AML IN MOTION:

FStech

NICE Actimize

How are financial institutions using technology to manage AML requirements in a fast-moving risk landscape?

INTRODUCTION & METHODOLOGY

METHODOLOGY

FStech and NICE surveyed 100 financial services professionals including heads of risk, heads of operations, heads of AML, heads of financial crime, as well as others from a range of leading financial institutions across the UK and EMEA regions.

INTRODUCTION

Maintaining an effective Anti-Money Laundering (AML) strategy against a backdrop of an ever-changing geopolitical landscape, rising data volumes, and an evolving risk landscape is becoming increasingly difficult for financial services institutions (FSIs) across the UK.

With high-profile cases hitting the headlines, organisations across the industry are reminded of the growing threats of money laundering and sanctions breaches.

These days, technology is vital in the ongoing battle against illicit finance. In this fast-moving risk environment, companies need to leverage innovation across the sector to meet AML requirements.

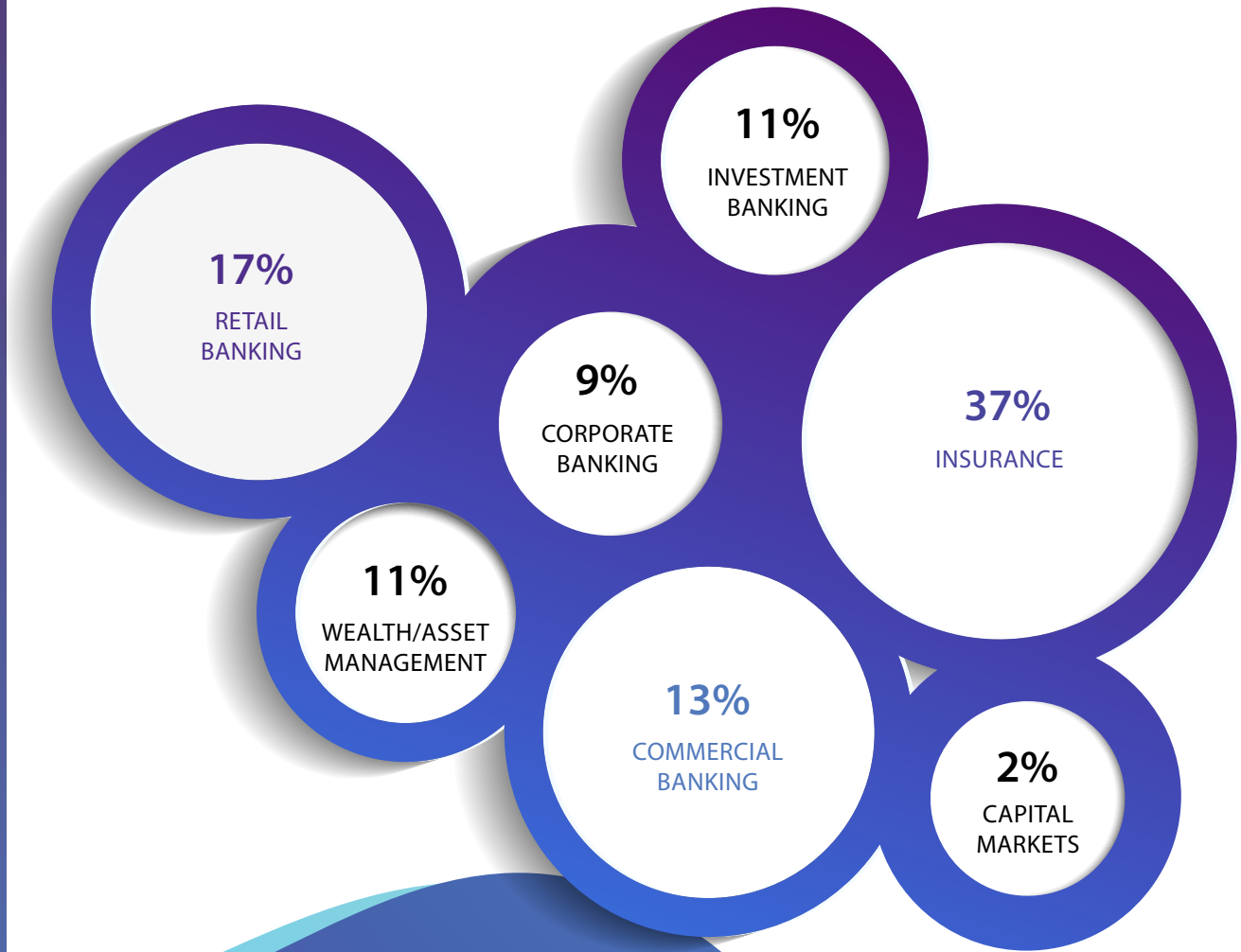
FStech and NICE Actimize conducted a survey to assess the top priorities and challenges for FIs as they develop their AML strategy and invest in the latest technologies to stay compliant and protect their assets, reputation, and clients from criminal activity.

The following results provide a representative snapshot of the key trends, drivers, and challenges for organisations as they implement their AML strategy.

CONTENTS

1. WHICH SECTOR OF THE FINANCIAL SERVICES INDUSTRY DO YOU WORK IN?

(Select one option)



2. WHAT ARE THE KEY AML CHALLENGES FOR YOUR ORGANISATION? *(Select all options that apply])*

Financial crime can undermine not only individual financial institutions but also the U.K.'s entire financial system, making it a priority for all organisations operating in the industry to detect and prevent it wherever it exists.

The survey shows that the majority of financial institutions—more than 60 per cent—are struggling with budget constraints when it comes to delivering their Anti-Money Laundering (AML) strategy. To address this, when rolling out a new AML strategy, firms could deploy a consolidated technology solution to help reduce costs while increasing effectiveness.

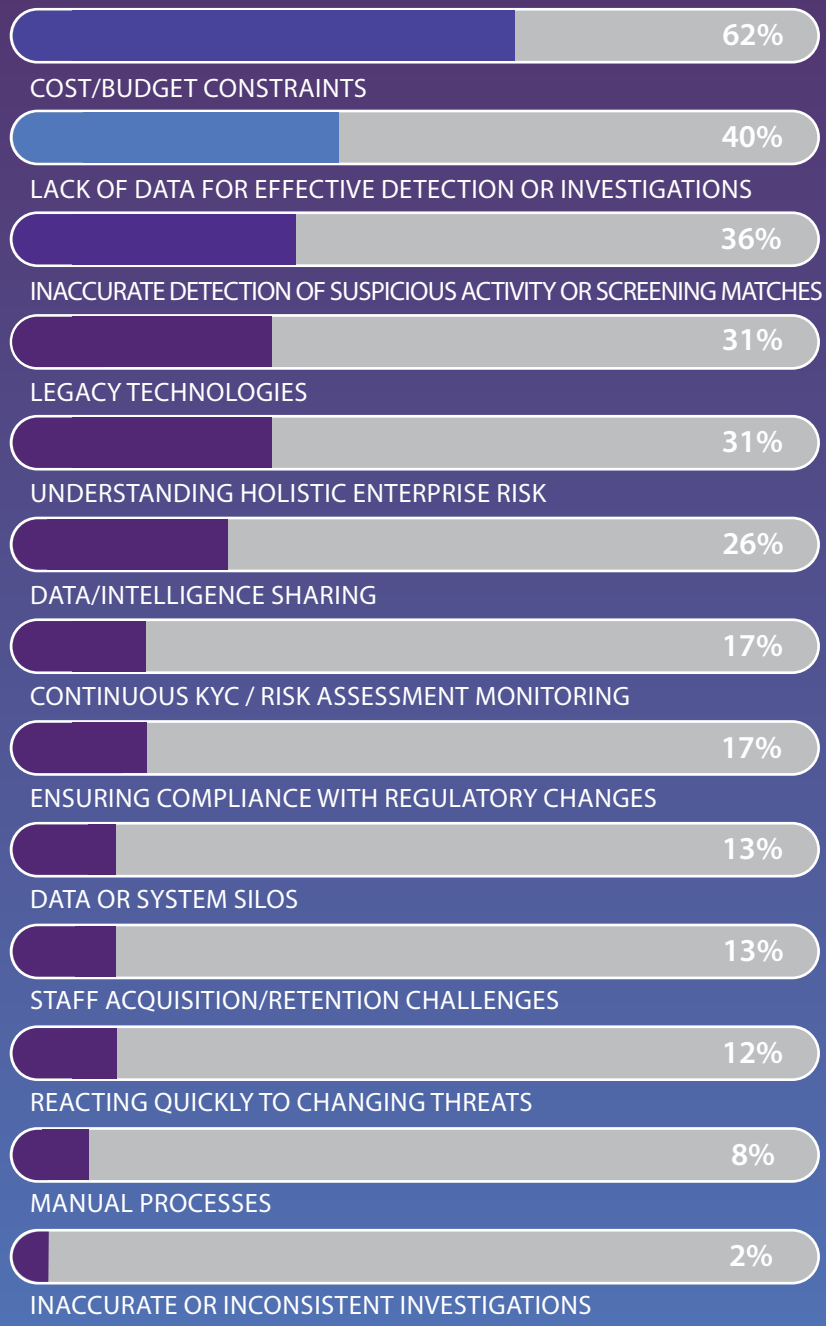
Two-fifths of respondents cited a lack of data for effective detection or investigations as a key AML challenge. The figures demonstrate that there could be room for improvement for many financial institutions when it comes to the collection and management of data to help identify illicit activity and support ongoing investigations. This is backed up by a further quarter—26 per cent —highlighting data and intelligence sharing as an obstacle and just over a third identifying inaccurate detection of suspicious activity or screening matches as a challenge.

The results are likely linked to the nearly third of respondents who believe legacy technology is a barrier, which could suggest that some companies are struggling with digital transformation efforts and lack the right technology to effectively collect, store, manage, and analyse their data.

But with only eight per cent highlighting manual processes as a challenge, it's clear that most financial institutions are no strangers to technology, with many implementing a level of automation in their AML processes.

Understanding holistic enterprise risk was also highlighted as an emerging challenge, with 31 per cent of respondents selecting this as an obstacle. The results could demonstrate a growing trend towards organisations looking to bring together data points to gain a centralised view of risk.

Just over one in 10 chose data or system silos as a challenge. While it is unsurprising that some financial institutions are struggling with data silos, as traditional systems and data pools were built adopting a siloed approach, it is perhaps surprising that this figure is not higher. The results could possibly suggest that organisations already have a plan in place to deal with siloed data and systems or simply have bigger challenges to overcome.



3. WHAT ARE THE KEY MONEY LAUNDERING RISKS YOUR ORGANISATION IS CURRENTLY FOCUSSED ON TACKLING? *(Select top three)*

With nearly a third—32 per cent—of respondents citing well known typology detection as a top-three money laundering risk that they are currently focussing on, it's clear that many financial services firms are still prioritising the basics when it comes to AML, likely because they are still finding this to be a common challenge.

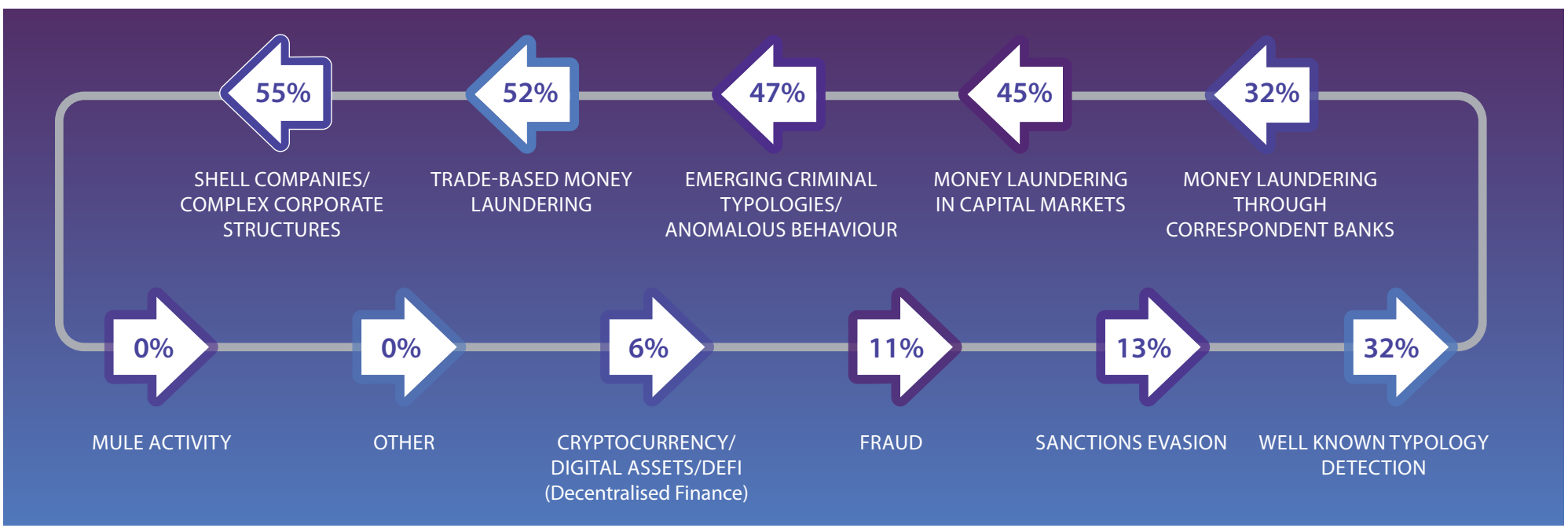
But even more respondents at financial institutions—nearly half—chose less well known or emerging criminal typologies and anomalous behaviour as a key focus, demonstrating that a large proportion of respondents are trying to keep their finger on the pulse when it comes to their AML strategy.

The results reveal that shell companies / complex corporate structures have become a key issue and priority for financial organisations, being chosen by the highest number of respondents. With 55 per cent concentrating on these opaque companies and their ultimate beneficiaries, it's clear that this is currently a significant issue for the industry.

Given the fact that money laundering in capital markets has been a key area of focus for regulators in recent years, it's no surprise that 45 per cent of respondents are also focussing on this as part of their AML strategy.

An even higher number—over half—are concentrating on tackling trade-based money laundering, which includes the misrepresentation of prices or quantities of goods that are transported via international trade routes. This has also been an area of focus for the U.K. government recently. Money laundering through correspondent banks was also highlighted as a key focus for financial institutions, with nearly a third selecting this as a top-three risk.

Lower down on the priority list are sanctions evasion, fraud, and decentralised finance. Mule activity is not an area of focus for any of the respondents in the survey. Given the current geopolitical landscape it is somewhat surprising to see that sanctions evasion is not a priority for businesses. The results may suggest that the participants who were surveyed do not manage sanctions controls or that organisations feel they have been well positioned in their sanctions controls to manage the significant changes in the compliance space over the past several months.



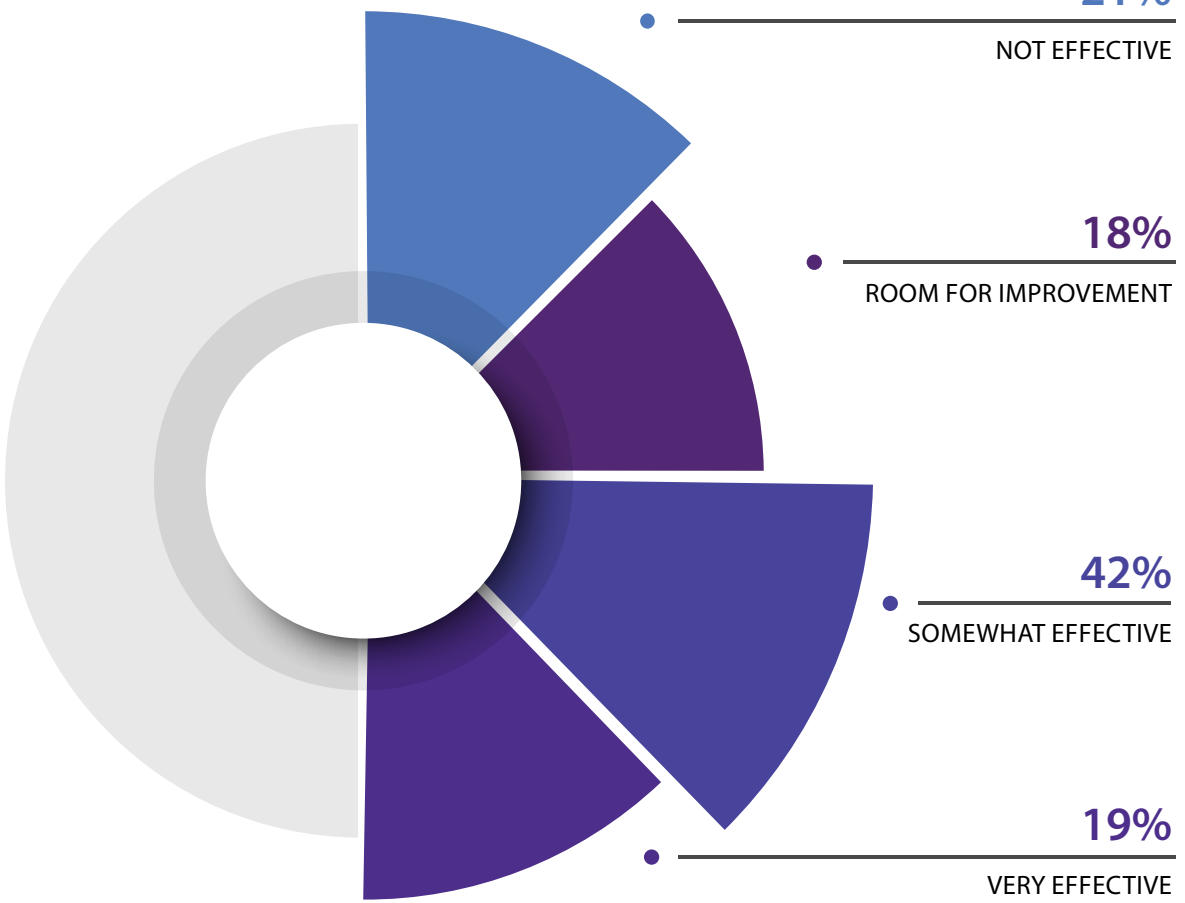
4. HOW EFFECTIVE ARE CURRENT KYC CONTROLS IN IDENTIFYING AND ALERTING ON RISKY ENTITIES BOTH AT ONBOARDING AND ON AN ONGOING BASIS? *(Select one option)*

The results show that most companies still believe there is progress to be made on their KYC controls.

The vast majority—a combined 60 per cent—of respondents are not entirely confident in the effectiveness of their existing KYC controls when it comes to identifying and alerting on risky entities at onboarding and on an ongoing basis. A further fifth of financial services providers don't think their current KYC controls are effective.

Having effective KYC controls is paramount in the battle against financial crime, it is therefore perhaps worrying that less than 20 per cent of those that took the survey are confident in the effectiveness of their KYC controls.

"Most companies still believe there is progress to be made on their KYC controls"

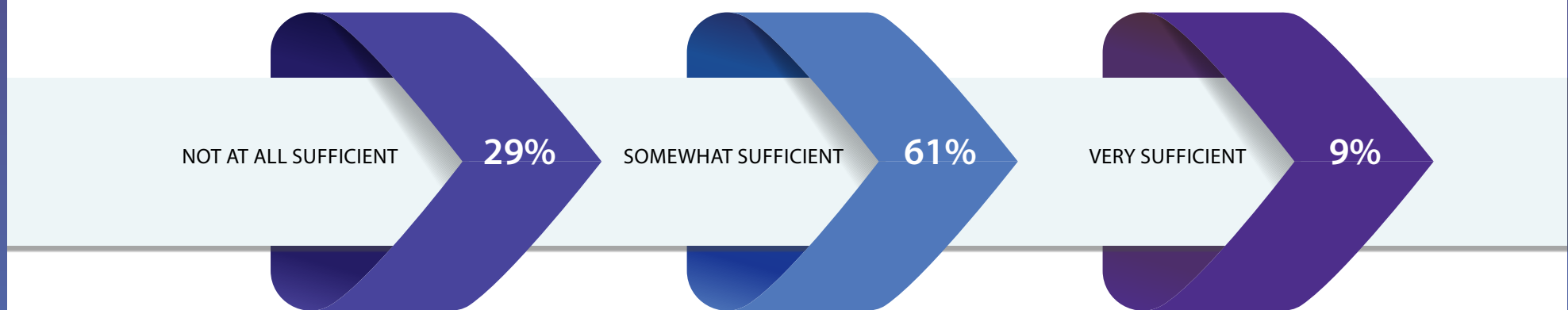


5. HOW SUFFICIENT DO YOU FEEL CURRENT KYC/ONBOARDING CONTROLS ARE IN IDENTIFYING SUSPICIOUS ACTIVITY OR RELATIONSHIPS IN CORPORATE NETWORKS?

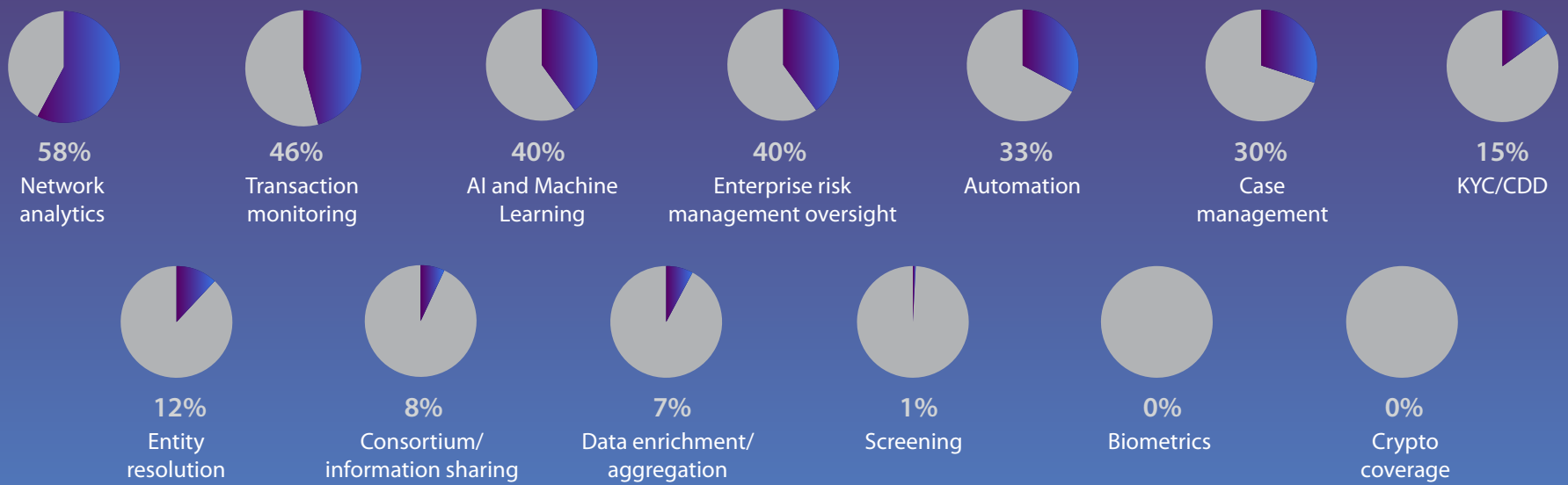
(Select one option)

The results reinforce the trend highlighted in the previous question, that most companies do not think their current KYC controls are sufficient.

When it comes to identifying suspicious activity or relationships in corporate networks, a combined 90 per cent feel that existing controls are either somewhat sufficient or not at all sufficient, while just under one in ten feel their controls are very sufficient.



6. WHICH AREAS OF FINANCIAL CRIME DETECTION WILL BE A PRIORITY OVER THE NEXT 18 MONTHS? *(Select top three)*



Reiterating trends highlighted elsewhere in the report around detection coverage, transaction monitoring was identified by nearly half of those surveyed as a top-three priority area over the next year and a half.

Network analytics, which focus on the connections between individuals and entities and compares them to known patterns of illicit activity to build a picture of money laundering risk, is by far the biggest priority for financial services providers, with almost 60 per cent of respondents selecting this option.

Only around one in 10 consider entity resolution, which operates on similar principles of building a 360-degree view of all parties and their relationships, to be a priority over the coming 18 months. This suggests t hat companies have either already implemented the process as part of a network analytics integration, are unaware of the technique and how it can increase effectiveness across an AML programme, or do not think it is important.

When added to AML workflows, by using entity resolution to duplicate entity records and create a centralised view of the customer and their risk, organisations can help investigation teams gain a complete, consolidated, and up-to-date understanding of entities, which can boost effectiveness and reduce risk throughout a customer life cycle.

Artificial intelligence (AI) and machine learning and enterprise risk management oversight are highlighted as key areas of focus for the months ahead, with two fifths selecting both. Going hand in hand with AI, automation is also a focus for a third of respondents. A further 30 per cent will be focussing on case management in the coming 18 months.

Despite the previous survey results revealing that the majority of financial services companies are not wholly confident in their KYC controls, it's surprising to see that only 15 per cent of those who took the survey said that this would be a top-three priority.

While consortium and information sharing and data enrichment and aggregation were picked by less than 10 per cent of respondents, falling to the bottom of the priority list was screening, with only one person selecting this.

Biometrics and crypto coverage is not on the agenda for any of the respondents.

7. WHICH OF THE FOLLOWING ARE YOU CURRENTLY USING AS PART OF YOUR AML STRATEGY?

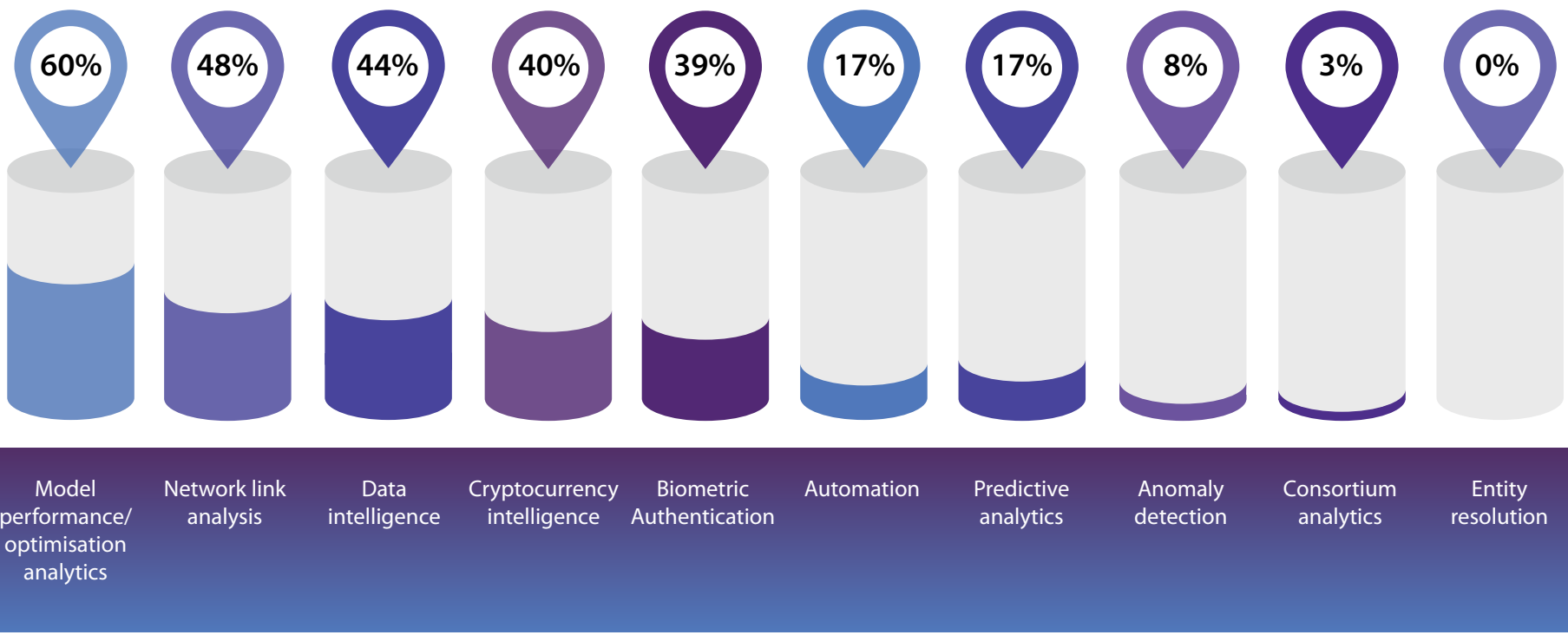
(Select all options that apply

Model performance/optimisation was chosen by the most respondents, while network link analysis was picked by nearly half, and data intelligence is being used by over two fifths. These basic but vital elements are backed up by emerging technologies like cryptocurrency and biometric authentication—which were each chosen by around two fifths.

While automation and predictive analytics are currently only being used by 17 per cent, this could reflect what earlier figures have shown us about companies planning on investing in these technologies over the coming year and a half.

Consortium analytics and anomaly detection are only currently being used by less than one in ten financial services firms, but that's not to say these methods won't be picked up in the future as these technologies continue to mature and are adopted more widely across the industry.

With none of the companies in the survey currently using entity resolution in their AML strategy, and earlier results revealing that the vast majority of financial organisations do not have plans to implement this method in the next 18 months, it's clear that this technique is not a priority for FIs nor is likely to be in the medium term.



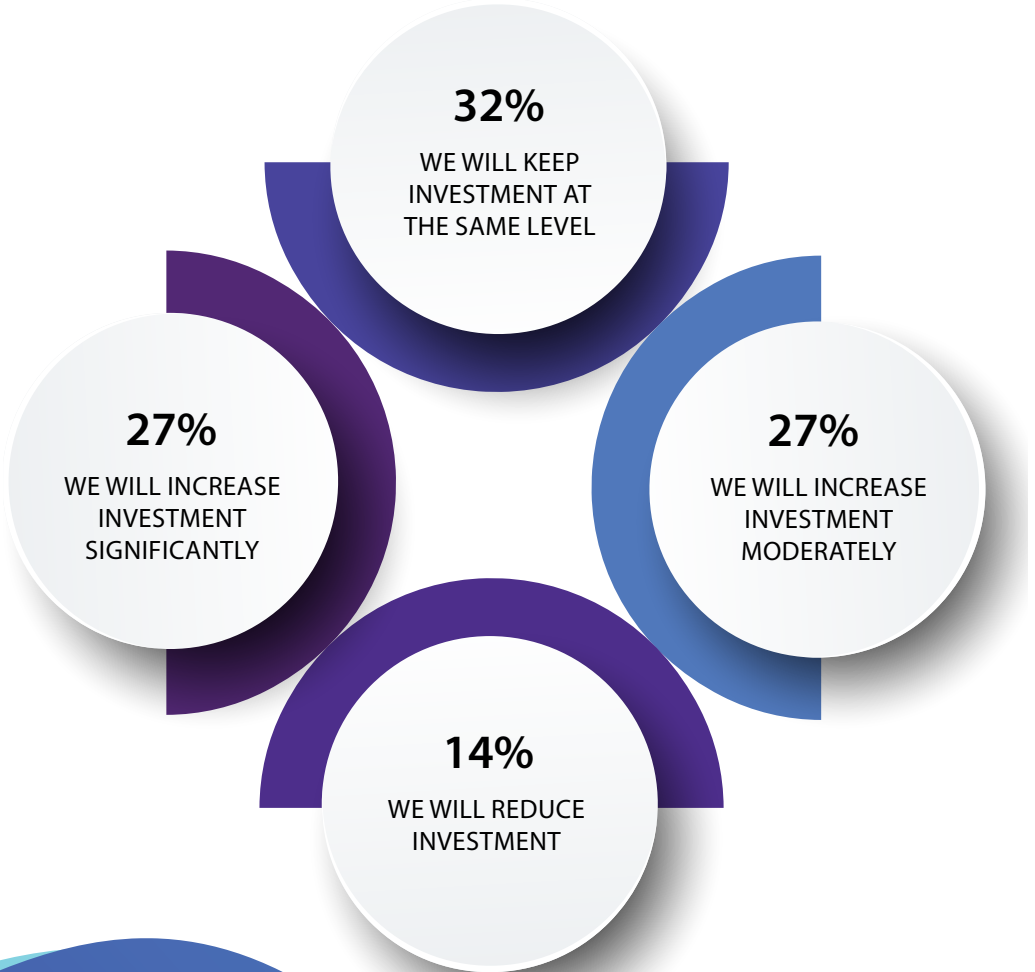
8. HOW IS THE CURRENT AML LANDSCAPE LIKELY TO CHANGE YOUR TECHNOLOGY INVESTMENT PRIORITIES OVER THE NEXT 2-5 YEARS?

(Select one option)

The survey shows that overall, investment in AML compliance is increasing in the medium term.

The majority—a combined 54 per cent—revealed that they are likely to increase investment either moderately or significantly over the next two to five years. With the number of fines for failings in AML on the rise globally, financial services providers may be increasing funding to avoid hefty penalties and sidestep the reputational and legal risk of falling foul of AML regulations.

Nearly a third aren't changing their investment plans at all, while there are some—just over one in 10—that plan to reduce spending. This could be linked to pressures associated with the current macroeconomic climate. With revenue sources disrupted, some financial institutions are being more cautious about spending.



9. HOW ADVANCED IS YOUR FINANCIAL SERVICES ORGANISATION IN SUCCESSFULLY PERFORMING CONTINUOUS MONITORING FOR CHANGES IN AML-KYC RISK?

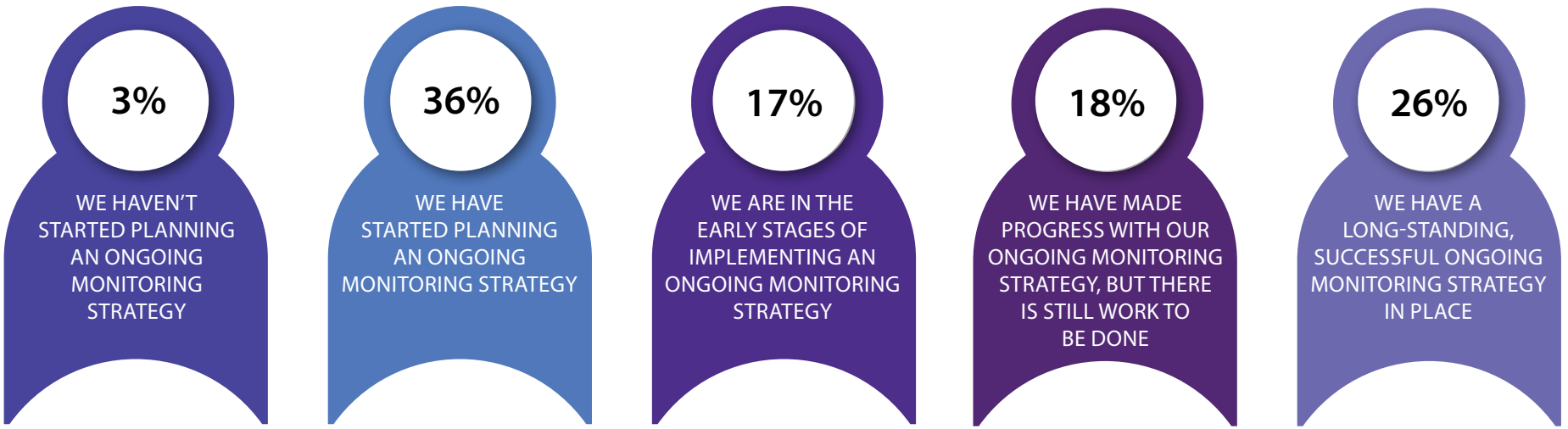
(Select one option)

Just over a quarter of respondents already have a long-term monitoring strategy in place. But most respondents haven't yet completed or solidified their monitoring strategy.

Nearly a fifth said that while they have made progress, there is still more progress to be made. A similar number of respondents revealed that they are still in the early stages of implementing a monitoring strategy.

The highest number of respondents—36 per cent—revealed that they haven't yet implemented a strategy but are in the planning stages. FSIs could implement new technologies to help speed up the roll out of their monitoring strategy.

Just three per cent revealed that they don't currently have plans for an ongoing monitoring strategy.



CONCLUSION

The survey shows that the most significant AML challenges currently impacting FSIs are budget constraints, a lack of data for effective detection, and inaccurate detection of suspicious activity, while understanding holistic enterprise risk appears to be an emerging obstacle for financial services organisations.

Shell companies or complex corporate structures were identified as the top money laundering risk that firms are currently focussing on. Both well-known typology detection and emerging typologies are also a key focus for businesses operating in the financial services market. With money laundering in capital markets high on the agenda for regulators, many FIs are responding by concentrating on this risk category.

Over the next 18 months, the greatest priority area of financial crime detection is network analytics, with almost 60 per cent of respondents identifying it as a key method. Transaction monitoring is also an important technique for organisations, alongside AI and machine learning, enterprise risk management oversight, and automation.

Entity resolution was only chosen by just over one in 10 respondents as a priority area, despite this technique having many benefits and arguably being necessary for successful, modern AML programme. The majority of FSIs—a combined 60 per cent—are not entirely confident in their KYC controls when it comes to identifying and alerting on risky entities both at onboarding and on an ongoing basis. Only a fifth felt their KYC controls are very effective, while even more said current controls are not effective at all.

Financial organisations are also not wholly confident in their KYC controls in relation to identifying suspicious activity or relationships in corporate networks.

A combined 90 per cent feel that existing controls are either somewhat sufficient or not at all sufficient, while the remaining 10 per cent think their company's KYC controls are very sufficient.
The most common methods currently being used by FIs as part of their AML strategy make up the core components for optimised and effective AML monitoring detection: model performance/ optimisation; network link analysis; and data intelligence.

Overall, investment in AML compliance is increasing in the medium term. Most respondents—a combined 54 per cent—said that they are likely to increase investment either moderately or significantly over the next two to five years.

The majority of respondents have not yet completed or solidified their monitoring strategy. The highest number of respondents—36 per cent—revealed that they haven't yet implemented a strategy but are in the planning stages. FSIs could implement new technologies to help speed up the roll out of their monitoring strategy and manage AML priorities in a fast-moving risk landscape.