As demonstrated in Exhibit 22, there is widespread interest across the industry in harnessing AI to improve the AML/CTF process where 91% of respondents said they were considering implementing AI. This sentiment is mirrored in Exhibit 28, with 97% of all respondents saying that they would allocate a portion of their budget to investing in digital tools over the next two years.

The majority of all respondents (52%) were likely to invest less than 10% of their AML/CTF budget in digital tools. 45% of total respondents indicated that they plan to invest over 10% of their AML/CTF budget for this purpose, with banks and payments institutions more likely to do so than asset managers.

Exhibit 29: Are you using any AML/CTF cloud solution tool for your activities?

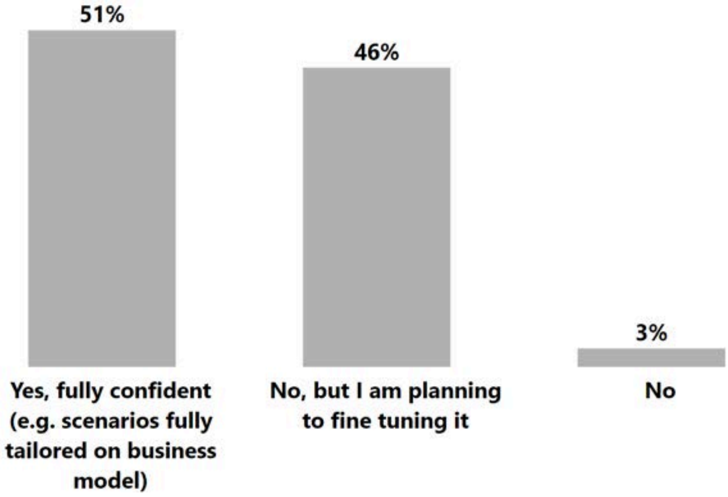


Note: Percentages may not add due to rounding.
Source: PwC Global AWM & ESG Research Centre

1	Our survey showed that there is a 50/50 split across respondents who have, and have not invested in cloud solutions. 38% of all respondents are planning on implementing AML/ CTF cloud solutions in the next 12-24 months, and only 12% stating they are not considering using cloud solutions. This is potentially driven by concerns about data sharing with cloud providers. For example, Exhibit 4 highlights that 43% of respondents felt that simplified data sharing rules would significantly improve their AML/CTF effectiveness.
2	Additionally, in Exhibit 24, 68% of respondents cited data sharing concerns as a key constraint in implementing AI, with 20% of banks not currently considering cloud solutions. This could be for a number of reasons, including there being no need because of the size of their operations and current technology being appropriate, not being able to secure sufficient budget, or not having the internal infrastructure that would allow them to consider cloud solutions.
3	Cloud based solutions often come equipped with advanced analytics and machine learning capabilities that can be leveraged to significantly enhance the detection and prevention of illicit activities. These technologies can process and analyse large datasets more efficiently than traditional systems, identifying patterns and anomalies that may indicate money laundering or terrorist financing activities. Machine learning algorithms can learn from historical data and transaction patterns to improve their predictive capabilities over time, reducing false positives and allowing compliance teams to focus on the most pertinent alerts. This level of sophistication in data analysis is crucial for financial institutions as they navigate complex financial networks and must comply with stringent regulatory standards. The cloud's computational power enables these advanced technologies to be leveraged without the need for financial institutions to maintain their own high-performance computing resources.
4	Implementing cloud based solutions for financial crime risk management can lead to significant cost savings for financial institutions. Cloud services typically operate on a subscription model, which can be more predictable and easier to manage from a budgetary perspective. This shift from capital expenditure to operational expenditure can free up resources for other strategic initiatives. Additionally, the cloud service provider manages the underlying infrastructure, reducing the IT burden on the financial institution. This means that IT staff can focus on higher-value tasks, such as fine-tuning fraud detection systems or developing new products and services, rather than on maintaining and updating servers and other hardware.
5	Cloud solutions offer financial institutions a powerful combination of scalability, access to advanced analytics, and cost efficiency, which are critical in managing the dynamic and complex risks associated with financial crime. These tools can enable institutions to stay agile and responsive in the face of threats, while also optimising their operational and capital expenditure.

Transaction Monitoring: A Closer Look

Exhibit 30: **Are you confident that your transaction monitoring approach is fit for purpose?**



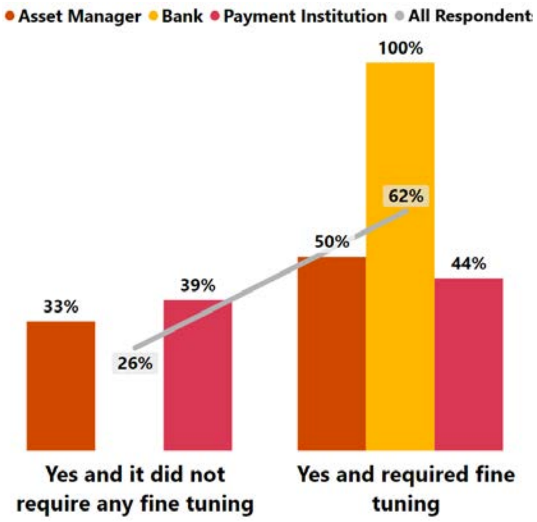
Note: Percentages may not add due to rounding.
Source: PwC Global AWM & ESG Research Centre

51% of respondents indicated that they believe their transaction monitoring approach is fit for purpose (e.g. scenarios are fully tailored in accordance with their business model), with 67% of payment institutions and 56% asset managers being the most confident.

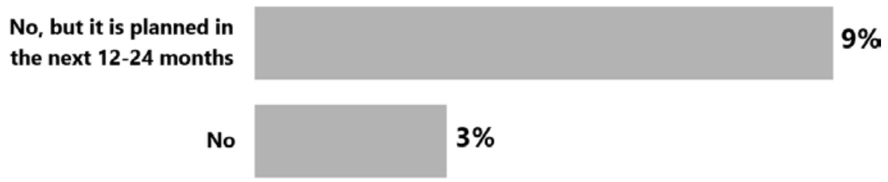
64% of banks indicated a lack of confidence in their transaction monitoring systems, but were planning on fine tuning their approach. This is in line with findings later on in this report (Exhibit 34), where 70% of banks stated that their numbers of false positive alerts are too high (compared with 67% of asset managers and 39% of payment institutions).

Exhibit 31: Did you perform any screening / transaction monitoring tool test and review in the last 24 months?

Respondents that performed screening or transaction monitoring tool test and review in the last 24 months



Respondents that did not perform screening or transaction monitoring tool test and review in the last 24 months



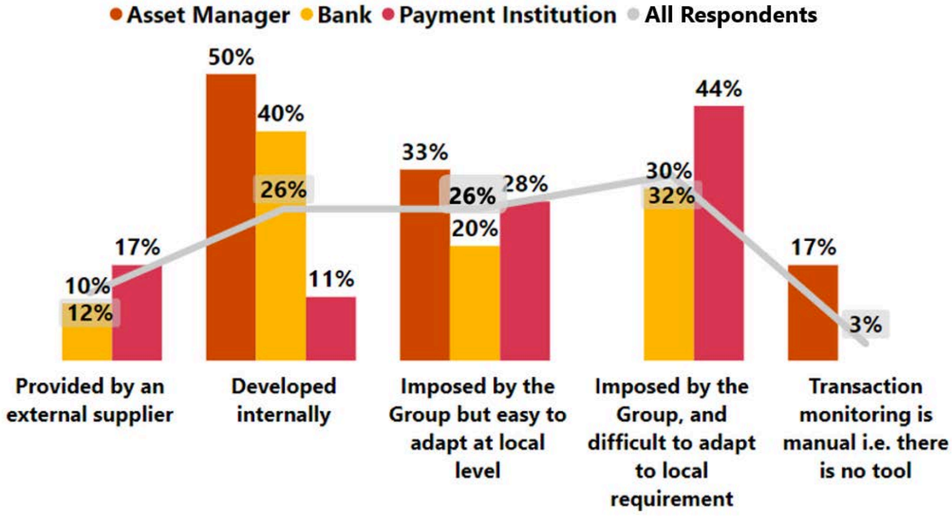
Note: Percentages may not add due to rounding.
Source: PwC Global AWM and ESG Research Centre

As seen in Exhibit 31, the majority of respondents (88%) have performed testing over their screening and/or transaction monitoring tools over the past two years. 26% of all respondents who have performed testing over the last 24 months indicated that their tools were performing well and did not require further fine-tuning, while the remaining 62% stated that the tools did require adjustments. A further industry breakdown shows that all bank respondents fall into this category. In the UK, banks, payment institutions, and asset managers are subject to stringent regulatory requirements. Regular testing and review of screening and transaction monitoring tools are critical components of these controls for a number of reasons, including:

- **Detection and prevention of financial crime:** Screening and transaction monitoring tools are essential for identifying suspicious activities that could indicate money laundering, terrorist financing, or other financial crimes. By regularly reviewing and testing these tools, institutions can ensure they are accurately detecting potential threats and suspicious activity, as well as taking appropriate action.
- **Risk management:** Regular testing helps in assessing the effectiveness of risk management strategies. It allows institutions to identify and address vulnerabilities in their systems, thereby reducing the risk of financial loss or reputational damage.
- **Adapting to emerging threats:** Financial crime methodologies are constantly evolving. Regular reviews allow institutions to update their systems to detect new typologies of illicit behaviour.
- **Operational efficiency:** Regular testing can lead to improvements in the operational efficiency of compliance processes. It can help streamline monitoring and screening processes, reducing false positives and ensuring that resources are focused on genuine threats.

Regular testing and review is particularly important for banks, not least due to the volume and complexity of transactions. Banks typically handle a higher volume and complexity of transactions compared to payment institutions and asset managers. This increases the potential for illicit activities to occur, making robust monitoring systems essential. Banks are also often subject to more intense regulatory scrutiny due to their central role in the financial system. Failures in their AML/CTF controls can have systemic implications. Given the size and prominence of some banks, they are more likely to be targeted by criminals seeking to launder money or finance terrorism. This higher risk of exposure makes rigorous testing and review of AML/CTF controls even more critical.

Exhibit 32: Which of the following applies to the tool and scenarios used by your financial institution for transaction monitoring purposes?



Note: Percentages may not add due to rounding.
Source: PwC Global AWM and ESG Research Centre

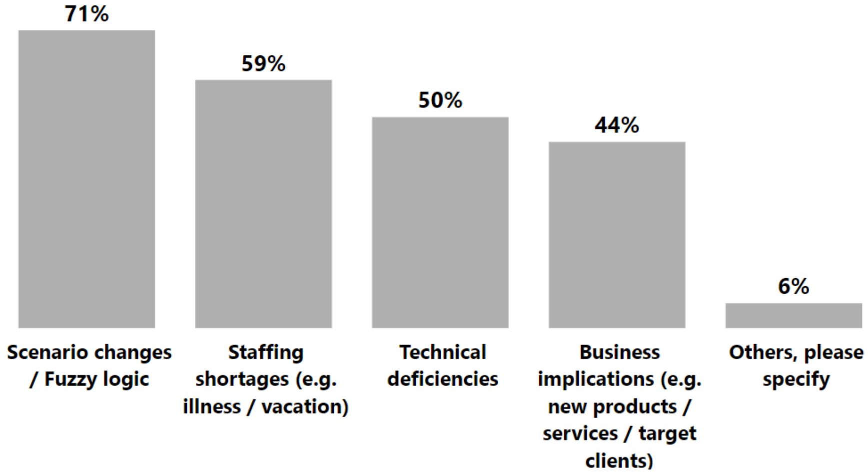
Nearly all of the financial institutions surveyed (97%) are using technology to monitor transactions. The survey highlights the issues with tools imposed at Group level and the practicalities of implementing them at local levels. Whilst approximately a quarter of respondents (26%) said tools were 'imposed upon them by the Group but easy to adapt at a local level, more respondents (32%) flagged that these were difficult to adapt at a local level. This means that just under a third of financial institutions are unable to fine-tune their digital tools as they are not flexible enough to adapt to 'local' needs. This is likely to be a factor in reducing the efficiency and effectiveness of these tools, with staff having to work around their digital infrastructure, rather than use it to its full potential.

Consequently, this may lead to inefficient and ineffective use of the tool at local level and an inability to properly manage AML/ CTF risk, as well as incurring higher operational costs through needing to manage higher volumes of false positive alerts.

Financial behaviours and transaction patterns can vary significantly across different regions. A group-level system may not account for UK local market nuances, resulting in either over-reporting or under-reporting of suspicious activities. As seen in Exhibit 34, over half of those surveyed stated that a key challenge with their transaction monitoring system was the high volumes of false positive alerts.

Of those institutions which do not rely on Group tools, there was a preference for internally developed tools (26%) rather than using an external supplier (12%). This highlights the difficulty of purchasing off the shelf tools and sometimes the need for technology to be developed on a bespoke, case-by-case basis.

Exhibit 33: **What are the main reasons for alert backlogs in your organisation?**



Note: Multiple choice question. Respondents were asked to select their top three answers.
Source: PwC Global AWM and ESG Research Centre

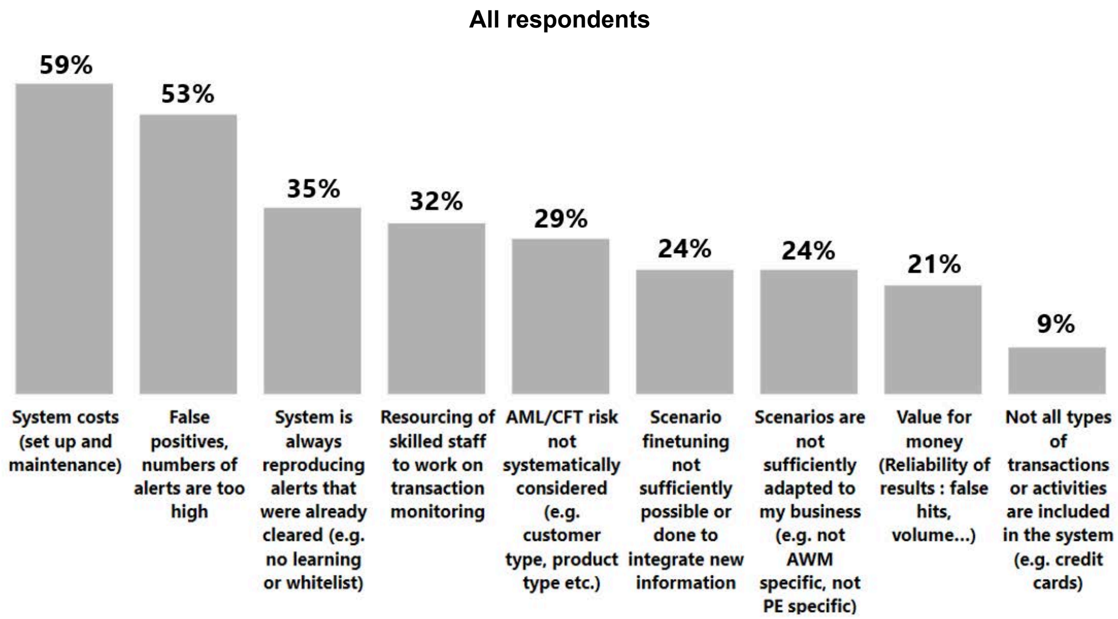
Though the transaction monitoring tools may be functioning efficiently, this in itself does not help to avoid alert backlogs. There can be a number of reasons for backlogs. Exhibit 33 shows that almost three quarters of the respondents surveyed, (71%) stated that scenario changes and fuzzy logic were a cause of alert backlogs.

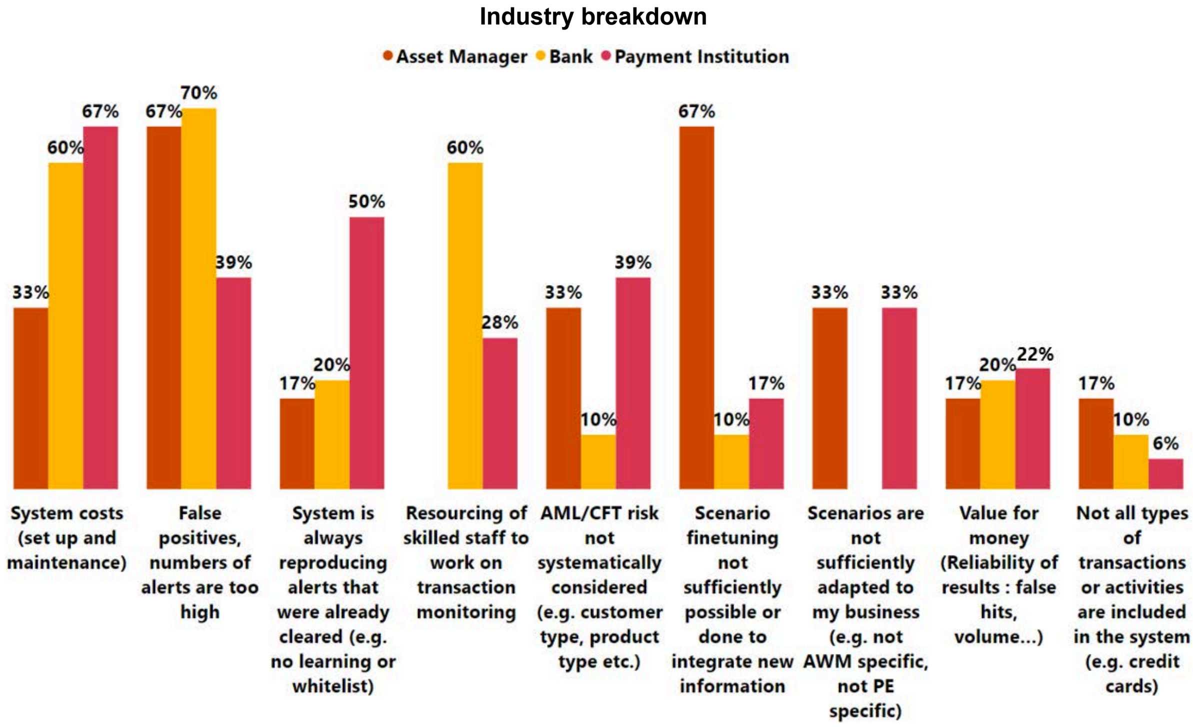
Once again, staffing is among the top answers: 59% of respondents frequently experience shortages of skilled staff. The concern around staffing emphasises the need to employ, train and retain skilled staff so that alerts are investigated appropriately and in a timely manner, avoiding backlogs.

> "Ever growing customer transactional activity leads to ever growing alert batch sizes – being tackled through ongoing focus on false positive alert reduction"

Survey respondent from the banking industry

Exhibit 34: **What are your main current transaction monitoring tool challenges?**





Note: Multiple choice question. Respondents were asked to select their top three answers.
Source: PwC Global AWM and ESG Research Centre

The biggest challenge regarding transaction monitoring tools in the UK is in relation to system costs for 'set up and maintenance'. In the wider EMEA survey, a smaller proportion (only 46%) of respondents cited this as a challenge, implying that costs are generally more of an obstacle in the UK, perhaps a consequence of the current macroeconomic environment in the UK. High numbers of false positive alerts was the top challenge cited by 48% of respondents across the EMEA region, compared to 53% in the UK.

Systems reproducing alerts that have already been cleared is another key challenge highlighted by respondents – this presents another argument for investing in new technologies using AI and machine learning to help streamline processes. The prevalence of these challenges could also flag an issue with the dependability of such solutions for UK institutions, which has a knock on impact on staffing levels required to handle alerts.

The lack of skilled staff also represents another challenge for transaction monitoring with 32% of UK respondents saying this is an obstacle. This results in delays in investigations, defensive escalations, missing risk indicators completely and re-work. Staffing issues have been a recurring theme across large parts of this survey. This finding is also echoed in the EMEA survey, suggesting that staffing is an issue across the entire region. It is also worthwhile noting that, as per Exhibit 24, 35% of respondents cited that a key constraint for AI implementation is the lack of sufficient talent. Having the right people, in the right place, with the right skills is fundamental to the effective management of AML/CTF risks. The lack of appropriately skilled resources can severely undermine a financial institution's ability to comply with regulatory requirements, effectively manage risks, and maintain operational integrity.

Conclusion

The analysis of the effectiveness of AML and CTF controls among UK financial institutions reveals a complex landscape marked by both challenges and opportunities for future improvement to maintain effectiveness.

Regulatory Landscape and Compliance

Financial institutions in the UK operate within a stringent regulatory framework and whilst these regulations are essential for preserving the integrity of the financial system, they also introduce considerable complexity and cost. The survey indicates that regulatory constraints are a primary barrier to the adoption of new technologies, which are crucial for enhancing AML/CTF controls. Institutions must navigate these regulations carefully to ensure compliance while seeking ways to streamline processes and reduce administrative burdens.

Operational Challenges

The operational environment for AML/CTF activities is fraught with challenges, particularly in maintaining up-to-date Know Your Customer (KYC) information and managing the high volume of false positive alerts generated by transaction monitoring systems. The survey highlights that updating KYC documentation is a significant concern and that the high number of false positives in transaction monitoring systems underscores the need for more sophisticated tools and better data quality to improve accuracy and efficiency.

Technology Adoption

The adoption of advanced technologies, particularly Artificial Intelligence (AI), is seen as a critical factor in enhancing AML/CTF controls. AI can automate routine tasks, reduce false positives, and provide deeper insights into suspicious activities. However, the integration of AI faces several hurdles, including regulatory constraints, data quality issues, budget limitations, and a shortage of skilled resources. Despite these challenges, there is a strong interest among financial institutions in leveraging AI to improve transaction monitoring, customer AML risk assessments, and screening processes.

Staffing and Training

The human element remains a cornerstone of effective AML/CTF operations. The survey reveals that staff training is considered the most effective control measure, yet it tends to attract minimal investment. Financial institutions recognize the importance of skilled staff in ensuring compliance and managing risks, but they face difficulties in retaining talent due to compensation issues and the monotony of tasks. There is a clear need for ongoing training programmes to keep staff updated on the latest regulations and tools, as well as efforts to make roles more dynamic and engaging.

Future Considerations

Looking ahead, financial institutions in the UK must balance stringent regulatory requirements with practical application to maintain operational effectiveness. This involves continuous adaptation to evolving risks and regulatory changes, investment in advanced technologies, and a focus on improving data quality. Institutions should also consider ways to enhance staff training and retention to ensure they have the necessary expertise to manage AML/CTF activities effectively. While UK financial institutions have made significant strides in their AML/CTF efforts, there is still room for improvement. By addressing the challenges identified in this survey - regulatory constraints, operational complexities, technology integration, and staffing issues -, financial institutions can strengthen their AML/CTF controls and better protect themselves and their customers from financial crime.

Contact us

Mark Loring
Financial Crime Partner,
PwC UK
mark.loring@pwc.com

Vibhuti Bhatt
Financial Crime Director,
PwC UK
vibhuti.bhatt@pwc.com