A 1LoD Survey

The 2025 Financial Crime Benchmarking

SURVEY & REPORT

LEAD SPONSOR

DOW JONES
RISK & COMPLIANCE

CO SPONSORS

FIRST DERIVATIVE
AN EPAM COMPANY

WorkFusion

Subscribe here
to receive new content and event information directly to your inbox

Introduction

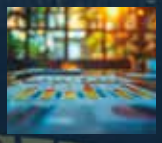
These are the results of 1LoD's inaugural Financial Crime Benchmarking Survey & Report. It combines the results of a survey of more than 25 organisations – taken from the Tier 1 and Tier 2 sectors in the US, Europe and Asia – and conversations about the results with financial crime leaders at those and other institutions. It incorporates a host of new datapoints designed to help you benchmark your own anti-money laundering (AML) and know your customer (KYC) processes and technology against your peers.

The survey is divided into the following sections:

i. Operating model

ii. Staffing, roles and responsibilities

iii. Technology



iv. Oversight, budget and resources

Key takeaways

94% of banks identify high manual workloads as a key operating challenge in AML/KYC

75% anticipate buying transaction monitoring (TM) technology in the next three years

60% of banks rely on manual intervention for more than half of their AML/KYC processes

69% anticipate buying KYC automation technology in the next three years

56% of banks use robotic process automation (RPA) in AML/KYC but still 38% of banks have automated less than a quarter of their AML/KYC processes

53% anticipate buying customer due diligence or enhanced due diligence (CDD/EDD) technology in the next three years

56% of banks are either neutral or dissatisfied with their current AML/KYC technology

67% anticipate buying workflow technology in the next three years

50% anticipate AML/KYC budgets increasing or remaining the same in the next financial year

50% anticipate buying media screening technology in the next three years

80% say that technology is the area of AML/KYC that requires the most financial investment

There are three big-picture takeaways from the survey and the accompanying interviews:

1 Banks are committed to getting AML/KYC right and, for many, budgets are rising

Given the level of recent enforcements this may not be much of a surprise, but senior management at banks large and small are making sure that they understand the challenges and bottlenecks in AML/KYC, and they are prepared to get their cheque books out to ensure that their processes can withstand regulatory scrutiny as well as deliver useful intelligence to law enforcement and mitigate the underlying risk of being used as a conduit for financial crime.

Over half (56%) of banks perceive senior management to be very involved in making decisions in AML/KYC, while 94% rate board effectiveness and awareness about financial crime-related risks as good or very good.

But, more importantly – and regardless of whether this is due to enforcement actions – this organisational commitment is backed up by resourcing. The survey found that 53% of AML/KYC compliance budgets have increased in the past two years, and 33% anticipate KYC budgets increasing in the next financial year.

Given the current volatile economic and geopolitical environment, the fact that a significant portion of the marketplace is seeing increases in resourcing, when other areas of compliance are feeling the squeeze, is a testament to the importance banks are placing on ensuring that AML/KYC functions have what they need.

And where are banks likely to spend these budget increases? Well, 80% say that technology is the area of AML/KYC that requires the most financial investment.

2 AML can make huge efficiency gains by eliminating manual processes

That investment is much needed. Despite advances in technology and the rapid digitalisation of other parts of banking, KYC is still a highly manual process. Banks find it difficult both to obtain digital versions of documents from clients and to avoid manual processes in verifying that information. The various name-screening processes for sanctions, politically exposed persons (PEPs) and adverse media throw up huge numbers of exceptions and queries that require manual remediation, and while initial TM is largely automated, investigating alerts and filing Suspicious Activity Reports (SARs) is a largely manual process.

Manual processes are slow, expensive and prone to errors. They annoy clients, they add significant friction to the business, and they are a target for regulators because it is easy to find problems with manual processes.

The survey confirms the seriousness of the problem: 94% of banks identify high manual workloads as the key operating challenge in AML/KYC, and for 60% of banks, more than half of their AML/KYC processes rely on manual intervention.

What are banks doing to solve the problem, and what kinds of solutions are they using? Just over half of the banks in the survey use RPA in AML/KYC, but this does not eliminate the problem – a large proportion of banks (38%) have automated less than a quarter of their AML/KYC processes.

Adoption of new technologies is still in its infancy: 38% of banks use some form of artificial intelligence (AI) or

machine learning (ML) in AML/KYC, while just 6% of banks use blockchain in ID verification.

3 Banks anticipate buying technology upgrades across all categories of AML/KYC

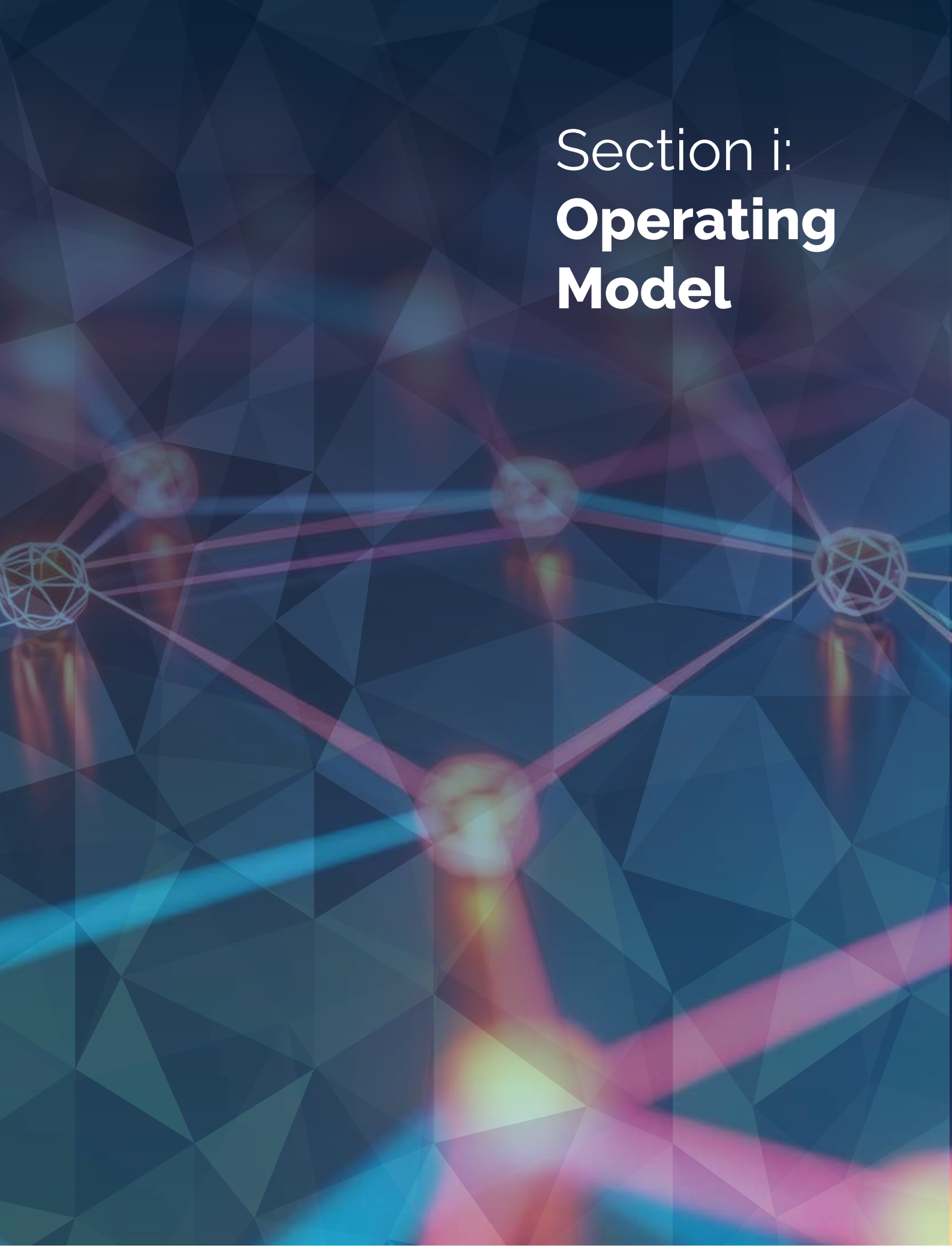
Given the issues with manual processing, a lot of time and effort in AML/KYC is spent on investigating, evaluating and implementing the technologies that could solve key problems in banks' processes.

What is surprising is how comprehensively banks want to upgrade their systems across all areas of their AML operations. Three quarters of banks are either neutral or dissatisfied with their current AML/KYC technology, and well over half anticipate buying new technology in TM, KYC automation, media screening, CDD/EDD, and workflow technology in the next three years.

What are banks most concerned about in their AML technology stacks? The two most common problems that they want to solve are integration with other systems and the reduction of errors and false positives in monitoring systems. Both trade monitoring and name screening require a lot of (mostly manual) work because they generate noise that must be investigated.

Even though banks say that technology is not about reducing headcount but about freeing staff to do more valuable work, more than half of firms surveyed measure tech effectiveness in terms of cost. Effectiveness gains are great, but cost savings – or the ability to cap costs – are better.

Over half (56%) of banks perceive senior management to be very involved in making decisions in AML/KYC, while 94% rate board effectiveness and awareness about financial crime-related risks as good or very good.



Section i: **Operating Model**

AML/KYC is an interesting case study in the problems of dividing functions neatly between the 1st and 2nd lines of defence. For the most mature institutions, there are AML teams in both the 1st and 2nd lines (and AML auditors in in the 3rd line).

As one compliance and financial crime chief put it, "The 1st line teams are managing risk day to day. The 2nd line teams are oversight and challenge – setting standards, controls, and an escalation point for certain decisions. I think of this as little different to credit risk…the majority of credit decisions sit entirely in the 1st line but overseen by a risk function."

In this setup, large banks split AML Operations and AML Compliance, sometimes with operations reporting to compliance, but sometimes with both functions reporting upwards to a compliance or risk function. Some AML compliance leaders are wary of this split, as it can create a "them and us" divide between risk and compliance, but they also dislike the idea that significant parts of the AML operation do not report to them.

Certainly, in terms of costs, AML/KYC is a significant proportion of compliance budgets, regardless of arguments about the division of duties. The survey found that AML/KYC consumes more than 50% of the total compliance budget in 21% of banks, while another 21% said it accounts for between 26% and 50%.

Who owns AML/KYC risk?

The question of risk ownership is key: if AML is a compliance function, then the risk it manages is compliance risk, defined ultimately by regulatory enforcement. So, compliance should own it. But if KYC is seen as a function that mitigates a fundamental business risk – dealing with risky customers and transactions which expose the bank to the risk of being used for criminal purposes – then that risk should be owned by the business. KYC is unusual, because although the risk is managed entirely in the 1st line, the business is not taking ownership of the risk.

If at least the core of KYC is a business risk, despite being enshrined in regulations, what should go in the 1st line? KYC for onboarding, including all types of name

CHART 1

What percentage of your compliance budget is allocated to AML and KYC operations?

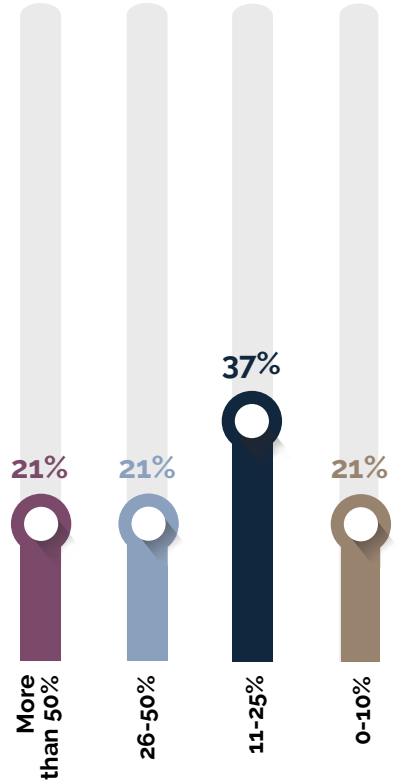
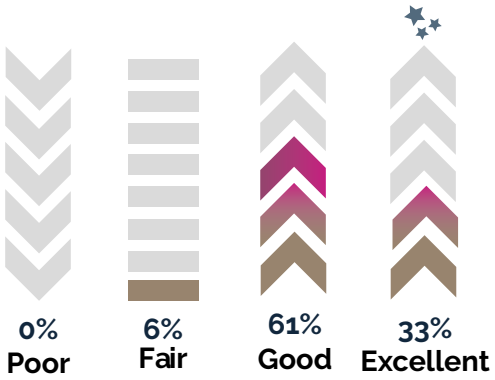


CHART 2

How would you rate the clarity of roles and responsibilities in the financial crime operating model?



and media screening? Ongoing or periodic reviews – including sanctions? Transaction monitoring?

One global bank's head of financial crime says: "From a purist perspective, everything goes into the 1LOD. In practice, I think you hold back approval of models used (e.g. client risk assessment, TM), a certain class of highest risk/profile pan-bank investigation, and decision rights on SARs. But that's my personal prejudice and arguably even some of this could migrate."

One interesting point about the split between different lines of defence is that several large banks, when faced with significant regulatory enforcements, pulled everything back into the 2nd line to ensure that the renewed function was fully compliant. Having achieved this, these banks are now pushing functions such as onboarding, periodic reviews and TM back into the 1st line.

The aim, as this head of financial crime at a global bank says, is: "AML expertise close to product, with a thin layer of 2nd line oversight, and a very thin audit function. The focus of the 2nd and 3rd lines would be less on compliance with regulation than on effectiveness. This would mean that many people currently in the 2nd line would be in the 1st line. For this to work, the front office (which is 1st line but tends to see operations as distinct) would need to take more ownership for operations activity. There would be no 1.5LOD."

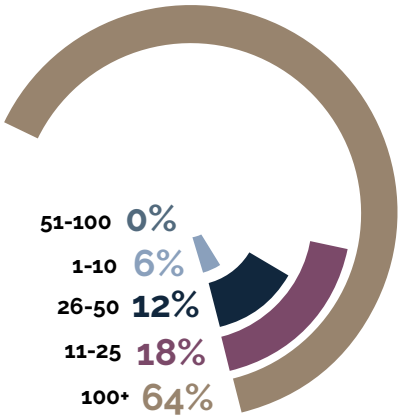
Despite the debates around divisions of responsibility, in practice, once banks have decided on a model, there is very good clarity of roles and responsibilities in the financial crime operating model **[Chart 2]**: 94% of respondents said that the clarity is good or excellent.

Right-sizing AML/KYC teams

Right-sizing risk and compliance functions is more art than science. Regulators are not much help here because they tend to fall back on generalisations about appropriateness and the suitability of any function relative to the size and complexity of an institution's business.

In terms of AML compliance, this can lead to seemingly anomalous results. A large bank with a very low-risk clientele operating in a very low-risk jurisdiction may have a smaller team than a much smaller organisation with a high-risk clientele or operating in a high-risk environment (often the same thing).

CHART 3
What is the size of your AML compliance team?



It's also true that the levels of technology adoption and automation will affect team sizes (see technology section for more details). Large, well-resourced banks will usually have much larger numbers of clients, products and transactions to monitor, which would imply larger teams, but they also usually have more resources to invest in efficiency, which should then allow them to reduce the size of the team.

All of this means that drawing conclusions about the nature of an institution, its clients or its risks purely from the size of its AML compliance teams is only one of many ways to understand the maturity of any organisation.

That said, this survey includes a range of institutions, from the very large, global players to the smaller neobanks. Those smaller, newer players do start with an advantage: They may focus on one client vertical (retail for example), and they are able to build their processes on modern technology from the get-go. These are the banks with the smallest teams, while institutions in the large domestic, regional or global categories all have teams of more than 100 people.

Few takers for outsourcing

AML compliance team size is highly correlated with institution size and with the centralisation of particular compliance functions. So, as the survey is weighted towards larger organisations, 60% of banks described their KYC function as centralised.

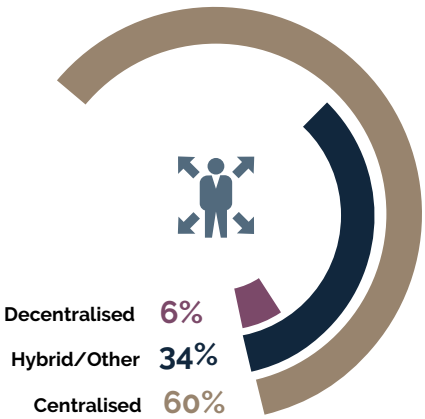
Just 6% of organisations have fully outsourced their KYC functions. Yet outsourcing ought to be an attractive solution given the costs of KYC, the development of external KYC repositories and of third-party KYC hub software solutions, and the obvious frictions that inefficient KYC processes impose on the business.

There are several managed service providers who claim to be able to provide a full AML compliance service, including KYC, TM, AML systems and controls, and independent AML audit, and some will even provide a Money Laundering Reporting Officer (MLRO) if required.

However, these services tend to be marketed to FinTech's and the smallest organisations, and the survey shows that these services only appeal to them.

CHART 4

How is your AML / KYC function organised?



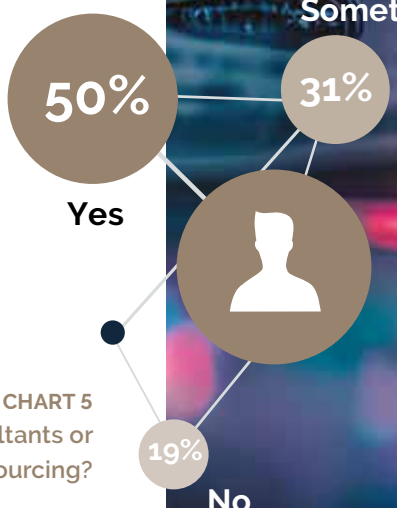


CHART 5

Do you use external consultants or partners for AML and KYC outsourcing?

Models are still inefficient

Regardless of the core operating model, banks across the spectrum report similar challenges with current AML and KYC operating models, all of which can be summarised in one word: inefficient. The biggest problem, raised by 94% of all respondents, was the manual workload. This includes the manual review and cross-referencing of identification documents for KYC, manual processes for checking against sanctions and watchlists as well as for more general negative news screening, and manual involvement in investigations and reporting from TM.

These manual processes are, in turn, the foundation for many of the other challenges. They cause delays and increased costs in onboarding and client review, which is bad for the clients and bad for the business. They also make it difficult to adapt compliance systems to changing regulations, and they cause high error rates. These issues are multiplied when manual processes are themselves inconsistent across different parts of the bank.

These problems can be solved with the use of external datasets, better workflow technology, newer compliance and RegTech solutions around identity and document verification (which are discussed in the technology section). But AML compliance teams also need better systems integration and upgrading internally. This requires a senior management understanding of (and commitment to) financial crime as these kinds of systemic change are beyond the purview of the 2nd line.

Client resistance to technology is part of the problem: it is difficult to get clients to supply digital information via bank portals, and while banks argue that improving KYC processes actually benefits clients enormously by avoiding pointless or duplicative contact, it is hard to change client habits.

CHART 6
What are the main challenges your team faces with the current AML and KYC operating models?

Looking in more detail at inefficiencies, the survey reveals the average onboarding time for new customers and the percentage of customers that require EDD. Combining this with team size gives a more detailed picture of how different banks structure their teams to cope with their particular risk profile.

Inefficiency does not appear to be related to the speed with which the AML policy and risk framework itself changes. The regulatory landscape in financial crime is one of the most dynamic – governments regularly legislate on economic crime, on counter-terrorist financing, and on sanctions – yet 50% of banks surveyed only review or adjust their AML policies and procedures once a year.

So, while banks typically respond to regulatory change as it happens, full reviews of frameworks and risk assessments are done with a more arbitrary frequency that is not related to the volatility of the regulatory environment. This makes sense. The annual, deep-dive reviews have significant ramifications downstream, and it would be counter-productive to do them too often otherwise the more granular control frameworks would be in a state of constant revision, creating errors, inefficiency and problems in explainability.

CHART 7

What is the average onboarding time for a new corporate client under your AML and KYC processes?

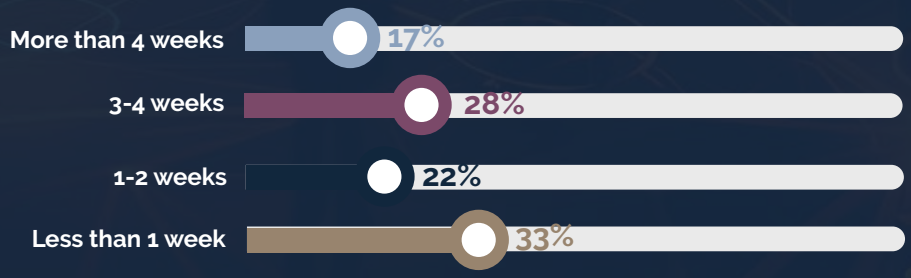
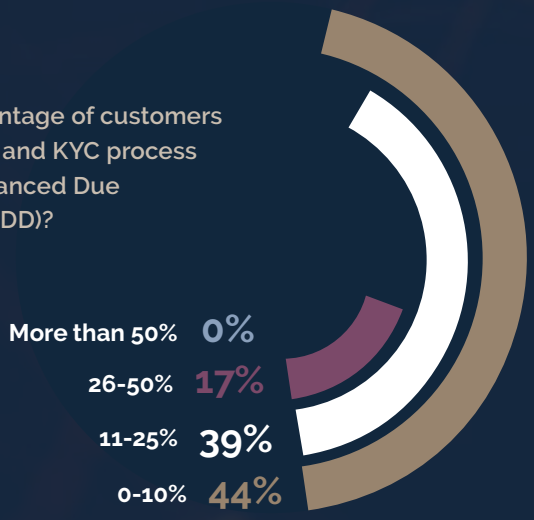
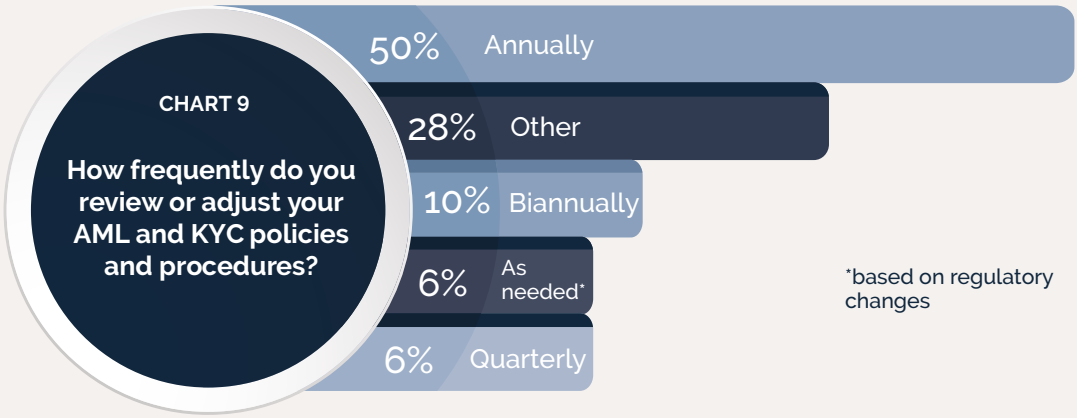


CHART 8

What percentage of customers in your AML and KYC process require Enhanced Due Diligence (EDD)?





It would also make them hard to audit. And since close to 90% of banks audit their AML and KYC operating models annually, it makes sense that framework reviews follow the same schedule, adapting both to the market and internal audit (IA) findings in the same cycle.

Inefficient, but effective?

Inefficiency is expensive, it gets in the way of doing business, and it can create errors. Yet banks seem to think that the inefficiencies they acknowledge do not have too serious an impact on their fundamental effectiveness. When asked about the ability of their current AML and KYC operating models to identify financial crime risks, 22% described them as very effective, while the remainder said that they were somewhat effective.

CHART 10
How often are your AML and KYC operating models independently reviewed or audited?

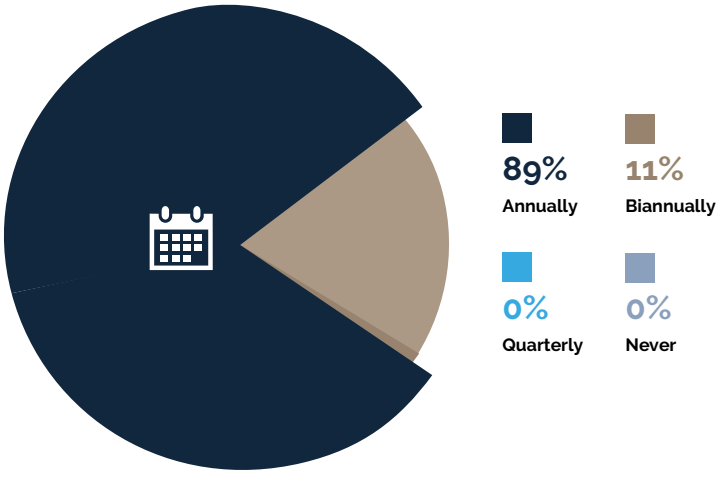
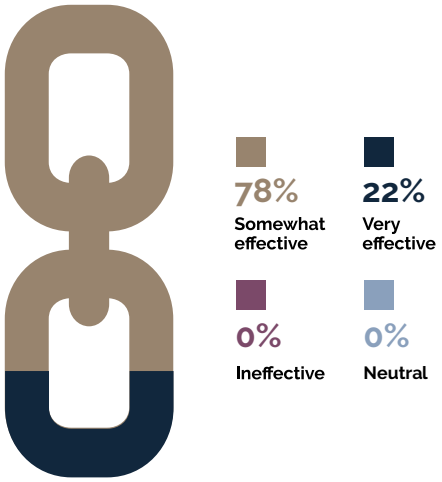


CHART 11
How effective are your current AML and KYC operating models in identifying financial crime risks?



Section ii: **Staffing, roles and responsibilities**

While discussions of operating models centre on where work is carried out and by which line of defence, the nature and composition of AML/KYC teams is equally important.

The survey shows that AML/KYC leaders uniformly rate the expertise of their teams as high or very high. This ties in with measures of the length of service and experience, which are particularly high: 88% of AML/KYC team members (excluding offshored contractors and the like) have more than four years' experience, and 41% have more than six years.

> Banks also report very low turnover rates: **53%** of respondents cited an annual turnover rate of between **6%** and **15%**, while **35%** have turnover rates below **5%.**

There are two ways to look at this data. One is to say that financial crime detection and investigation is a complicated and multi-faceted activity that requires staff who have gained considerable experience from doing the job for many years. The other is to wonder whether such low turnover means that teams fail to evolve at a rate that is commensurate with that of a sector where new technology and new ideas about operating models are developing so rapidly.

When pressed, AML/KYC leaders admit that they are concerned about the impact of a low attrition rate on diversity of thinking and skillsets. But they also stress that activities such as EDD, alert escalation from transaction monitoring, name/media screening, as well as evaluations concerning SAR filing all require high levels of expertise that come largely from experience.

For example, one financial crime leader at a large European bank said, "We did have a quite high rate of attrition in one team, but that was mainly due to issues around pay and packages. More generally, we do have relatively low attrition and that does trouble me, because I can see that it gets in the way of keeping the teams fresh and of having the diversity of thought that I would like, particularly in teams where the majority of people are drawn from the same types of background and career path. That said though, as we introduce more automation, and potentially focus teams around the higher-skilled investigators, then the issue of a narrowing of the pool of recruits and the implications of that become more of an issue."

They also point out that recruiting the right talent for financial crime roles is hard (for 18% of respondents) which case staff retention and low turnover are essential for maintaining the quality of the AML/KYC team.

In cases where staff attrition is a problem, it is usually the result of several factors. Banks in the throes of a complex remediation may find it difficult to keep staff while going through a painful process. Smaller institutions may be outbid for those roles in the greatest demand. And, with 38% of banks saying that their biggest challenge in building teams is how to balance workloads with the necessity for transformation, staff burnout is a real issue.

CHART 12

How would you rate the expertise of your AML and KYC team in managing financial crime?

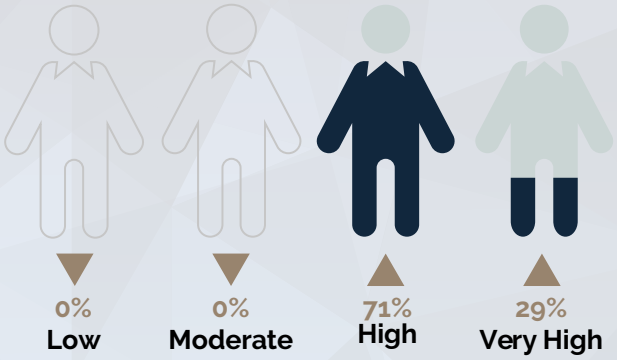


CHART 13

What is the average experience level of your AML and KYC team members?

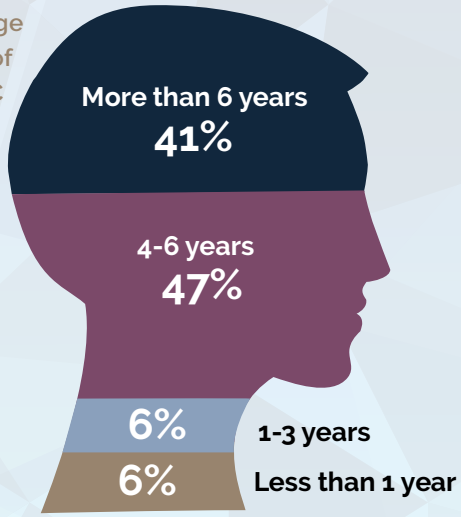


CHART 14

What is your team's employee turnover rate in the AML and KYC functions?

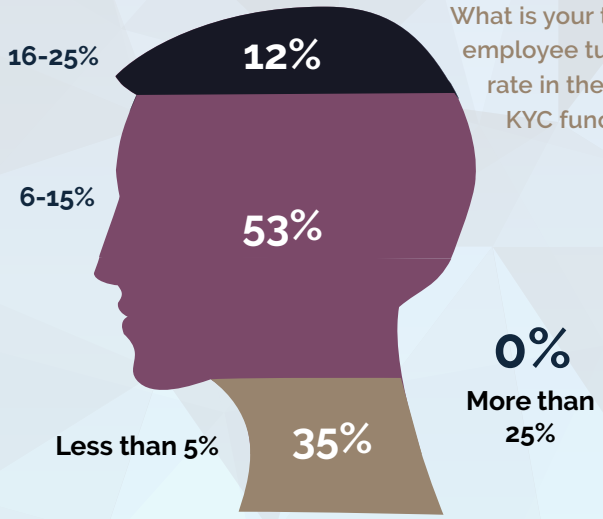
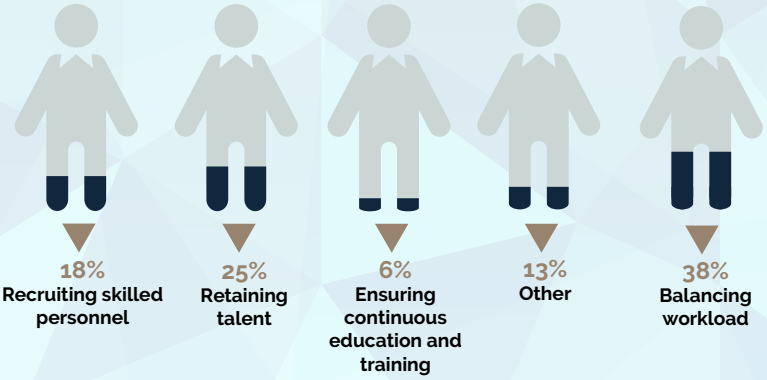


CHART 15

What is the biggest challenge in building effective AML and KYC teams?



Training and awareness

A key element of maintaining AML/KYC compliance is training. In the UK, for example, the core money laundering regulations include compulsory requirements relating to staff training and awareness for regulated organisations. All training should be appropriate to employees' roles and firms should be able to answer questions about how they ensure that employees are aware of financial crime risks and of their obligations in relation to those risks, how they ensure that training is of consistent quality, and how they assess the effectiveness of this training. This includes requirements to keep a comprehensive written record of all training undertaken.

The survey shows the variety of ways in which banks interpret the regulations. Given the explicit regulatory requirements, it is interesting that just 35% of respondents use regular formal training sessions, versus 36% who use on-the-job or ad-hoc training. It is surely easier to document and justify a formal training programme than one that relies on irregular, event-driven training. It is also easier to ensure consistent coverage of the key topics.

It is less surprising that 81% of respondents favour an irregular, 'as needed', approach to training about regulations. The field of AML/KYC is notorious for its regulatory fragmentation, inconsistency and rapid evolution (especially where sanctions are involved). It therefore makes sense to keep on top of change by responding quickly when it occurs.

It is also interesting how many banks use e-learning modules. Everyone who has ever worked for a large organisation, and has done training in cybersecurity or HR or any other topic, will know how easy it is to treat this kind of training as a chore which must be ticked off as quickly as possible. They will also know that its effectiveness is limited, because once modules have been 'passed', they are often quickly forgotten.

CHART 16

What is the primary method of training your team receives on AML and KYC requirements?

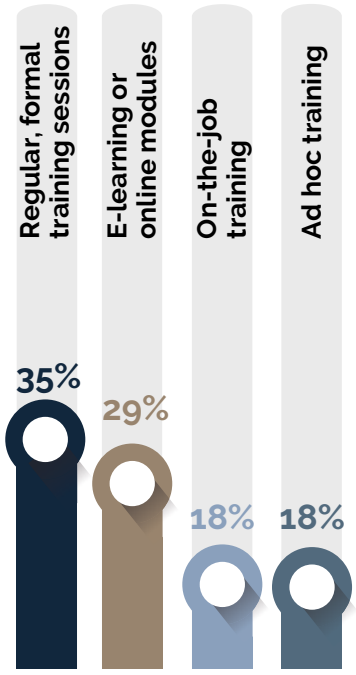
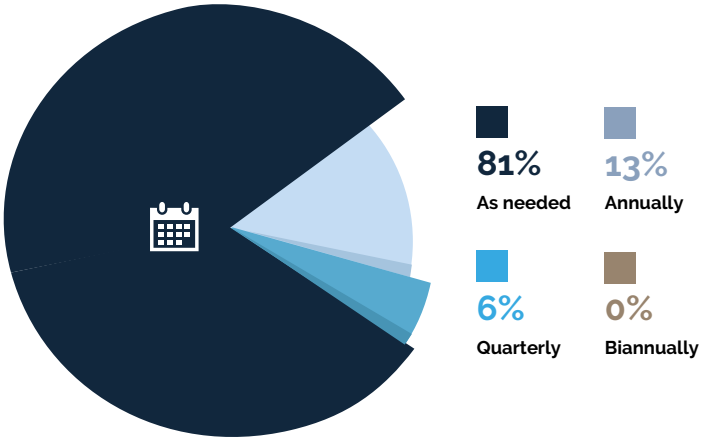


CHART 17

How often are your AML and KYC teams trained on the latest regulations?



Performance measurement

Measuring the performance of an AML/KYC operation is extremely complex and depends significantly on how institutions view the function in the first place. If AML/KYC is viewed largely as a compliance function, with the primary risk being managed as regulatory enforcement risk, then KPIs for compliance will dominate. This has a knock-on effect because compliance functions are seen as cost centres and so operational efficiency is key, including measures related to adherence to agreed deliverables, error rates, and the level of friction introduced into key business processes such as onboarding.

This is a controversial topic. Most banks say that their AML/KYC functions are there to manage the risk that the bank is used for the furtherance of financial crime, and the related costs and reputational damage. But when asked to define those losses, they do so in terms of regulatory sanction or, in the worst case, criminal prosecution. It is hard to avoid the conclusion that AML/KYC functions are designed from the ground up to ensure compliance, and then as a by-product of that design they deliver some level of true risk mitigation. It is certainly hard to see any bank doing the opposite: building an AML/KYC function from a non-compliance-based risk assessment, and presenting that to the regulators.

The survey bears this out. Error rates in customer files and compliance are the most chosen measures of AML/KYC team performance.

However, close behind is 'quality of financial crime investigations' (41%). This reflects the fact that many banks also view the quality of their suspicious activity reports (SARs) as a key performance indicator. This can be seen as a compliance metric, since regulators closely monitor the number and quality of SARs across the industry and regularly quiz banks who they feel are falling outside the industry norms. But it can also be seen as evidence that banks do regard AML/KYC as a function designed to make a real impact on underlying financial crime.

CHART 18
How is the performance of your AML and KYC team measured?

Section iii:
Technology

CHART 20

What is the main challenge your team faces with its current AML and KYC technology?

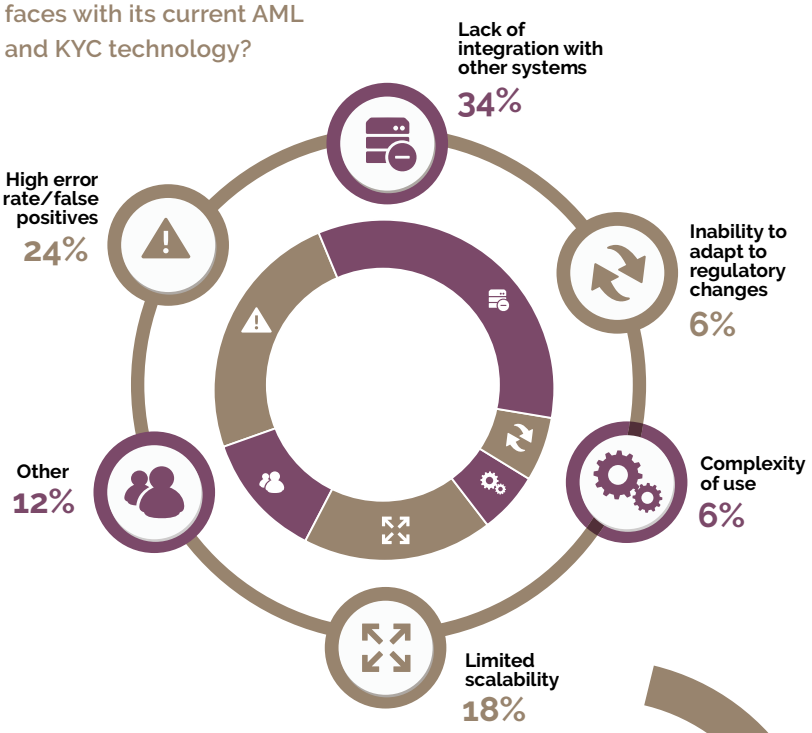
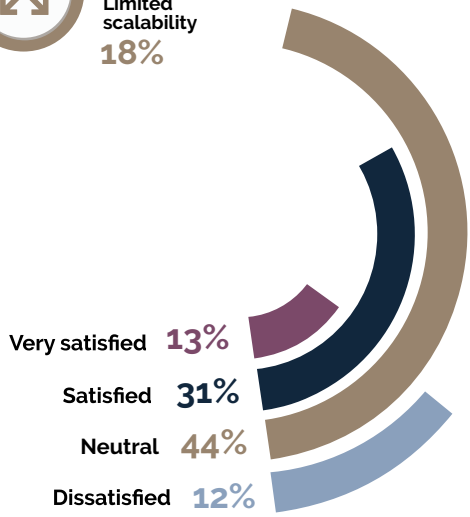


CHART 19

How satisfied are you with your current AML and KYC technology solutions?



The scale and complexity of AML/KYC compliance and risk management has always made it a prime candidate for the use of technology. However, 56% of banks are either neutral or dissatisfied with their current AML and KYC technology solutions.

The main challenges they identify are largely the outcome of legacy technology systems that were never designed to work together, and which may well have been inherited from different organisations as banks grew by merger and acquisition.

Roughly one third (34%) of respondents noted the lack of systems integration within their AML/KYC operations. This fundamental issue then leads to problems of limited scalability (18%), complexity of use and inflexibility – in particular the inability of systems to quickly respond to regulatory changes, creating more reliance on manual systems.

Despite these issues, or perhaps because of them, when asked about which area of AML/KYC requires the most financial investment, 80% of respondents said technology upgrades, and just 13% said staffing

The main driver behind that desire for technology upgrades **[Chart 22]** is operational efficiency and not better risk detection. Where new technology delivers both (as in TM – see below), that is a bonus.

Removing manual processes

The most obvious way to improve operational efficiency in AML/KYC is get rid of manual processes. By far the most common complaint that financial crime leaders have about their operating model is the high manual workload needed for AML/KYC processes **[Chart 6]**. This leads to delays in onboarding, high error rates, and difficulty in adapting to new regulations.

Digging further into the issue of manual processes, we find **[Chart 24]** that 88% of firms say that more than half of their total AML/KYC processes still need to be automated. And **[Chart 23]** for 60% of banks, more than 50% of their AML and KYC processes still rely on manual intervention despite technological improvements.

So where are the bottlenecks? The short answer, according to one US financial crime leader, is everywhere: "We're still talking about the process flows that are amongst the most inefficient process flows in the corporate world, right? TM, negative news screening, PEPs, screening, sanctions screening, periodic reviews – it's not where we need it to be or where we want it to be."

CHART 21

Which area of AML and KYC requires the most financial investment?

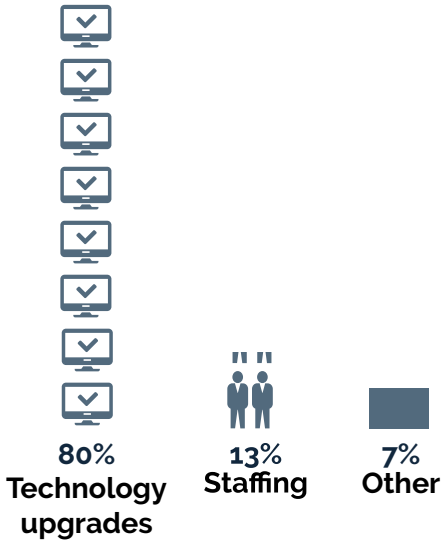


CHART 22

What is the primary driver for upgrading AML and KYC technology?

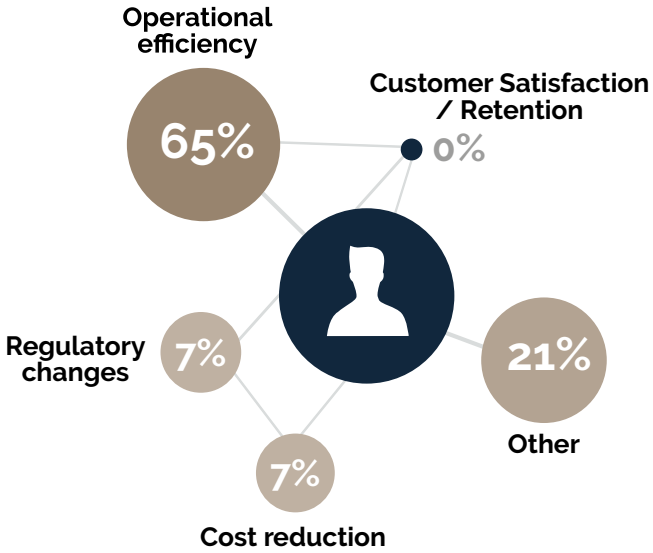


CHART 23

What percentage of your AML and KYC processes still rely on manual intervention despite technological improvements?

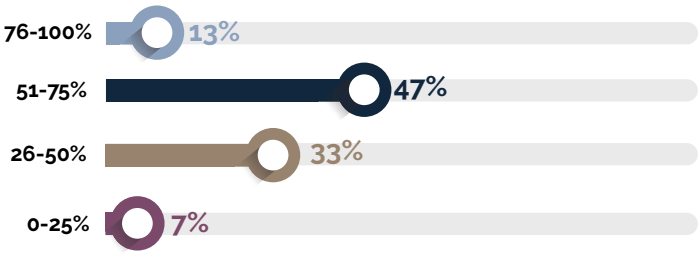
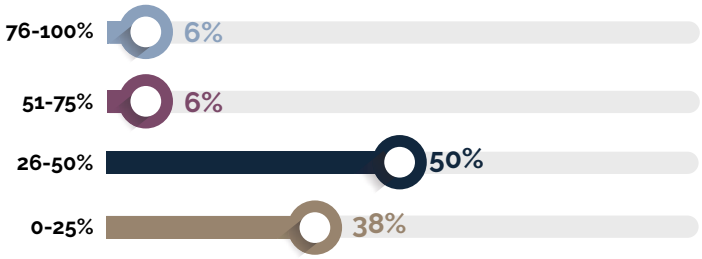


CHART 24

What percentage of your AML and KYC processes are automated?



"TM, negative news screening, PEPs, screening, sanctions screening, periodic reviews – it's not where we need it to be or where we want it to be."

Technology investment choices

However, there are clear areas in which banks plan to invest in the next three years **[Chart 25]**.

First, 75% of respondents anticipate upgrading TM systems in the next three years.

TM is an attractive target because new technology can be applied in a conceptually straightforward way to its existing processes without the need for extensive re-structuring of data and systems. TM can also be incrementally improved by smarter data aggregation and the application of next-generation behavioural and network analysis in the future. By adding unstructured data to the existing structured datasets, banks will be better able to identify anomalous transactions and bad actors.

One example of how new technology is helping both to drive automation and better risk surfacing in TM is the use of machine-learning automation for prioritising alerts for escalation.

As one UK bank's financial crime head explains, "We have got that working well – a system that lets us prioritise alerts on a risk basis rather than just having the TM system output a stream of alerts that we process sequentially. And now we are close to the point where we could simply not process alerts based on this risk-weighting."

In other words, where the machine learning tool indicates that there is, say, a 95% chance that the alert is either a false positive or does not indicate a risk worth investigating, the bank would accept that as the final verdict and close the alerts. Better use of wider datasets (including, for example, from cybersecurity departments or fraud related to devices, IP addresses or location data) and the application of true AI will drive this type of automation further and faster, if regulators accept that the machines do at least as good a job as humans and that testing protocols are robust.

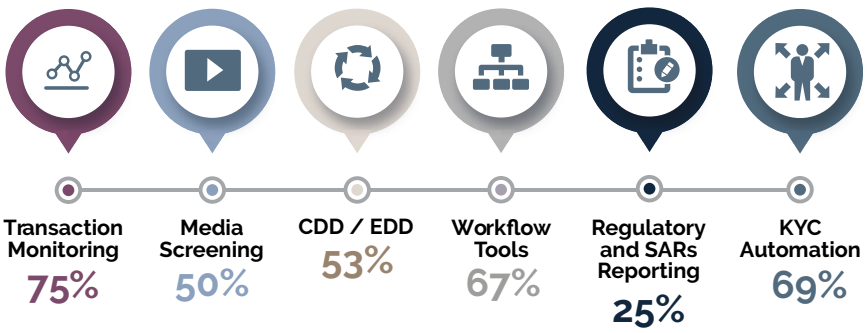
There may also be a regulatory driver behind the focus on TM. Recent enforcement actions by the US Office of the Comptroller of the Currency (OCC) emphasised that banks must be able to demonstrate that they have procedures and controls to ensure that TM systems apply appropriate rules, thresholds, and filters for monitoring transactions, accounts, customers, products, services, and geographic areas; and all of that activity must be commensurate with banks' Bank Secrecy Act (BSA) /AML risk profile.

Moreover, everyone's methodology for establishing and adjusting rules, thresholds and filters must be properly appropriately documented; and its automated TM systems must undergo periodic independent validation. Any time those tests identify something that comes up short, the findings must be documented and promptly addressed.

When regulators find issues with one bank, they tend to look for them everywhere else. So, investing in TM would be a proactive move to stay ahead of enforcements.

CHART 25

Which technologies do you anticipate buying to support your financial crime function in the next 3 years?



Automating KYC is a priority

After TM, KYC automation is the next priority for survey respondents: 69% of banks surveyed said they anticipate the purchase of technology to drive this forward in the next three years.

Banks generally do not mean continuous KYC when they talk of KYC automation. They mean investing in much more basic improvements in the building blocks of a straight-through process for onboarding and periodic review. As one EMEA-based financial crime leader says, "I'm not all that interested in continuous KYC. I'm interested in automated KYC."

Breaking that down, the initial KYC process, including identity verification and other CDD, is still described as "cumbersome and time-consuming" by those running the function. Then there is all the manual intervention required for TM, in alert dispositioning, alert escalation and investigation.

The same is true with sanctions. Much remains to be done in terms of control automation and in the evolution of control testing away from manual audit to more automated processes.

For most banks, the goal is not the application of smart technology and triggers to create a more sophisticated risk management process in AML, it is 'zero touch KYC' – the least possible use of direct client outreach and the greatest use of digital forms of basic information.

What does that mean? First it means digitalising and aggregating anything possible in the initial building of a KYC record with a goal of pre-populating these records as far as possible without human intervention, and then having an RPA perform QA on the record to ensure that fields are correctly filled out.

Very basic improvements include: creating client portals that allow clients to upload documents in digitised form; basic optical character recognition (OCR) for document processing; automated identity verification; and the application of very simple digitalisation to the easiest client groups (e.g. listed entities in highly developed markets).

But technology struggles to overcome the core problems. Clients cannot be forced to use portals or supply digital information, and they want to be able to choose the way that they interact with their bank. "Some want to remain paper-based where they email you information. Other people want digital access where they can just go in and update their records when they feel like it. Others want to be contacted just once to do all 27 subsidiaries in one go and then never be contacted again. So, we have to deal with that – and that also drives models around global, regional local hubs, not just technology," says one EMEA KYC head.

Passports pose a problem. Many corporate executives, especially those who are effectively proxy ultimate beneficial owners (UBOs), are reluctant to email passport images, and are very unwilling to keep on doing so. Another KYC head says, "getting copies of passports is really always a challenge. People also complain, 'if you've already verified me once, why do you need to verify me again? I haven't changed my identity.' But many regulators will not allow an expired passport to sit on a KYC file and so we need the new details."

Some of the manual processes still in use are eye-opening. Major banks still use staff to perform full Google searches on individuals and businesses as part of the onboarding process and also as part of KYC checks for transactions such as M&A.

This is partly out of fear that missing anything on Google would be impossible to explain to regulators. And in M&A it is because standard media screening tools are not flexible enough to handle the tailored queries that banks want answered.

Investing in workflow tooling

This search for very practical improvements in basic KYC processes is behind the 67% of respondents who anticipate spending on workflow tools in the next three years.

The client lifecycle in KYC is extremely complicated. Huge numbers of records need to be reviewed and updated at any given time and that process in its entirety needs to be organised in such a way as to be manageable with the resources available.

The process is broken up into different phases in which the KYC team updates what it can and then has to pass issues over to relationship managers or other parts of the bank for help. Sanctions, adverse media and other data sources must be looked at and incorporated – preferably with some level of automated reminder in the system.

The core requirement is to be able to track the entire life cycle of the KYC record through the different parts of the organisation that need to participate in the record review process. The tooling must be able to incorporate the multiple levels of approvals and possible escalations that can be triggered during a review.

And the tooling must be flexible enough to cope with the fact that many of the requirements within the lifecycle will change with regulations or changes in risk assessment, and the fact that the entire workflow may change over time too.

Many banks have built extremely complicated but highly inflexible versions of this functionality and are looking for more modern solutions. Again though, this is the reality of much of KYC: simply executing the basics is difficult and applying technology to the problems is not a simple exercise.

Enhancing adverse media screening

Half (50%) of respondents also anticipate spending on media screening in the next three years. Most banks run daily adverse media (AM) screening for high-risk clients, with other frequencies and depths of search for different client segments. They export names of individuals and entities to third-party vendors and rely upon those vendors' information sources and search-query capabilities to tailor screening to their own needs.

This process generates large numbers of false positives. It relies upon often inflexible and broad search categories, and it is unintelligent in the sense that sources are not usually weighted according to authority or credibility or veracity, so that stories with multiple sources are not assigned more credibility than outliers and so on.

In short, banks are outsourcing much of the judgement about which sources to use and how to use them – and then handing over much of the responsibility for how searches work to the vendors as well.

New AM solutions claim to overcome many of these challenges. They use AI as well as statistical methods to try to determine veracity, credibility and bias. The use of sophisticated natural language processing (NLP) gives them a better chance of identifying the correct person or organisation and allows the software to read entire articles and not simply samples or headers. And, unlike a human team, they can read everything.

This allows newer solutions to provide highly curated material to human teams for review. This should reduce noise while producing more true positives, many of which would most likely have been missed by traditional processes.

CHART 26

Do you leverage cloud-based solutions for AML and KYC operations?

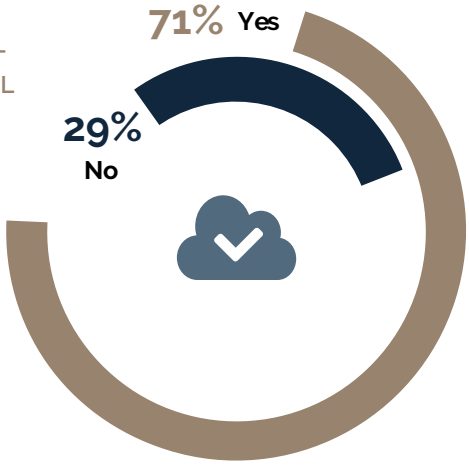


CHART 27

Which external data sources do you leverage for AML and KYC checks?

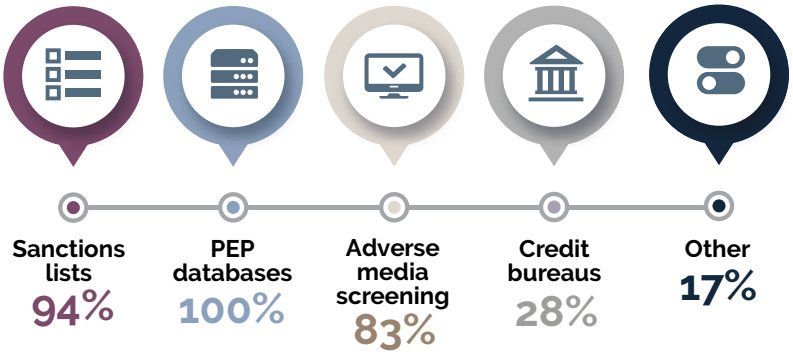
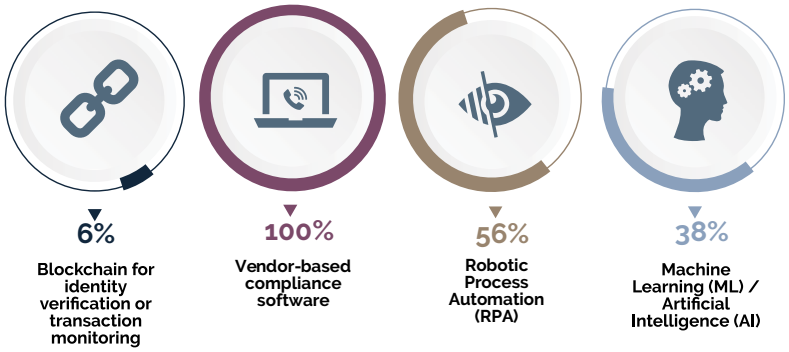


CHART 28

Which technology solutions do you currently use for AML and KYC processes?



Increased adoption of next gen tech

More generally, banks are moving up the curve in their use of both technology and data solutions. All of the banks polled **[Chart 28]** use third-party compliance solutions of one kind or another – in this space, building core functionality is not seen as an option. More than two thirds (71%) use Cloud solutions **[Chart 26]**. And a large majority use third-party, external data sources for key AML and KYC functions **[Chart 27]**.

There has also been reasonable progress in the application of basic process automation techniques such as RPA (56% of respondents use this) and more than a third of organisations are using solutions that incorporate ML or AI.

AI is being applied in three distinct ways. One vendor describes it like this: "The first could be described as administrative assistance; the second is machines starting to make substantive risk determinations; and then, in theory, there is a future in which the machine becomes the compliance officer."

The first stage is here now in AML and KYC. AI and ML are already key tools in the battle to process false positives in TM. The next stage is the use of large language models (LLMs) which are being used to summarise investigations reports, create other kinds of risk summaries, and even to run queries against onboarding data and summarise the results in the form of a recommendation. "The use cases that we started with are things like using LLMs to create risk narrative on TM closures or enhanced due diligence memos, stuff like that," says one US-based financial crime chief.

The second stage is to identify true risks more effectively and efficiently. This could also be called the search for false negatives in TM. Regulators worry far more about the possibility that a compliance process misses a real risk than they do that it generates useless noise. AI holds out the promise of being able to lower the percentage of false negatives significantly, especially if used to augment existing human processes. This idea of augmentation appeals to AML/KYC leaders because it offers a path towards a more technology-driven future that is still acceptable to regulators.

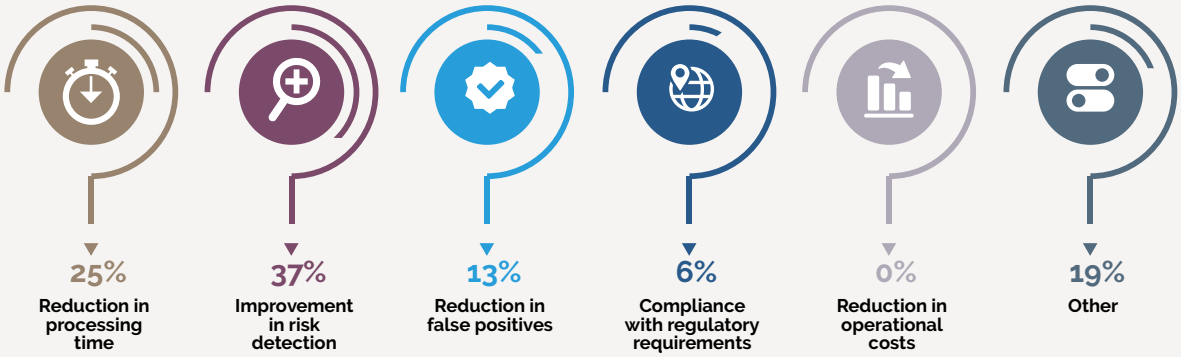
As one financial crime leader says, "Augmentation is a great way to get value fast, on top of what you already have, while remaining in regulatory compliance. It's a good way to balance upside with downside. And it gives us a way out of the 'rip-and-replace' technology strategy that is hard to get buy-in for."

From there, more exotic use cases are being explored, including various types of behavioural and network analysis to detect anomalies and potential risks through smarter analysis of disparate datasets. These rely upon levels of data aggregation many banks still struggle with, given that data siloisation is the root cause of many of their core AML/KYC challenges – such as single view of client and entity resolution. They are the future, but for many banks, that future is distant.

Data is a problem in another way too. The regulators are not only looking at explainability for models that begin to automate risk decisions, but are also looking at the data that underpins those models. They know, as well, that garbage in means garbage out and so before they need to know how an AI model works, they need to be reassured that the data going into the model is good.

CHART 29

What is the primary method for assessing the effectiveness of your AML and KYC technology?



As the detail in recent enforcement actions has shown, regulators are now very interested in the minutiae of banks' data governance and processes. For example, it explicitly requires the bank to "document data dictionaries and data sourcing process maps and desktop procedure(s) related to the Key BSA/AML and OFAC Sanctions Compliance Systems; to create data lineage documentation for the Key BSA/AML and OFAC Sanctions Compliance Systems, and to create comprehensive end-to-end data lineage documentation from Key BSA/AML and OFAC Sanctions Compliance Systems to upstream sources, perform quality assurance of lineage documentation, and define an enterprise process for notification of systems-related projects."

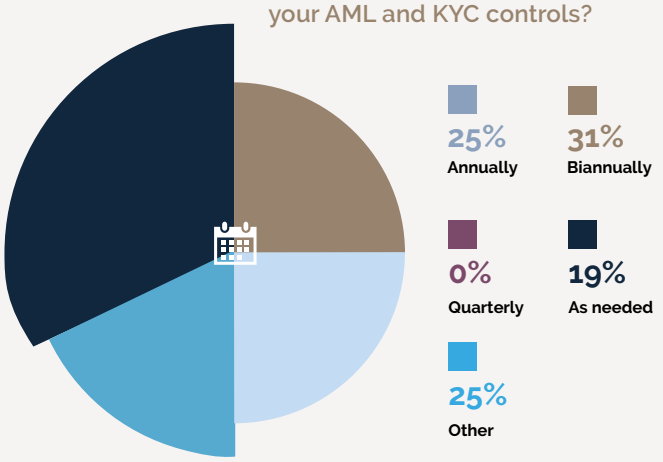
These are not trivial requirements and AML/KYC leaders already report that they are spending more time on these kinds of issues than on core risk management.

The search for effectiveness

While operational efficiency is the primary driver for most technology investment, banks do also look at how technology impacts underlying risk mitigation. When asked specifically about measures of effectiveness, banks clearly define that in terms of 'improvement in risk detection': 37% gave that as their primary method for determining effectiveness. Interestingly, only 6% of respondents equated effectiveness with compliance – which is at least indirect evidence that, regardless of operating model, AML/KYC leaders recognise that the real risk being managed by their teams is a business risk, rather than simply the risk of regulatory sanction.

CHART 30

How often do you review and calibrate your AML and KYC controls?



Section iv: **Oversight, budget and resources**

Given the very public and significant enforcement actions in financial crime recently, it is interesting to see how the management at banks are responding. Are they becoming more involved in the details of AML/KYC and freeing up more resources, or not?

> An overwhelming majority (94%) of financial crime leaders report that senior management awareness and effectiveness in relation to financial crime risks is good or very good [Chart 31],

while 56% say that senior leadership is very involved in making decisions about AML and KYC processes **[Chart 32]**.

In the current political environment, in which pushing back against regulation has become more public and insistent, there are bank leaders who are happy to point out the many shortcomings of the AML/KYC regime.

For example, at a recent roundtable with banking executives led by Senate Banking Committee Chairman Tim Scott, JPMorgan Chase CEO Jamie Dimon called "The AML/Fincen rules…extraordinary" and characterised enforcement as banks being afraid to be fined "because if after the fact something goes wrong — coulda, woulda, shoulda — you could pay a billion dollars." The implication being that the regulatory environment was somewhat arbitrary with regulators able to take a 20:20 hindsight view of decisions that banks do not have.

CHART 31

How would you rate board effectiveness and awareness about financial crime related risks?

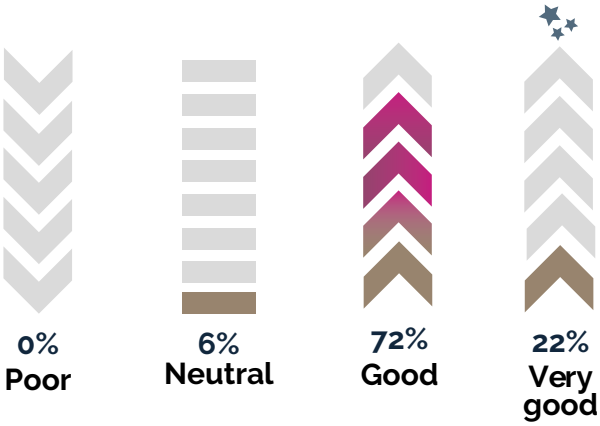
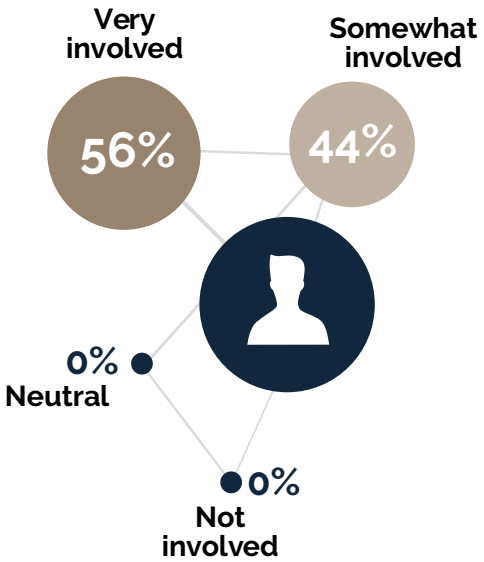


CHART 32

How involved is senior leadership in making decisions about AML and KYC processes?



Budgets, staffing sufficient

While senior management and politicians debate the legislative and regulatory framework, those at the frontline of AML/KYC are happy with the current staffing levels in their functions: 88% **[Chart 33]** say that those levels are sufficient to manage AML and KYC processes effectively, and 67% **[Chart 34]** say that their current AML and KYC budget is sufficient to meet compliance needs – which is not the same as saying that those budgets are sufficient to manage the underlying financial crime risks to their organisations.

There is good reason for most banks to say this. Recent studies estimate that the total cost of financial crime compliance in the US and Canada has reached $61 billion. In EMEA, that figure is estimated to be $85 billion and in the UK alone, UK financial institutions spent the equivalent of $49.5 billion, an increase of 12% on the previous year and up 32% since 2021, according to one recent study. The global total is estimated at a staggering $206.1billion. This amount parallels more than 12% of worldwide research and development (R&D) spending and translates to a monthly cost of $3.33 for every working-age individual globally.

It would be surprising then, with this level of expenditure, for banks to conclude that it wasn't enough. In any case, our survey shows that over the past two years **[Chart 35]**, the budgets at 53% of the banks surveyed increased.

> One third (33%) of banks surveyed said that their budgets fell, but there is a sound explanation: in many cases, spending is tied to specific remediation programmes so when these are completed, budgets revert to a BAU level – a level that has been growing rapidly for the past decade.

Mixed picture going forward

The predictions for the future reflect those dynamics. Half of those who responded predict a fall in budgets, but almost a third think they will increase. This apparent lack of agreement about the future is driven mostly by factors particular to each bank, rather than a more strategic view of the future regulatory or technology environments.

Several large institutions have emerged or are emerging from significant enforcements and their budgets will revert to lower BAU levels. However, some mid-tier banks predict that they will have to invest more to get closer to industry best practices as regulators focus on a more detailed analysis of their data quality, data governance frameworks and on their overall market coverage. And all banks have reasonably well-planned technology cycles, and so are at various stages of plan, spend, run, replace.

Banks are also unsure about the net effect of investment in sophisticated new technologies and the cost savings that may result. Those who are sceptical about pKYC, for example, worry that it will significantly increase their costs. Regulators may want banks to run parallel periodic reviews and pKYC processes, and the new alert stream from pKYC will need to be analysed. One bank calculates that pKYC could increase the level of required client outreach by a factor of four or five because the new alerts will force them to check back with clients more frequently and in greater detail.

More generally, banks accept that if they are to make the best use of new technology, the upfront costs – not just in new AI and other tools, but also in widespread improvements in data – will be significant and it will take time to deliver any promised savings.

Budget predictions may change again if it becomes clear that we have reached the high-water mark in AML/KYC regulation as some banks believe.

Watch this space.

CHART 33

Are your current staffing levels sufficient to manage AML and KYC processes effectively?

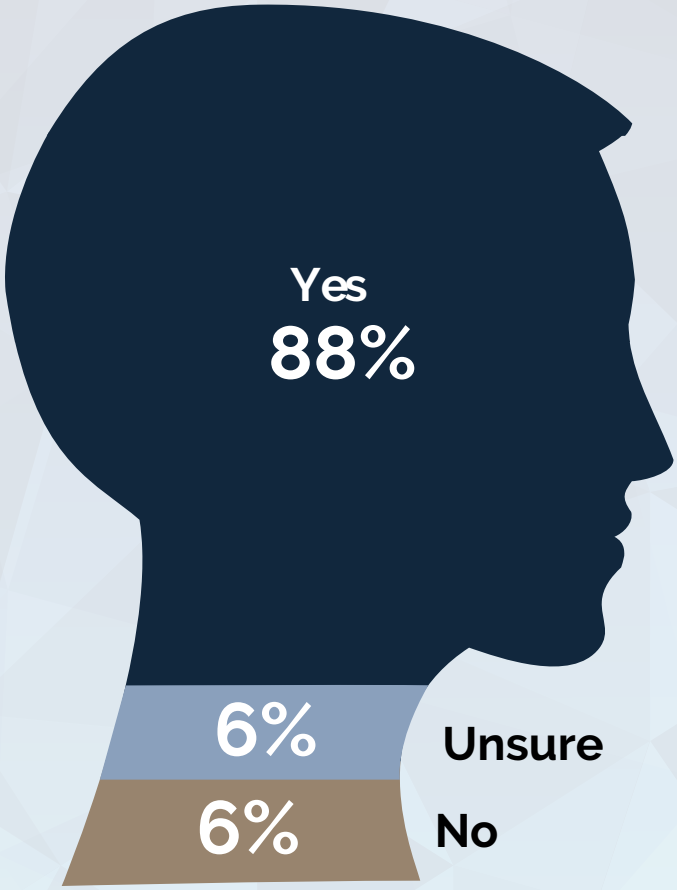


CHART 34

Is your current AML and KYC budget sufficient to meet compliance needs?

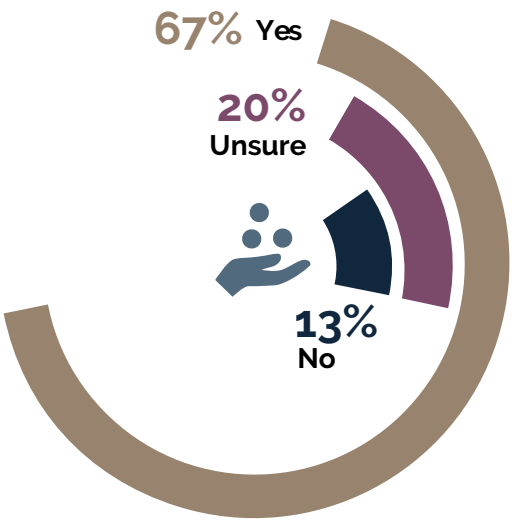


CHART 35

How has your AML and KYC budget changed over the past 2 years?

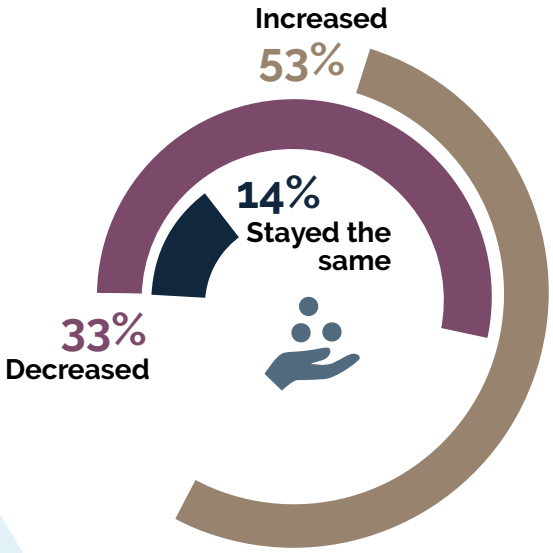
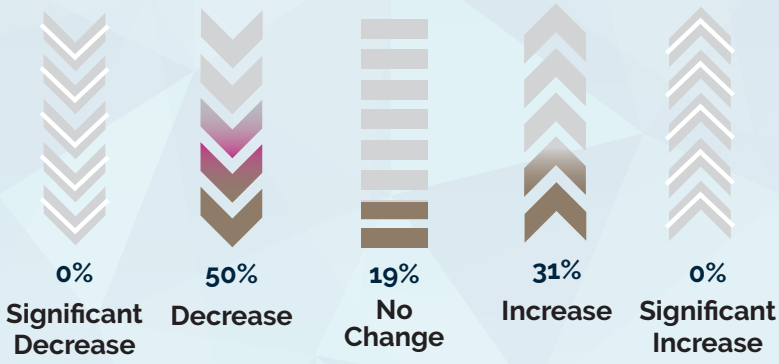


CHART 36

How do you expect the funding of your KYC function to change over the next financial year?



Upcoming Financial Crime events

1LoD®

2025

Strengthening Financial Crime Risk Management through Innovation, Collaboration, and Technology

IN-PERSON CONFERENCE

A 1LoD event

The Financial Crime Summit®

LONDON

11 | Sep | 2025

VIRTUAL EVENTS

01&02 July	Onboarding & KYC Deep Dive
21&22 Oct	AML Deep Dive
02&03 Dec	Fraud Risk Deep Dive

www.1lod.com