The State of Global Anti-Money Laundering Compliance Report

November 2022

The Money Mule Market

The staggering amount of money laundered each year - as much as $2 trillion - is comparable to the GDP of some of the world's most advanced economies. It falls to anti-money laundering (AML) compliance professionals to address the almost Herculean task of stopping money laundering and the harmful crimes it finances, from illegal drug sales, weapons trades, human trafficking, and more. AML compliance costs reached $213 billion worldwide in 2020.

But as this report details, the job of AML compliance teams becomes more challenging by the day. Take the financial services landscape itself, for example. As open banking regulations expand, advanced data orchestration becomes critical for compliance teams. Yet, under half of the survey respondents note that this is the least successful element of their AML strategies. As such, almost two-thirds (61%) of organizations are prioritizing the automation and consolidation of AML/KYC data across their various legacy systems over the next five fears.

Meanwhile, emerging payment types (e.g., cryptocurrency) now play a critical role in enabling money laundering to flourish globally via shadow economies that circumvent detection. More than half of AML professionals said multi-customer, cross-wallet activity was the top money laundering typology of concern. This refers to a customer's ability to have opaque fiat and crypto wallets with several financial institutions. Cryptocurrency exchanges and money mule schemes were cited as the top two money laundering techniques and key pain points for AML professionals.

The good news for AML professionals is that global financial organizations are raising alarms over cryptocurrency as a money laundering vessel. The World Economic Forum and the International Monetary Fund have recently called for cryptocurrency regulations to promote safer adoption. Recent regulatory guidance from the EU's Markets in Crypto-Assets (MiCA) and the US Framework for International Engagement on Digital Assets indicate a desire to provide regulatory clarity. This push for greater crypto regulation comes as fraudsters turn digital currency into a $1 billion industry using a variety of scams, according to the Federal Trade Commission (FTC).

Despite the rise of cryptocurrency as a money laundering tactic, our survey found many financial institutions are ill-prepared to address it. Only 26% of respondents said they used technology to evaluate cryptocurrency's risk. That translates into nearly three-quarters of respondents who are behind on assessing their crypto risk.

Global AML regulations have become incredibly nuanced in response to Russia's invasion of Ukraine. Additionally, regulations are constantly changing. Russia is viewed as the riskiest country for money laundering, followed by China and the United States.

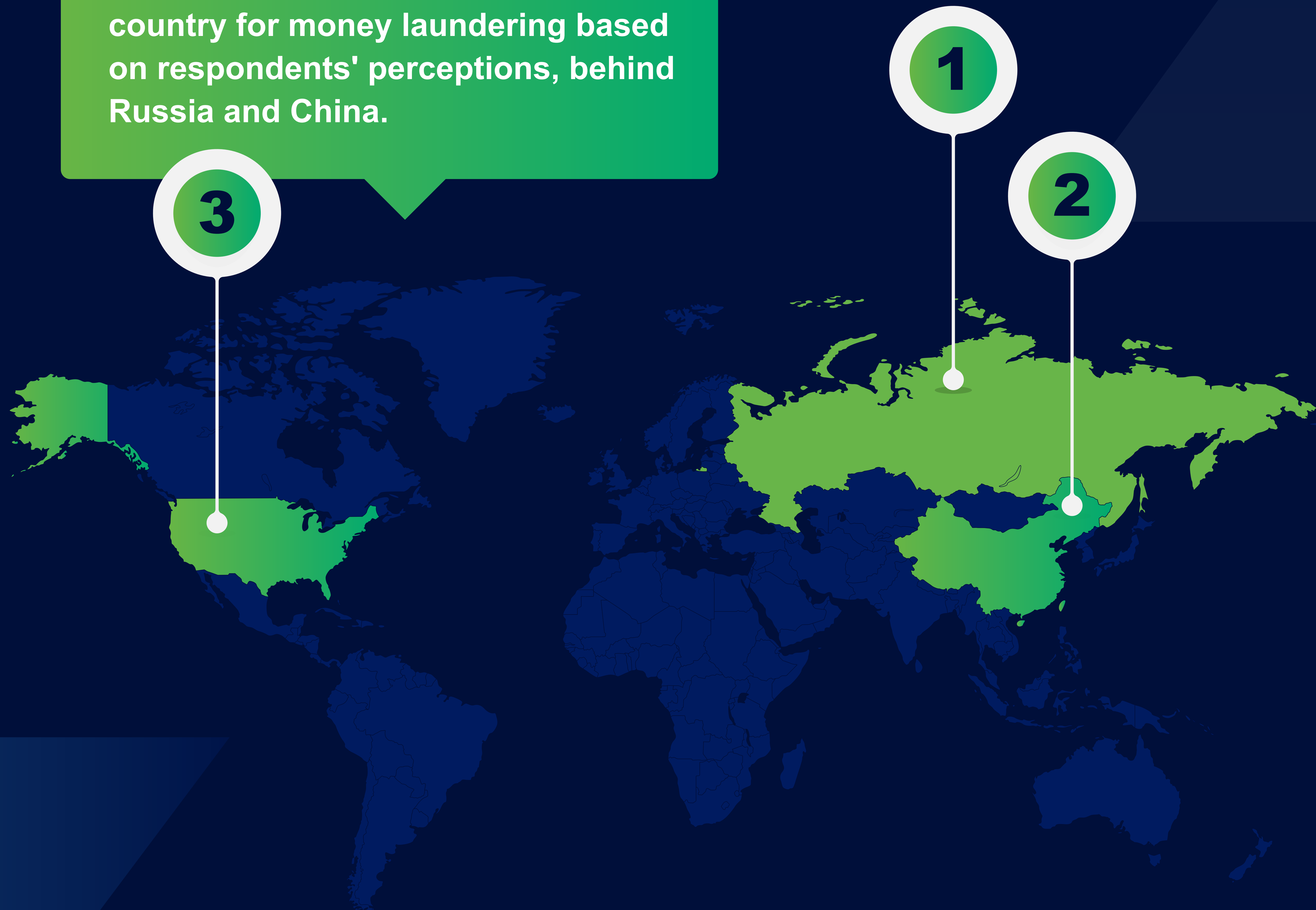
This gap in perceptions of the most significant money laundering risks and how to address them is a recurring theme among respondents. The exclusive findings in the report noted that analysts and executives are frequently on different pages regarding how to handle money laundering challenges.

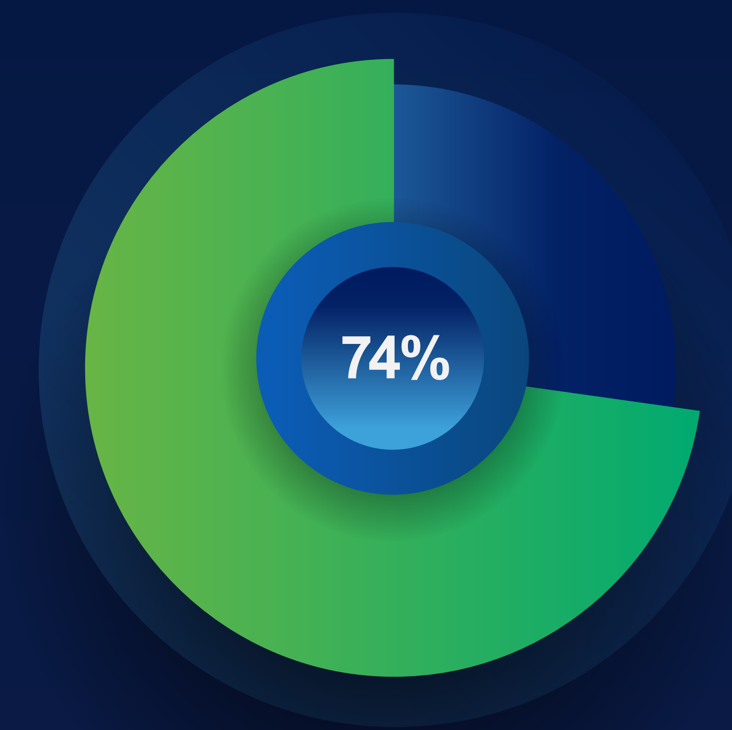
Risk is also top of mind during these times of economic uncertainty, with whispers of a recession and rising inflation putting many people on edge. These uncertain economic conditions create fertile ground for money mules, be they witting, unwitting, or complicit. It is, therefore, no surprise that 74% of banks worldwide cited money mules as their most common money laundering typology. This has prompted several global banks to post warnings to their customers about the risks of participating in money mule scams. Some banks even warn their customers that they risk prison time for participating in a criminal organization's mule scam.

Feedzai's new *Global Anti-Money Laundering for Financial Services Survey Report*, based on input from AML professionals worldwide, sheds light on the scope of the money laundering challenges compliance professionals face. The survey is based on over 630 answers submitted by AML compliance experts around the world to 19 questions in four categories.

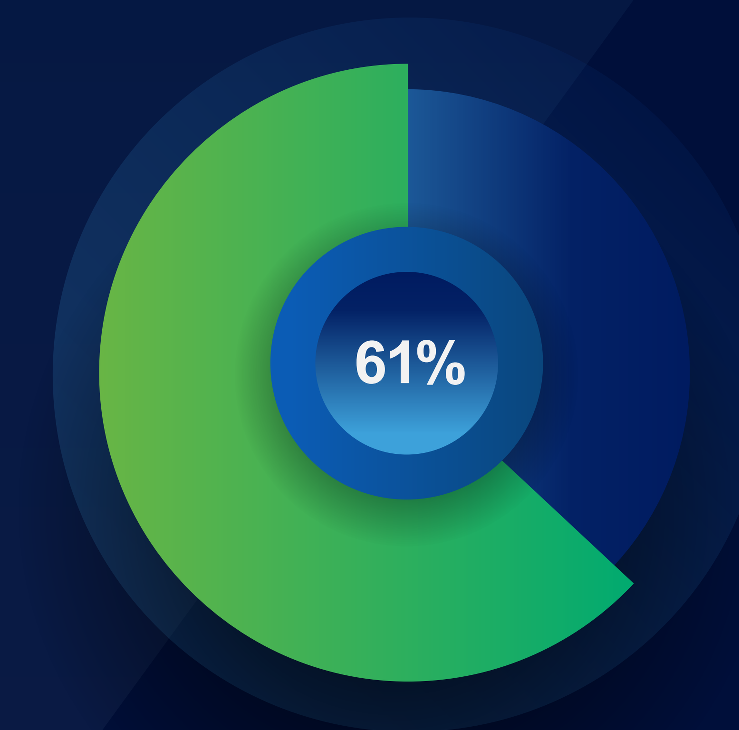
Key Findings

The US ranked as third riskiest country for money laundering based on respondents' perceptions, behind Russia and China.

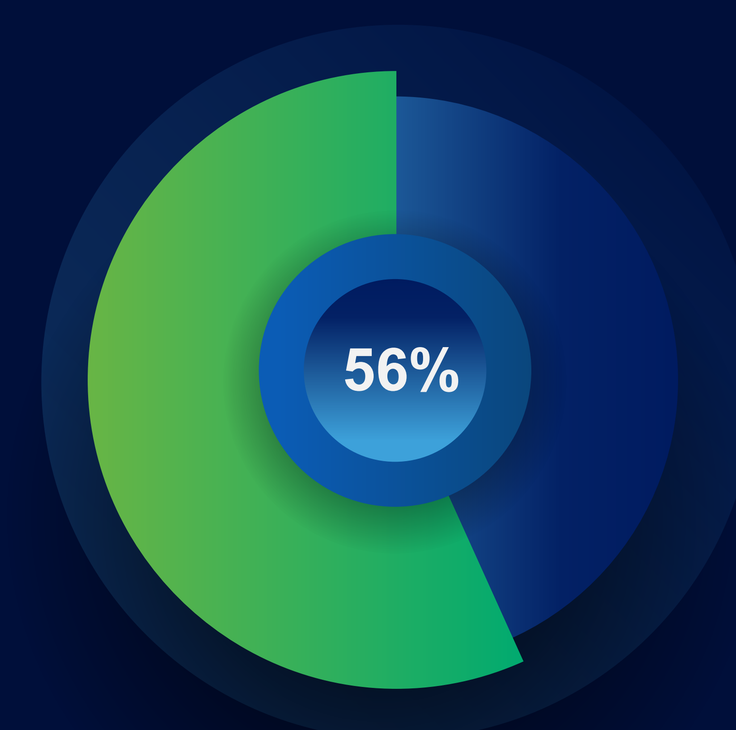




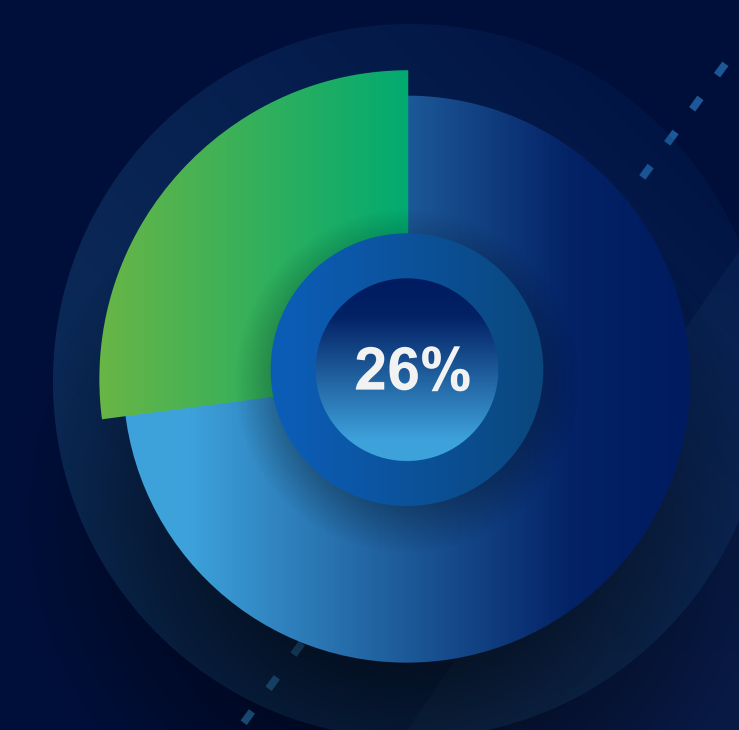
74%
of money laundering typologies involve money mules



61%
of organizations are prioritizing automation of AML/KYC data from multiple vendors over the next five years



56%
of AML professionals cite multi-customer cross-wallet activity as the top money laundering typology



26%
of respondents said their organization wasn't using technology to evaluate cryptocurrency risk, even though cryptocurrency ranked as a top money laundering technique

The Global State of Anti-Money Laundering

North America

AML efforts are gaining strength in North America following a series of regional initiatives. The US Congress passed the Anti-Money Laundering Act of 2020 (AMLA) in 2021. Two notable changes in AMLA are the creation of a national beneficial ownership database and expanded subpoena powers for law enforcement. Congress is expected to continue exploring, educating, and moving ahead with preliminary decisions on legislating the cryptocurrency space as a medium of exchange and asset class. This action will lead to downstream considerations for US law enforcement on managing associated risks within the crypto ecosystem.

Meanwhile, the financial industry is quickly moving ahead with its own AML safeguards. Many FIs are adopting perpetual Know Your Customer (pKYC) programs that will tangentially impact their transaction monitoring and sanctions screening capabilities. At the same time, collaborative efforts between fraud and AML teams are increasing, with organizations implementing information-sharing processes to improve their financial crime programs' efficiency.

Europe

In July 2021, the European Commission proposed a major reform in the plan for a European AML Authority (AMLA) and the implementation of four legislative proposals aimed at strengthening the EU's AML/CTF rules. The measure proposes a consistent framework to ease compliance obligations for covered entities, particularly for those with “cross-border” activities. While this won't be operational until 2024, the proposed measure will use the Financial Action Task Force’s (FATF) framework as a baseline. This reflects of the complexity of the Sixth Anti-Money Laundering Directive's (6AMLD) requirements across member states, their implementation approach, and the implications for financial institutions operating across and within Europe.

Data sharing and regulations around GDPR have fostered views that AML effectiveness is hampered because financial institutions can't share customer data, such as KYC and suspicious transactional information. However, progress is being made through “private-private partnerships.” Examples of this are the Dutch and Nordic Banks setting up such arrangements. While these are early and limited examples, their scope and participation may expanded significantly.

Virtual currencies are also a key regulatory focus with greater alignment to the FATF's guidelines and “Travel Rule,” which requires organizations to share information for certain digital transfers. The data “travels” with the transaction to every bank it encounters until it reaches its final destination.

The UK is experiencing an increase in the use of money mules. Whether they are witting, unwitting, or simply vulnerable individuals is not clear. Money mules are anticipated to increase significantly given the financial challenges facing many in the UK. As Sarah Pritchard, the Executive Director for Markets at the UK's Financial Conduct Authority, explained, "Sadly we expect financial crime to become even more prolific during the cost of living crisis.”

Asia Pacific

The Asia Pacific (APAC) region has various regulatory requirements and standards, leading to a wide range of AML/CTF compliance maturity. The good news is that most jurisdictions have implemented FATF and other internationally recognized best practices into local legal and regulatory frameworks. Financial institutions demonstrate a higher propensity for adopting advanced technologies such as artificial intelligence (AI) and machine learning (ML) to manage financial crime risks effectively. Still, they need people to run these programs and investigations. There are ongoing AML/CTF staffing challenges to meet operational and executive-level requirements. Investment in technology and staffing will likely remain the biggest priorities for financial institutions in combating financial crime in 2023 and beyond.

The Middle East and Africa

The rapid move to digital payments due to the pandemic, the emergence of cryptocurrency, and the need to appeal to global investors drive a recognized need for more significant AML efforts in the Middle East and Africa (MEA), but progress is slow.

The United Arab Emirates (UAE) has taken numerous steps to improve and strengthen its AML/CTF frameworks, yet in March 2022, the FATF placed the region on a “gray” list. The gray list indicates the UAE is deficient in its AML/CTF frameworks but is working with the FATF. This collaboration produced commitments by the UAE in the critical areas of combatting sanctions evasion and increasing financial intelligence resources. The UAE also made high-level political commitments to support these initiatives.

South Africa's FATF Mutual Evaluation Report (2021) identified several flaws in its AML framework. These include a better understanding of primary profit-generating crimes and the routes for laundering these funds, adopting national AML/CTF regulations for high-risk entities, and suggestions for mitigating the perceptions that the financial system is tolerant of crime.

Latin America

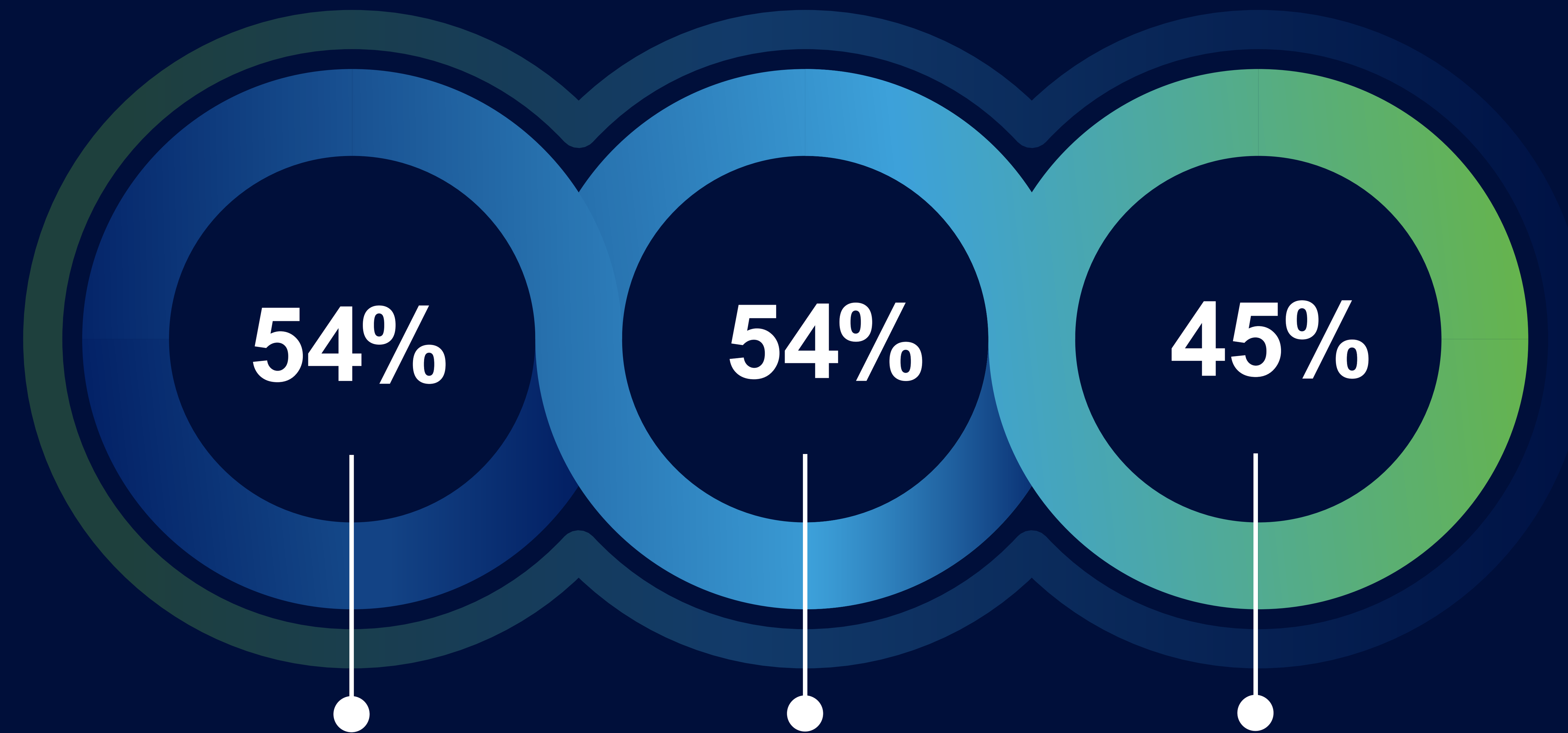
Anti-money laundering compliance is still in its infancy in Latin America (LATAM) compared with other regions. Primarily, this is because LATAM lacks the infrastructure to create a cohesive approach to address corruption, money laundering, and organized crime. Of the twenty countries in Latin America, six are on the Basel AML Index, an independent annual ranking of risk for global money laundering and terrorist financing (ML/TF). Unfortunately, the pace of technological advancement paired with the region's economic challenges blunt any real progress. A step in the right direction would be a commitment to technological advancement to combat illicit activity for both regulated organizations and regulatory bodies. Moving forward, greater collaboration between local governments and regulatory authorities is critical.

Survey Results

What are your main goals for 2022 and beyond?

Financial institutions spend $213 billion annually on compliance. The effort does not equal the $2 trillion problem, but they're also not getting a good value based on their results.

Banks are looking to be smarter and more efficient at compliance. pKYC and the reduction of false positives are tied for the number one goals for 2022 and beyond. pKYC monitors customer changes, such as changes in address information, potential adverse media alerts, or occupational changes, in real time rather than during periodic reviews. Improving false positives means that AML analysts investigate the right leads. The second goal of worldwide organizations is to accelerate AML investigations, which are enabled by data analytics. This allows teams to make risk-based decisions using the correct data. Reducing false positives was the number one goal when viewing responses by roles in an organization.



Achieve pKYC/real-time customer monitoring

Reduce false positives/ improve accuracy

Accelerate AML investigations

Other goals lagged considerably behind the top three:

- **29%** Create a single customer view using all data points
- **28%** Improve adverse media screening/monitoring
- **23%** Increase data sharing between company departments
- **19%** Accelerate onboarding/reduce “time to revenue”
- **4%** Outsource AML/KYC

From a regional perspective, only North America deviated from the overall results. North American banks typically have larger transaction volumes and are likely more concerned with costs as they deal with more customers and transactions than other regions.

APAC, EU, MEA

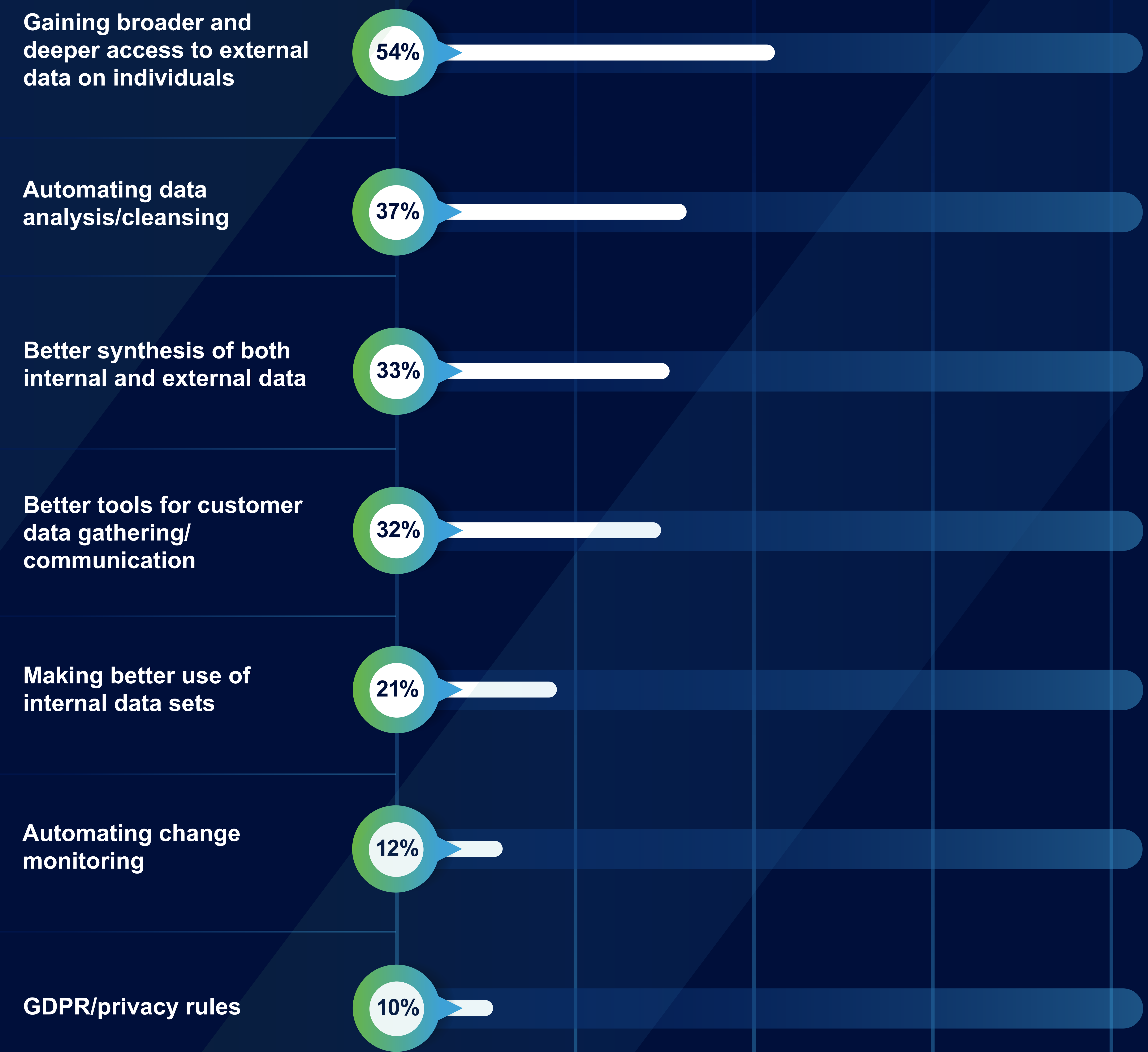
1. Achieve pKYC/ real-time customer monitoring
2. Reduce false positives/ improve accuracy
3. Accelerate AML investigations

NORAM

1. Reduce false positives/ improve accuracy
2. Accelerate AML investigations
3. Achieve pKYC/ real-time customer monitoring

What are your top data challenges or pain points?

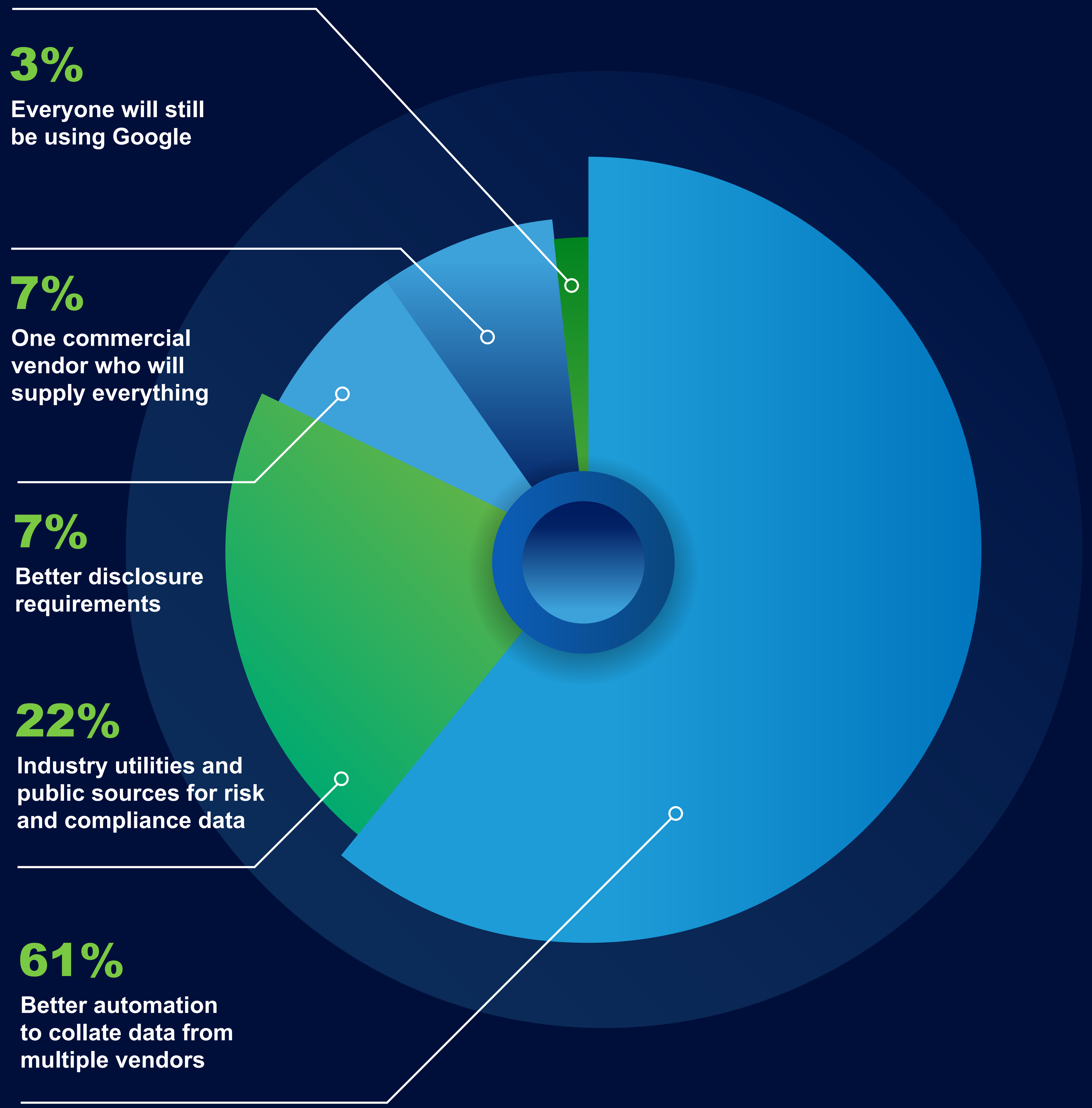
AML teams must gather data from numerous sources to understand the risk associated with each customer. These include watchlists, social media, and adverse media. For some small banks, this means analysts must Google their customers. Such tedious tasks cause high error rates. All financial institutions need access to comprehensive, accurate data to make fast, correct risk decisions.



What will the future of AML/KYC data look like over the next five years?

Accessing data is only one piece of the puzzle. The next step is doing so efficiently. A third of banks expect better automation for data collation to be a standard practice in the next five years.

There is an additional benefit to automating data collation across vendors: digital trust. Firms that take a RiskOps approach use a single platform across fraud and AML. This means risk teams can use KYC data to verify identities and protect against fraud at the transactional level.



There were no significant differences across roles, but there were some differences among different regions. The Middle East and Africa prioritized better disclosure requirements.

APAC, EU, NORAM

1. Better automation
2. Industry utilities and public sources for risk and compliance data
3. One commercial vendor who will supply everything

MEA

1. Better automation
2. Industry utilities and public sources for risk and compliance data
3. Better disclosure requirements

What is the most common money laundering typology you've identified?

Money mule schemes are the most common money laundering typologies identified by AML professionals.

Multi-customer cross-wallet activity, a favored tactic of money launderers, ranks number one on the list. In a multi-customer cross-wallet activity scheme, Jane, who banks with ACME has multiple accounts or wallets within ACME and moves money between them and also to John, who similarly has multiple accounts.

Financial institutions should agree on fraud labeling practices and share data to make a meaningful impact on money mule schemes. This collaboration would better protect unwitting money mules from scams. It would also help organizations identify money laundering sooner.

56%
Multi-customer cross-wallet activity

51%
Use of crypto and non-compliant exchanges

44%
Unwitting money mules

30%
Witting money mules

19%
Laundering through cryptocurrency ATMs

What is the most challenging AML regulatory issue?

AML teams have always had to navigate complex regulatory changes issued by numerous governing bodies. But the sanctions against Russia are unprecedented in their nuances.

Additionally, teams have had to contend with new regulations. The most significant is the EU's 6AMLD and the FATF Travel Rule. AML compliance teams are under extreme pressure.

77%
Increased regulatory expectations

45%
Understanding regulations outside home country

38%
Increased enforcement of current regulations

22%
Understanding regulations in home country

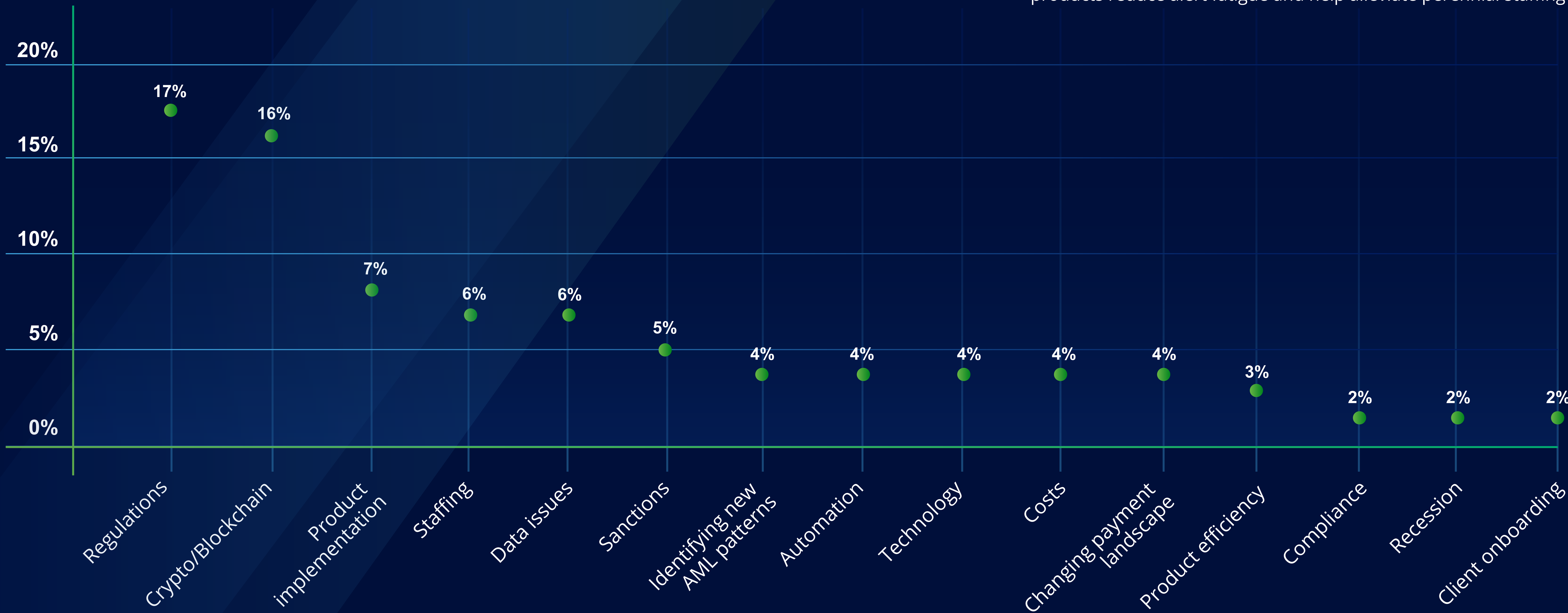
19%
Formal regulatory criticism

Name the two biggest market challenges that will impact your AML program in the next two years.

This write-in question was answered by 305 respondents who shared 551 responses.

The top response was definitive across regions and roles, with regulations and crypto/blockchain posing the most significant challenges by almost three times as much as the next pain point. Crypto is an urgent challenge, but only a quarter of organizations address crypto risk.

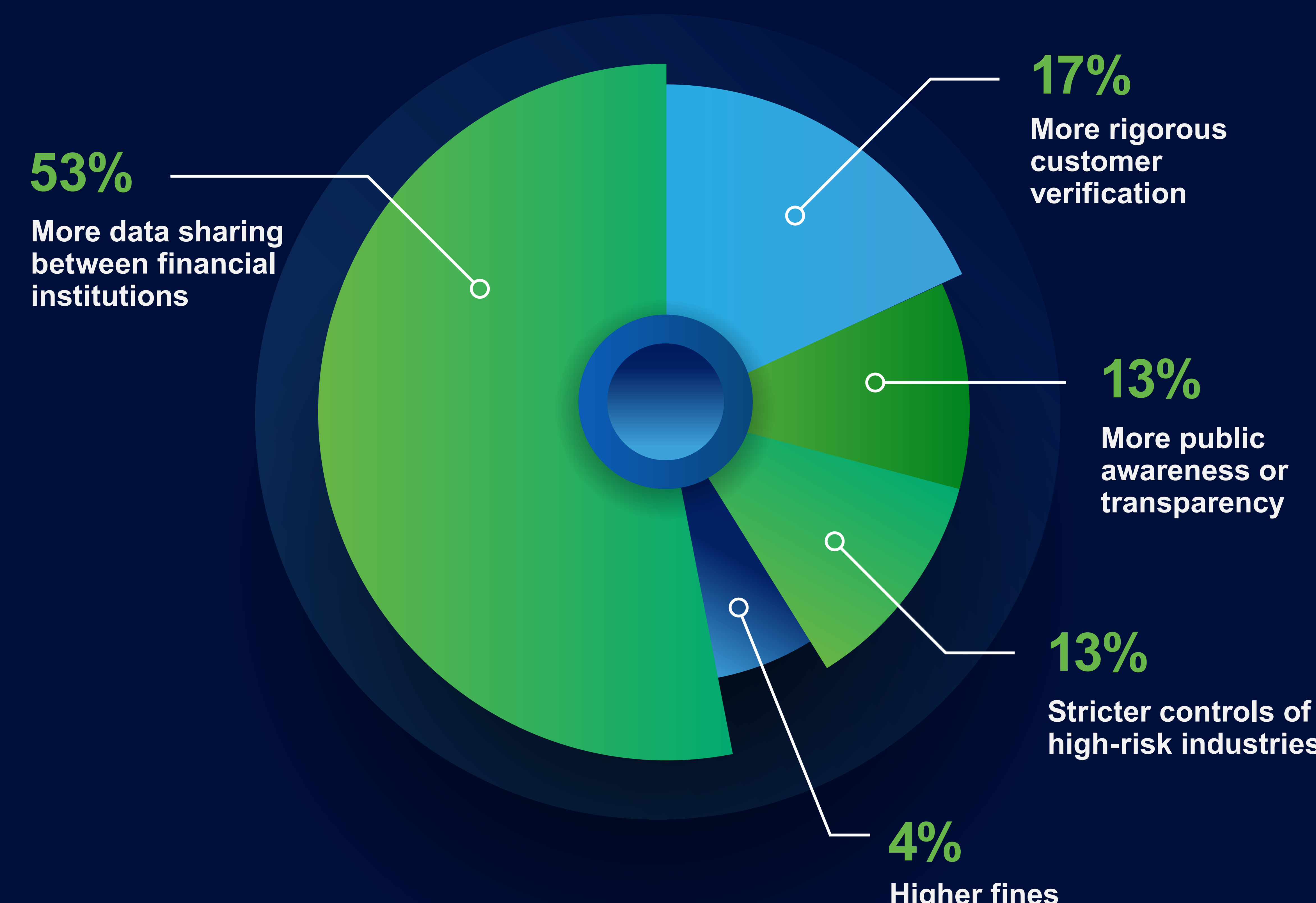
The following two categories are product and staffing. Advanced AML products reduce alert fatigue and help alleviate perennial staffing issues.



What market change needs to take place to reduce money laundering and associated crimes significantly?

Building strong public/private partnerships is increasingly important to reduce money laundering. Data sharing can make a significant impact on reducing money laundering and associated crimes.

Organizations often share fraud data but do not share money laundering data. Some regulators are looking to change this. In the US, 314(b) of the US Patriot Act allows institutions to share information without being liable for doing so. In the EU, the newly created AMLA ensures information-sharing among AML/CFT supervisors and any relevant non-AML/CFT authorities.



Europe deviates from the answer to these questions by placing the need for more public awareness and transparency in the top two responses. The release of the Panama Papers kicked off a privacy vs. secrecy debate, likely reflected here. The UK responded to the Panama Papers by creating an Ultimate Beneficial Owner (UBO) registry. Still, the UK's Crown Dependencies and Overseas Territories, which came under the most scrutiny, do not participate. Without all regions participating in UBO registries, it weakens their value.

More data sharing between FIs ranked number one across all regions, roles, and the financial services industry. The EU differed from the other regions on the second most important market change needed to reduce money laundering.

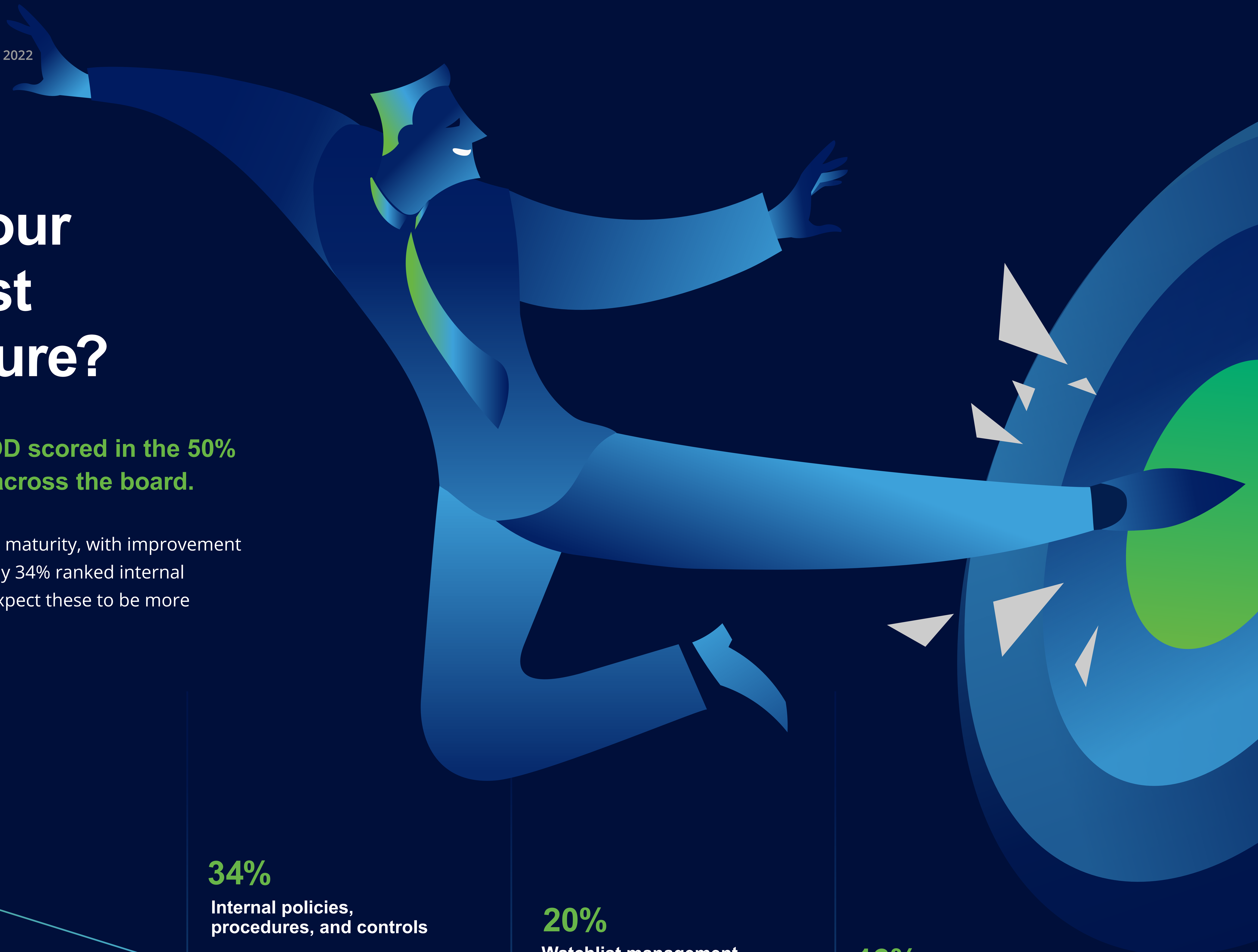
More rigorous customer verification

APAC, MEA, NORAM

More public awareness or transparency

EU

In which area is your AML program most successful or mature?

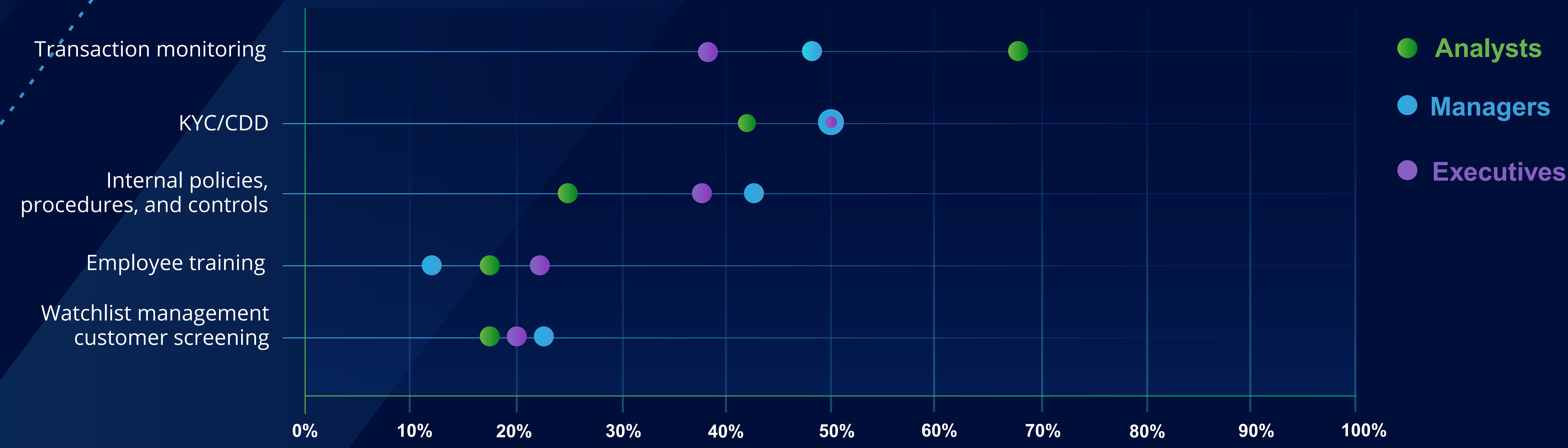


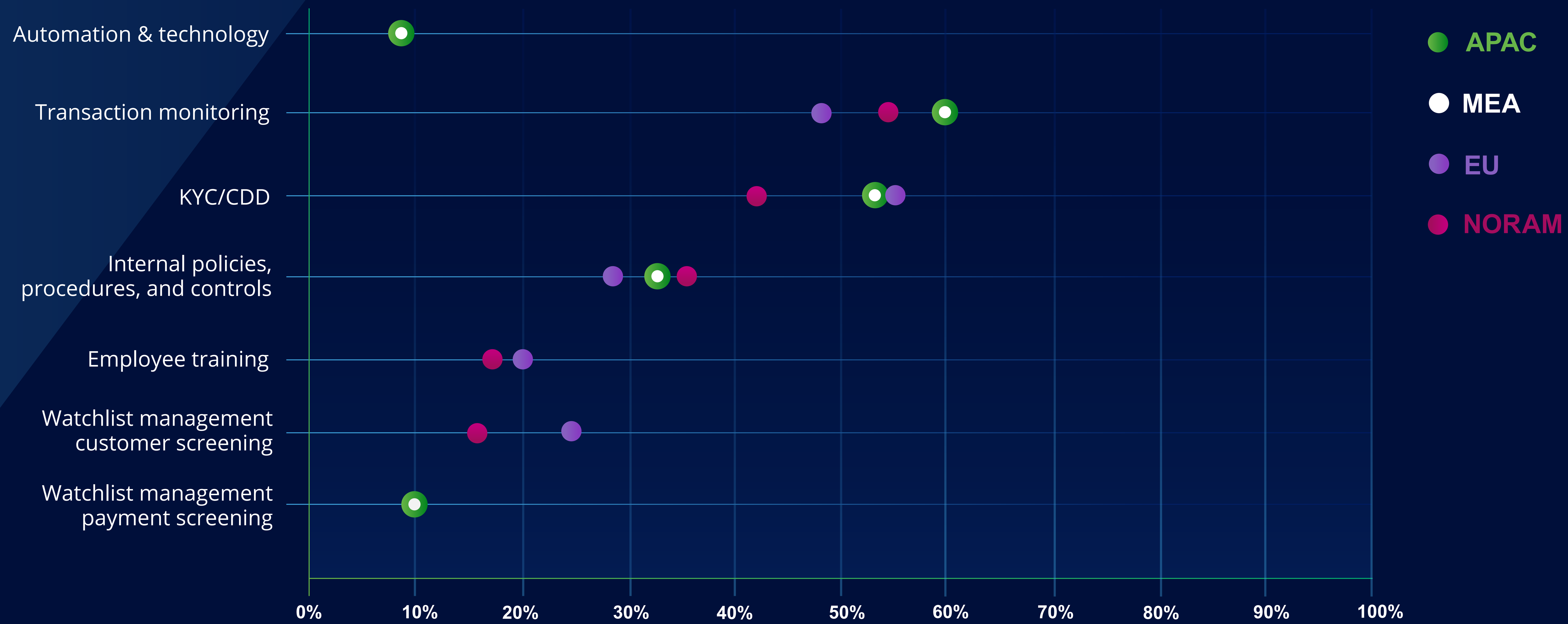
While transaction monitoring and KYC/CDD scored in the 50% range, the responses are relatively weak across the board.

This validates our assertion that AML programs lack some maturity, with improvement needed across critical aspects. Slightly alarming is that only 34% ranked internal policies, procedures, and controls as mature. We would expect these to be more mature.

Response by role:

in which areas are your AML program most successful or mature?

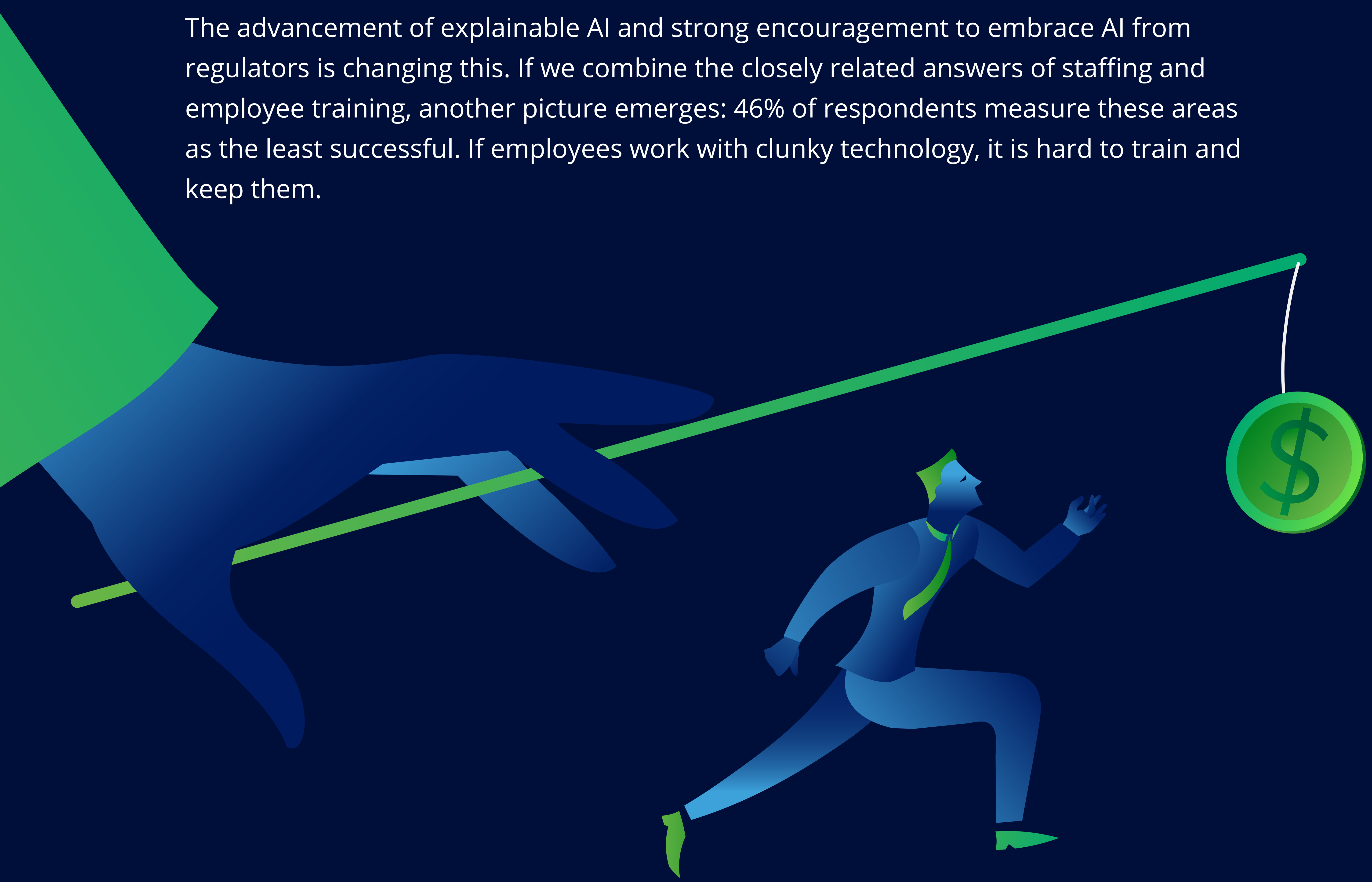




In which areas are your AML program least successful or still developing?

AML automation is still relatively new, and many AML program leaders have been reluctant to embrace it because they're unsure how to explain decisions to regulators.

The advancement of explainable AI and strong encouragement to embrace AI from regulators is changing this. If we combine the closely related answers of staffing and employee training, another picture emerges: 46% of respondents measure these areas as the least successful. If employees work with clunky technology, it is hard to train and keep them.



Customer screening and payment screening are also closely related. Taken together, 31% of respondents said this was an area that was still developing.

- 44% Automation/ technology
- 25% Transaction monitoring
- 21% Employee training
- 17% Internal policies, procedures, and controls
- 13% WLM payment screening
- 26% Independent testing
- 24% Staffing
- 18% WLM customer screening
- 13% KYC/CDD

All roles agreed automation was the least successful area of their AML programs, but Analysts and Managers ranked employee training and staffing as second and third, respectively. Executives did not list staffing or employee training in the top three, choosing independent testing and transaction monitoring instead.

This potentially highlights a "culture of compliance" gap within organizations. Staffing challenges are often linked with training.

While general AML training fulfills compliance requirements, it does not compare with training modeled on university courses. Additionally, organizations can do more to take advantage of front-line employees' knowledge of day-to-day operations and customer interactions, particularly in changing environments.

Analysts/Managers

1. Automation/technology
2. Employee training
3. Staffing

Executives

1. Automation/technology
2. Independent testing
3. Transaction monitoring

APAC

42%	Automation/technology
32%	Employee training
25%	Independent testing
20%	Watchlist management payment screening
20%	Transaction monitoring

MEA

60%	Transaction monitoring
54%	KYC/CDD
33%	Internal policies, procedures, and controls
10%	Watchlist management payment screening
9%	Automation/technology

EU

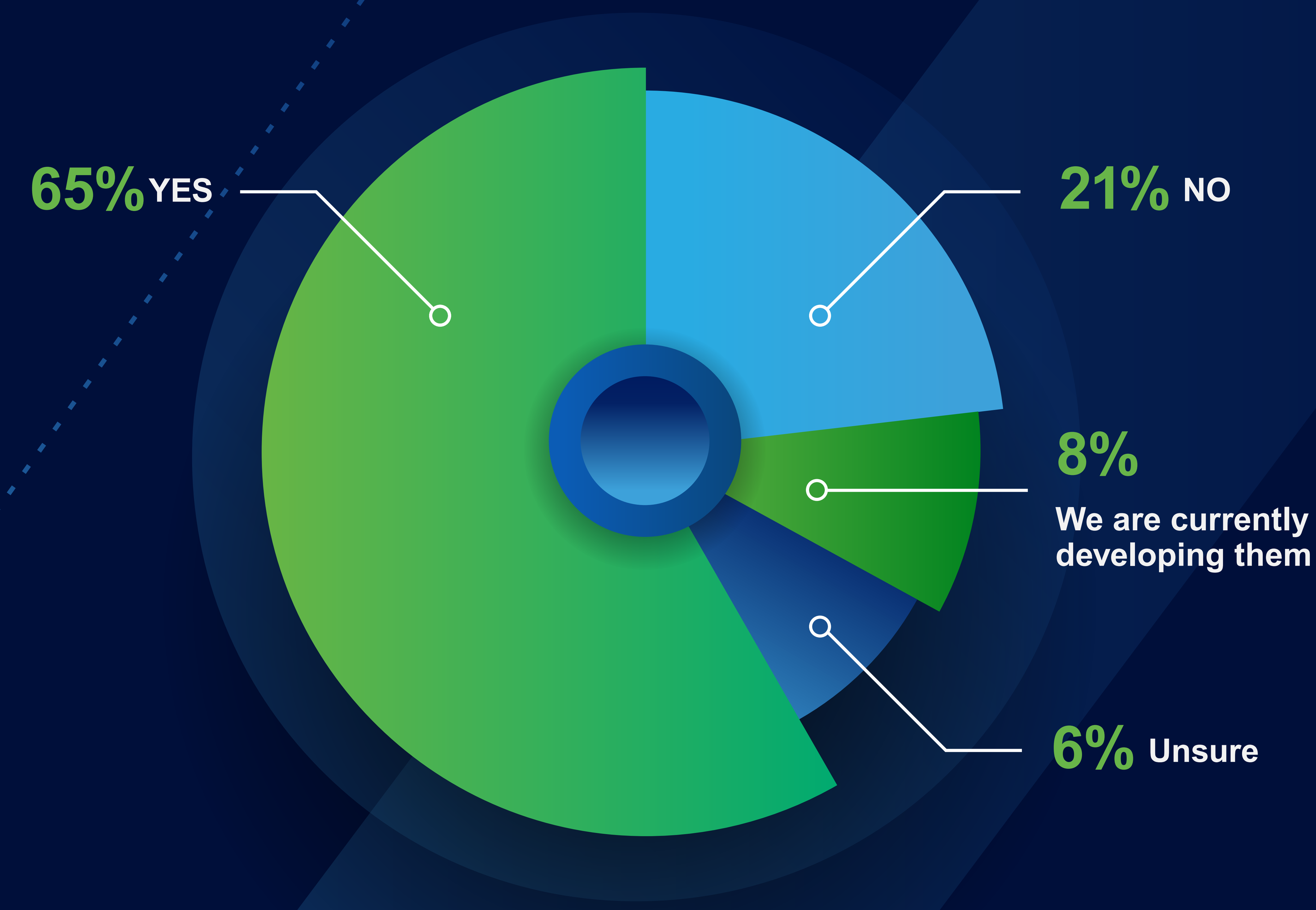
45%	Automation/technology
32%	Independent testing
31%	Transaction monitoring
23%	Staffing
18%	Employee training

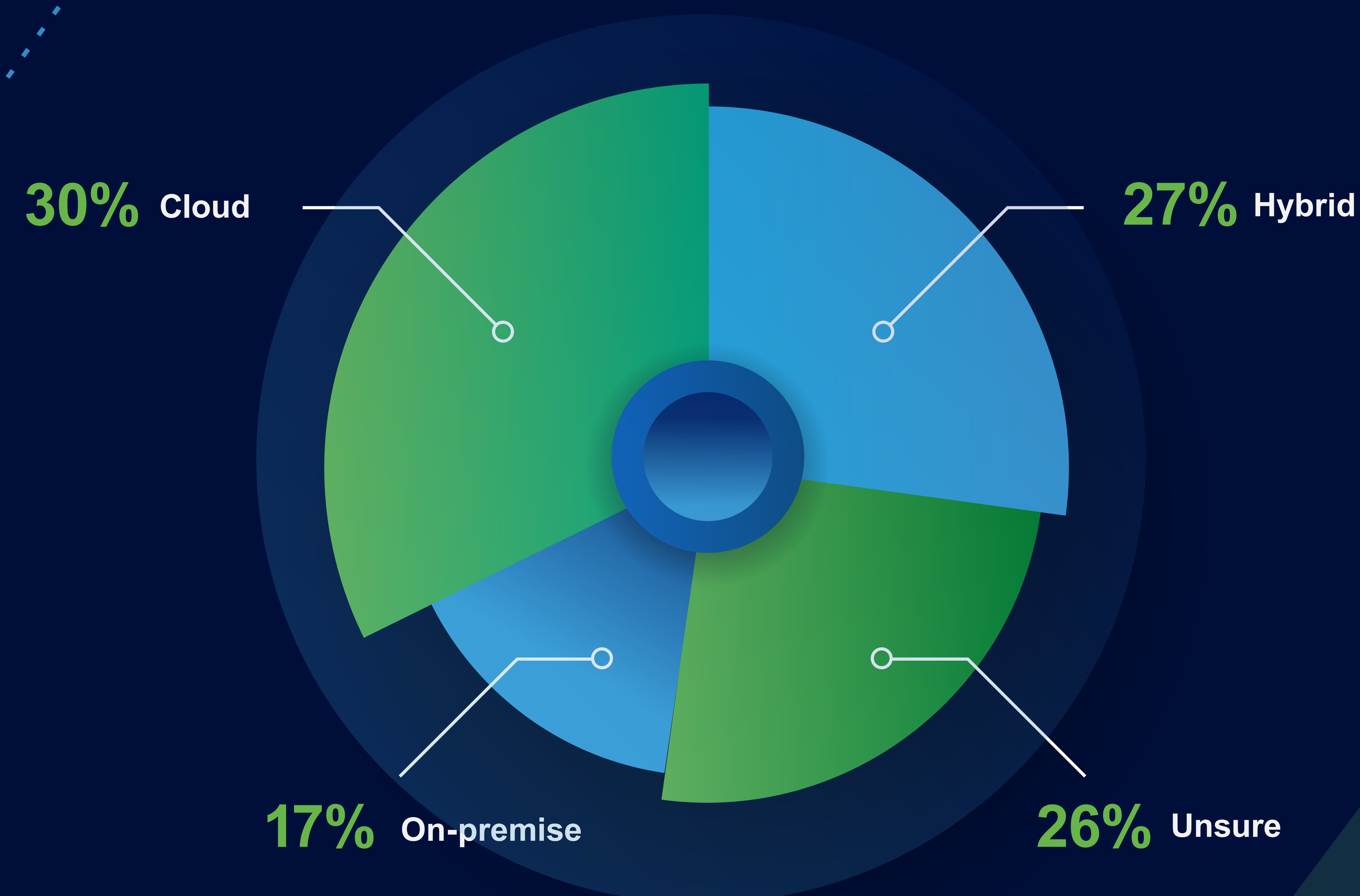
NORAM

41%	Automation/technology
30%	Staffing
24%	Independent testing
22%	Employee training
22%	Transaction monitoring

Do you have clearly defined policies that drive the sources and information to be collected by jurisdiction and customer type?

The response is the same across all roles, regions, and industries.





How is your AML platform hosted?

We see a strong preference for cloud or hybrid hosting: cloud hosting eliminates data volume issues and allows programs to test models and scale production quickly.

Do your fraud and AML teams share a single case manager?

Where there's money laundering, there's fraud. A unified case management system allows AML analysts to see previous fraud alerts on any customer or account. This additional evidence is helpful for alert investigation and filing suspicious activity reports (SARs).

Sharing a case manager across fraud and AML teams also creates operational efficiencies. The AML team can leverage the work already done by the fraud team, especially if it's a confirmed fraud, adding to the overall audit trail and providing explainable decisions.

To make a real impact on financial crime, we need 70-80% of teams to take a RiskOps approach and share a single case manager.

41% Yes

41% No

19% Unsure

From a regional perspective:

Yes, we share a case manager:

49% NORAM

45% EU

44% MEA

No, we do not share a case manager:

56% APAC

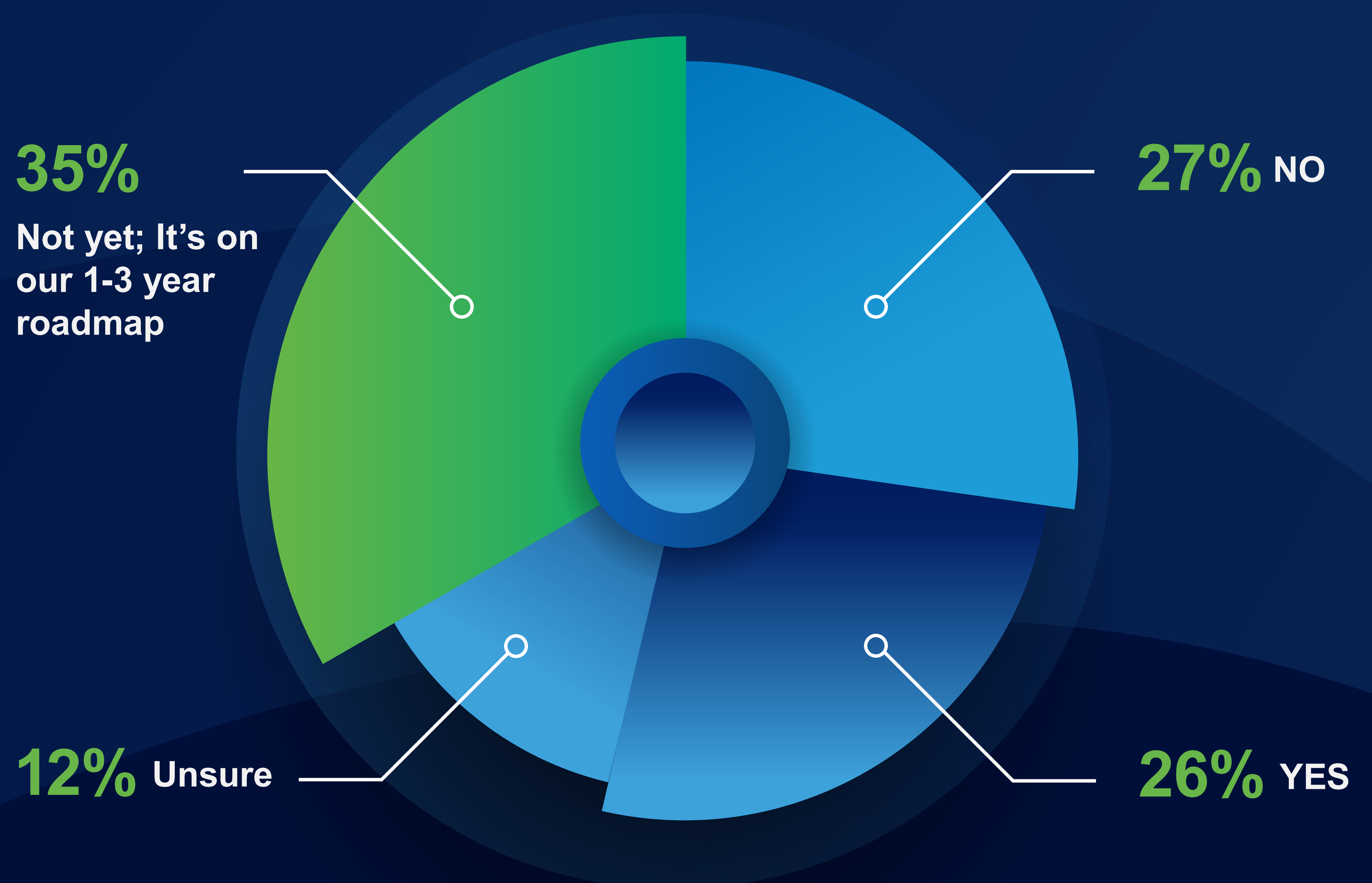
Broken down by role, there appears to be a perception gap between fraud and AML analysts and leadership teams (executives and managers) over whether teams share a single case manager (CM). A strong majority of analysts said they did, with 28% unsure. But just under half of executives and managers said they did.

One possible explanation for this gap is that the surveyed analysts work in either fraud or AML and may not know if a single CM is shared across the organization. Executives and managers have visibility across both systems.

Is your firm using technology to evaluate its crypto risk exposure?

Crypto exchanges, eMoney services, and other alternative payment platforms have gained significant ground in recent years but are still relatively new.

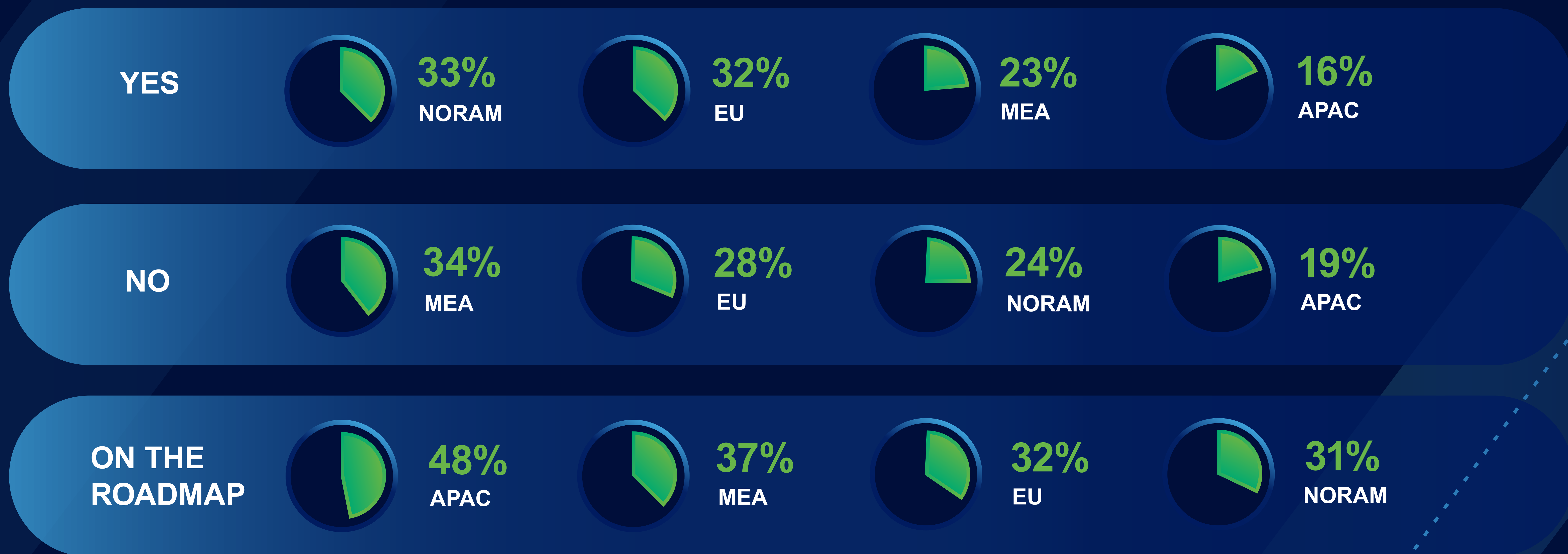
AML professionals are skeptical about these currencies and have taken a wait-and-see approach. However, this approach creates dissonance as cryptocurrency is a top pain point.



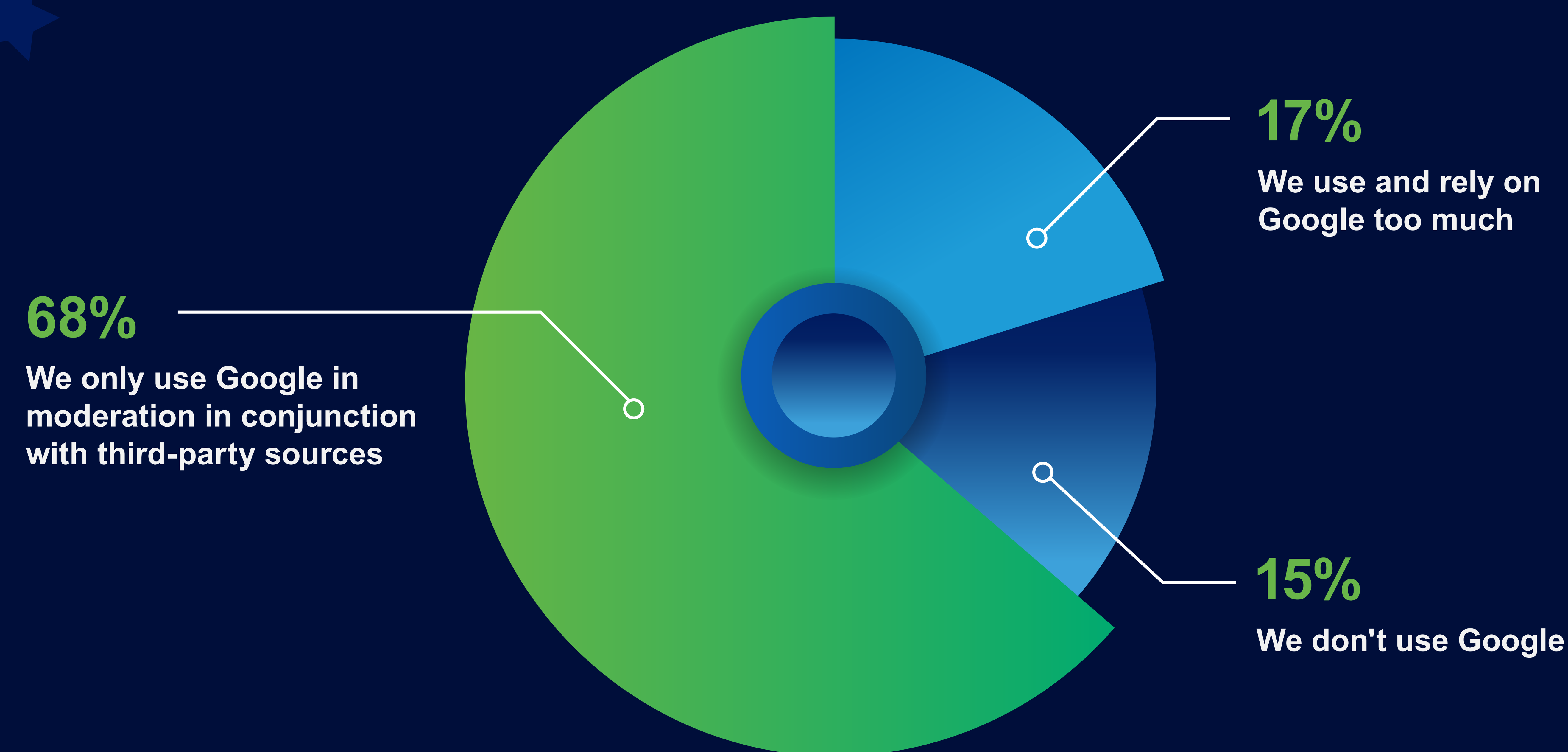
Reviewed by region, NORAM and the EU are leading the charge on crypto adoption, including the acquisition of licenses and regulation. While adoption in APAC appears to be lower, several nations in the region are adopting their own regulations at their own pace, with some moving faster than others.

The Monetary Authority of Singapore (MAS), for example, is not currently regulating crypto directly. However, MAS is applying existing laws and regulations to crypto exchanges focusing on money laundering and terrorist financing risks.

Regional Responses: Is your firm using technology to evaluate its crypto risk exposure?



Which statements match your current use of Google for due diligence/risk investigations?

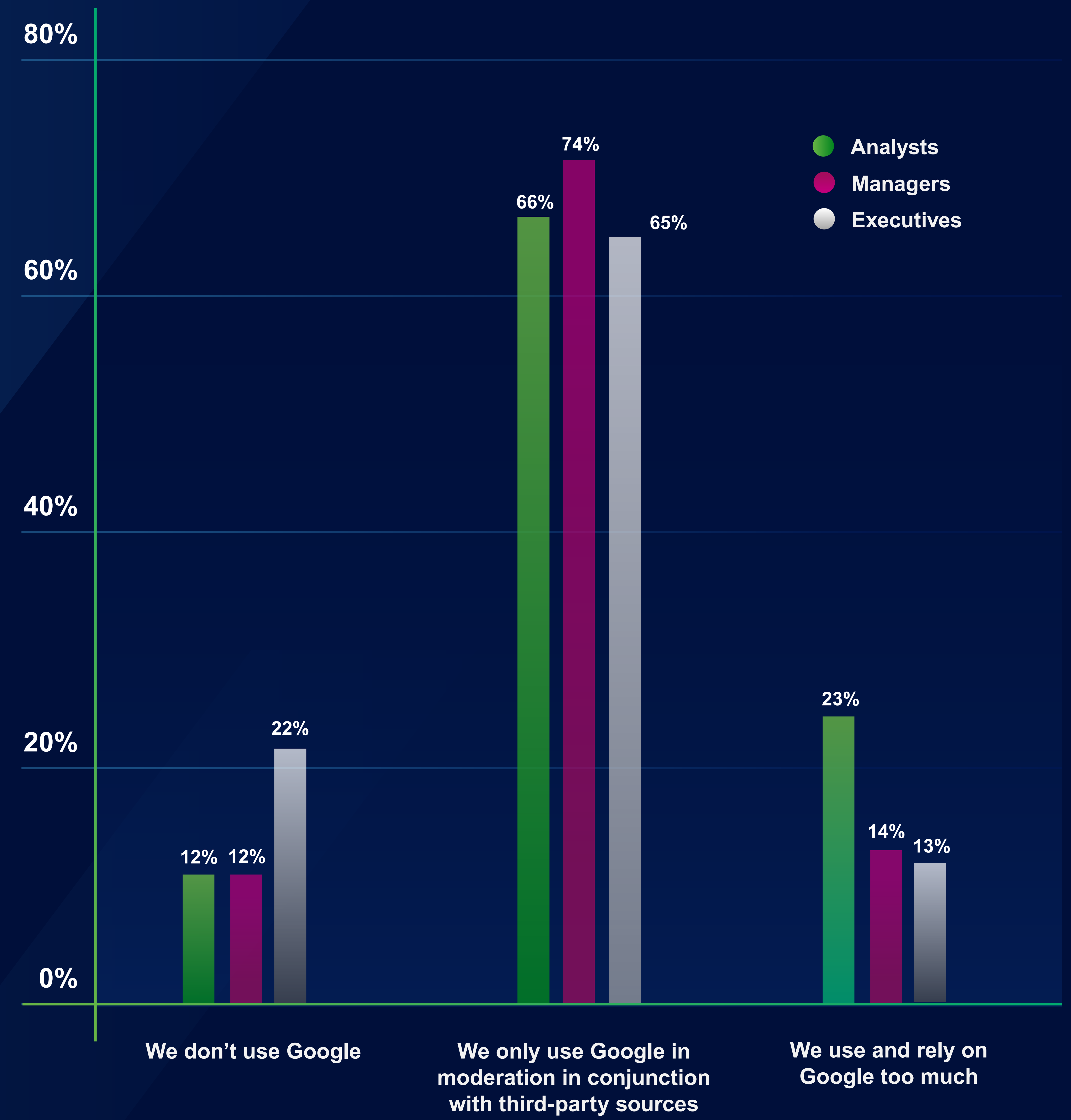


NORAM was the only region that followed the overall chart. All others chose "we don't use Google" as the second most common answer.

This is likely due to stricter AML policies in other regions. Policies dictate what sources and methods organizations utilize.

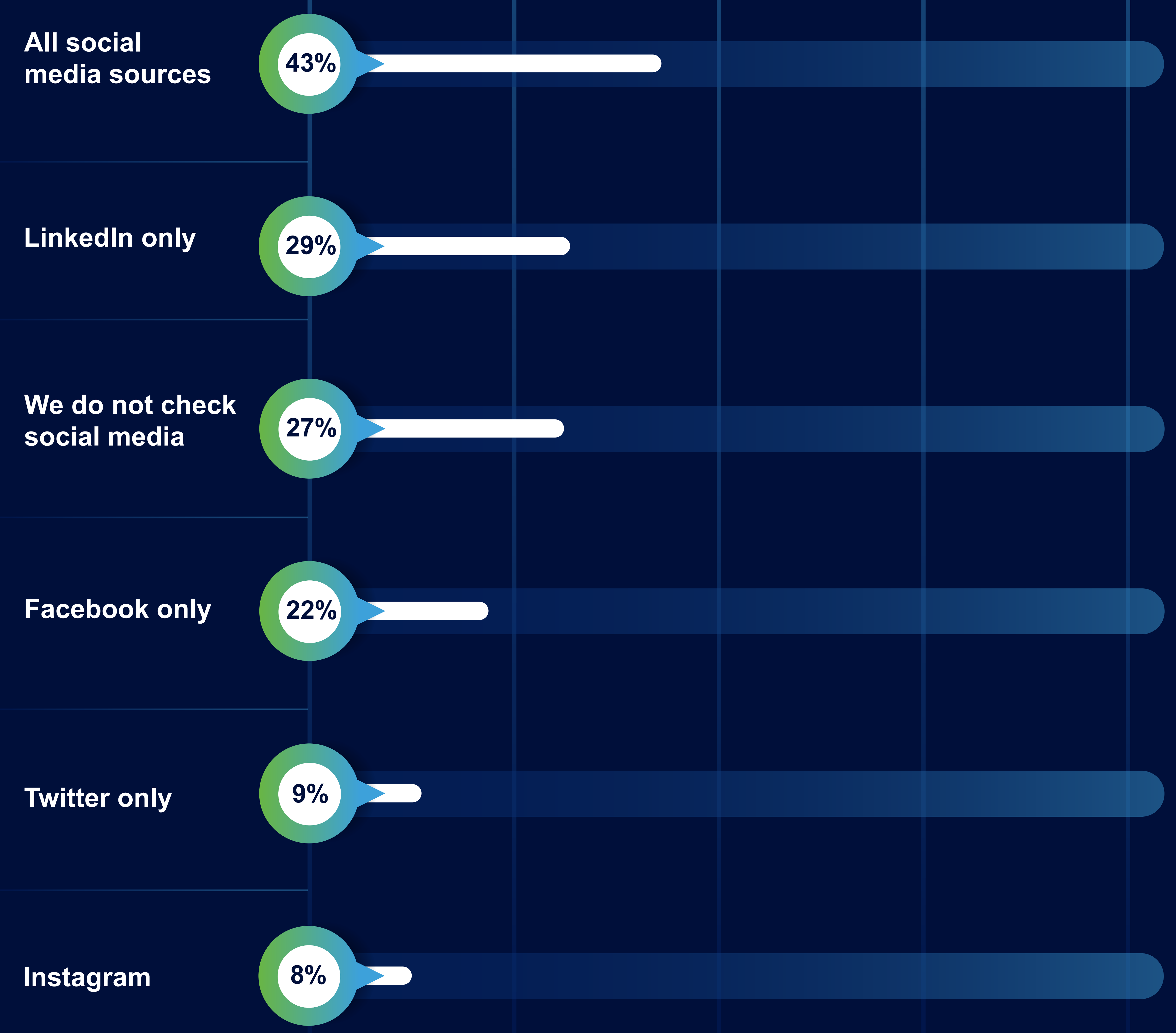
Performing adverse media checks with Google is tempting, but problematic. Does one draw the line at results from page one or results from page 20?

The time it takes for analysts to review Google search is an inefficient operational choice.



Which social media platforms do you review for due diligence/risk investigations?

Twenty-seven percent of organizations do not check social media, an astonishing revelation because social media is where people volunteer personal information and reveal their affiliations.



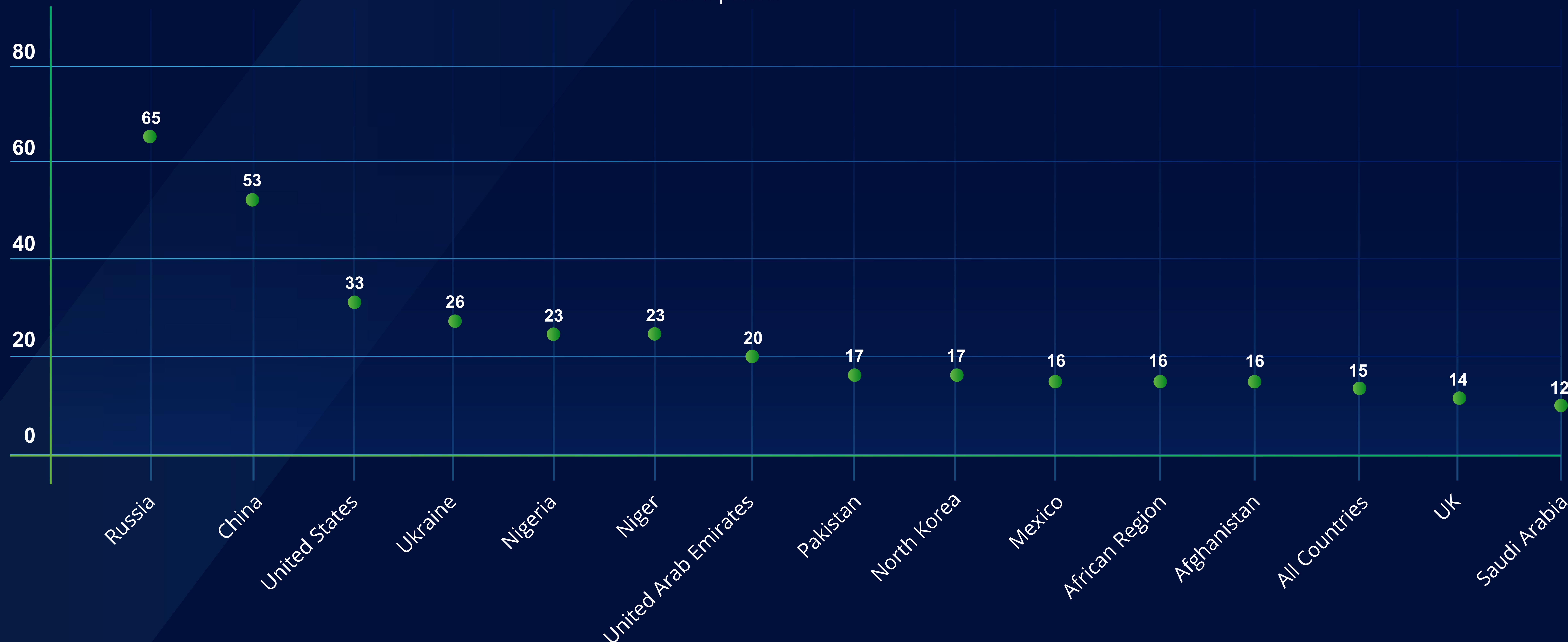
Write-in answers included Lexis, Bloomberg, and Dunn & Bradstreet, and several respondents said they only check social media if other sources of information fail.

What countries present the biggest money laundering risks?

Assessing a country's risk involves both subjective and objective data.

327 respondents shared 701 countries or regions they consider risky. Organizations consider politics, crime, and regulations in their risk decisioning. Unsurprisingly, Russia and China lead the list of the top 15 risky countries according to 52% of the respondents. By some accounts, powerful figures in Russia have over $1 trillion in “dark money” stashed overseas, while an estimated $141.2 billion is linked to money laundering in China at any given time.

Surprisingly, Mexico was the only region in Latin America to make the top 15 list, and the UK scored lower than expected.



How would you rate your company's ability to share and collectively maintain customer and counterparty data across your organization?

1-5 scale; 5 being excellent and 1 being poor

FIs have invested heavily in their data management capabilities and solutions. After all, having clean and single views of customer and counterparty data across the organization is a core tenant of knowing your customer and goes beyond just an AML risk-mitigation requirement. There is also the potential for this data to provide sales revenue intelligence.

Based on the overall score, there's a perception that firms have room for improvement to achieve "excellent" ratings.

3.50

APAC had the poorest self-ratings, while Europe ranked themselves the highest, but all were average.

3.53 EU

3.51 MEA

3.47 NORAM

3.44 APAC

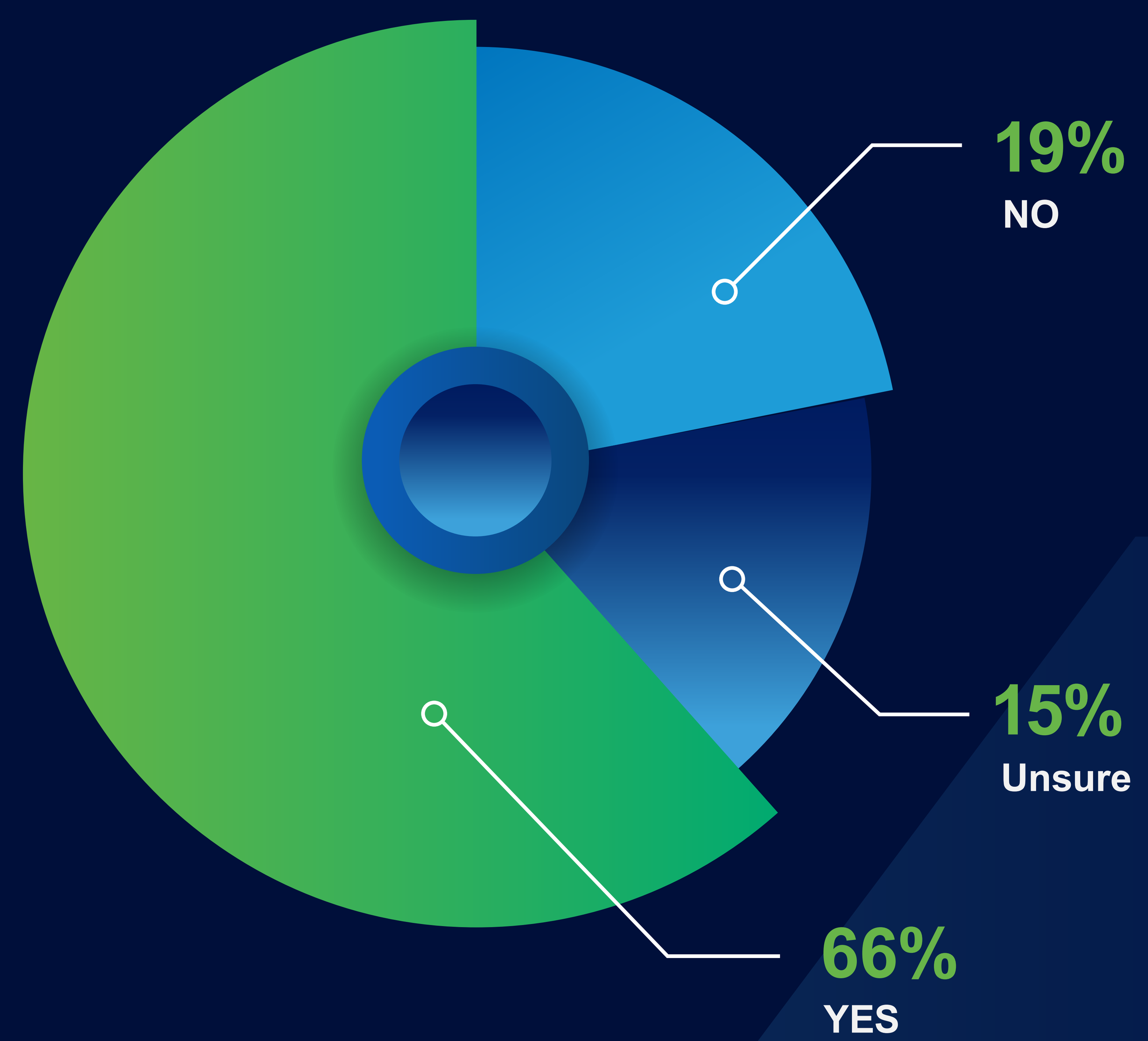
Analysts reported the highest percentage of poor (1) and excellent (5) ratings at 3.5% and 16.8%, respectively.

Does your firm share information and data across fraud and AML teams?

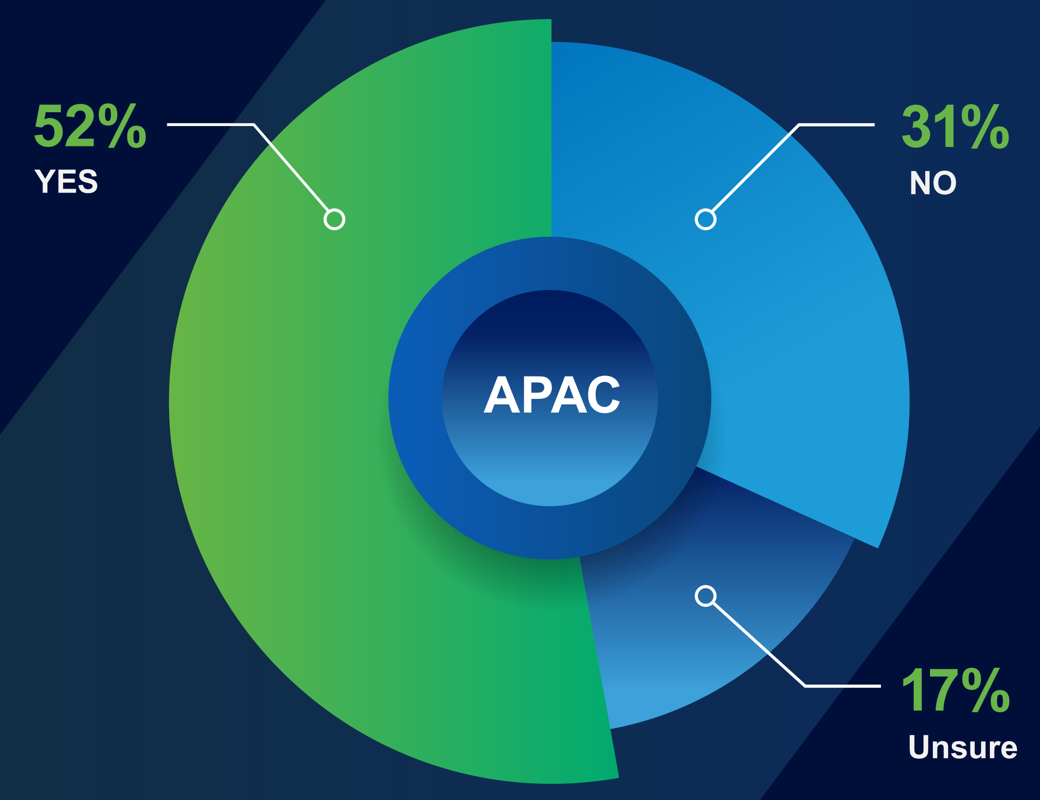
Overwhelmingly, fraud and AML teams share data. Or do they? When we look at this question across roles, we see a very different answer:

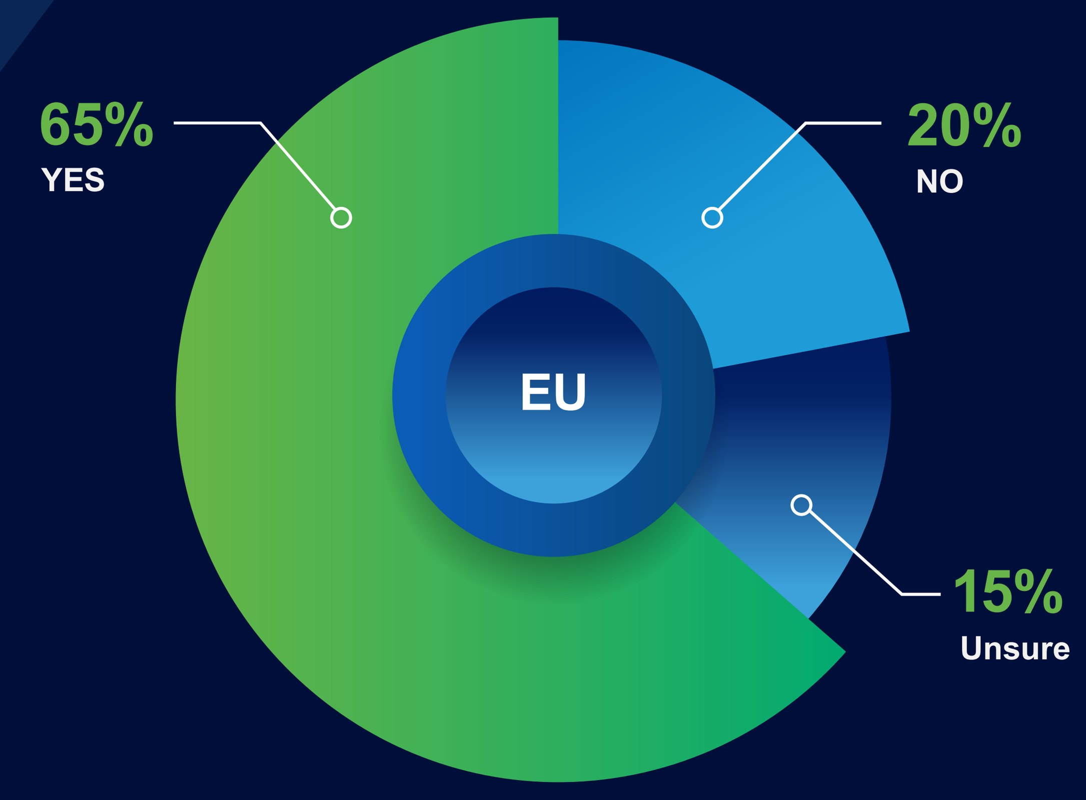
59% of analysts say data is not shared between fraud and AML teams, but 53% of managers say it is.

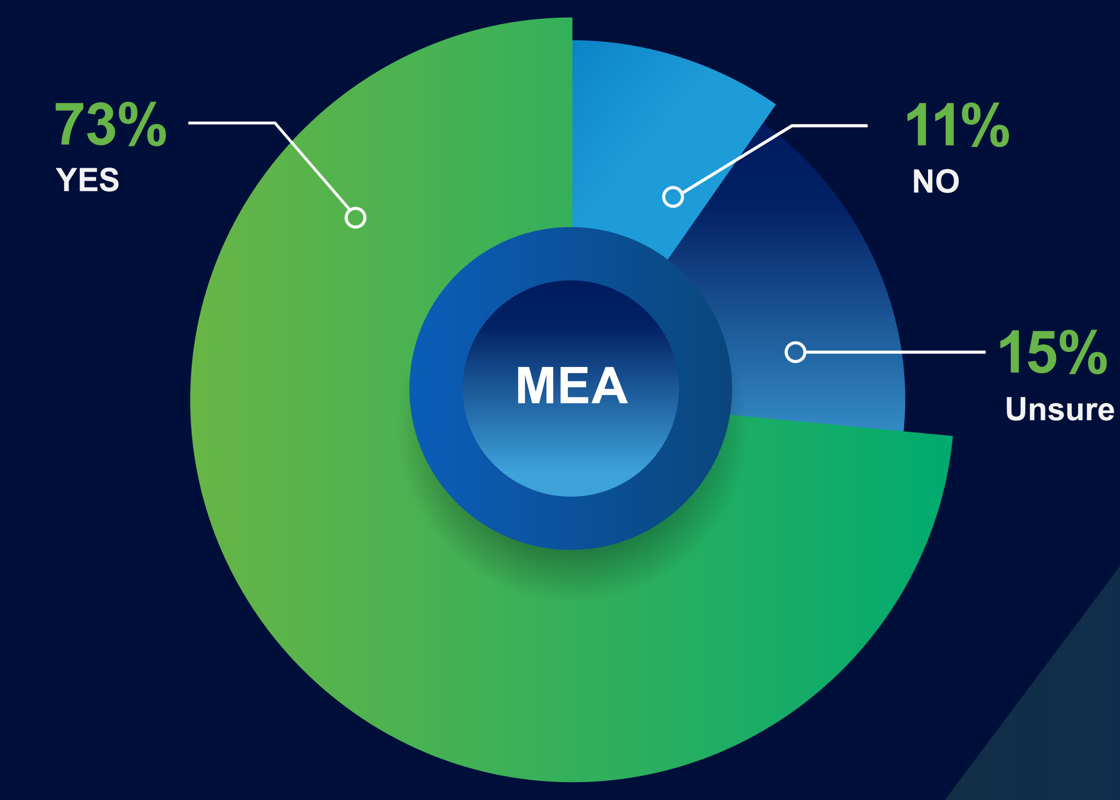
With the surge in money mules, it is essential that fraud and AML teams share data. Sharing data allows teams to discover money mules at a much earlier stage. Firms that adopt a RiskOps approach can detect and prevent criminal activity sooner.

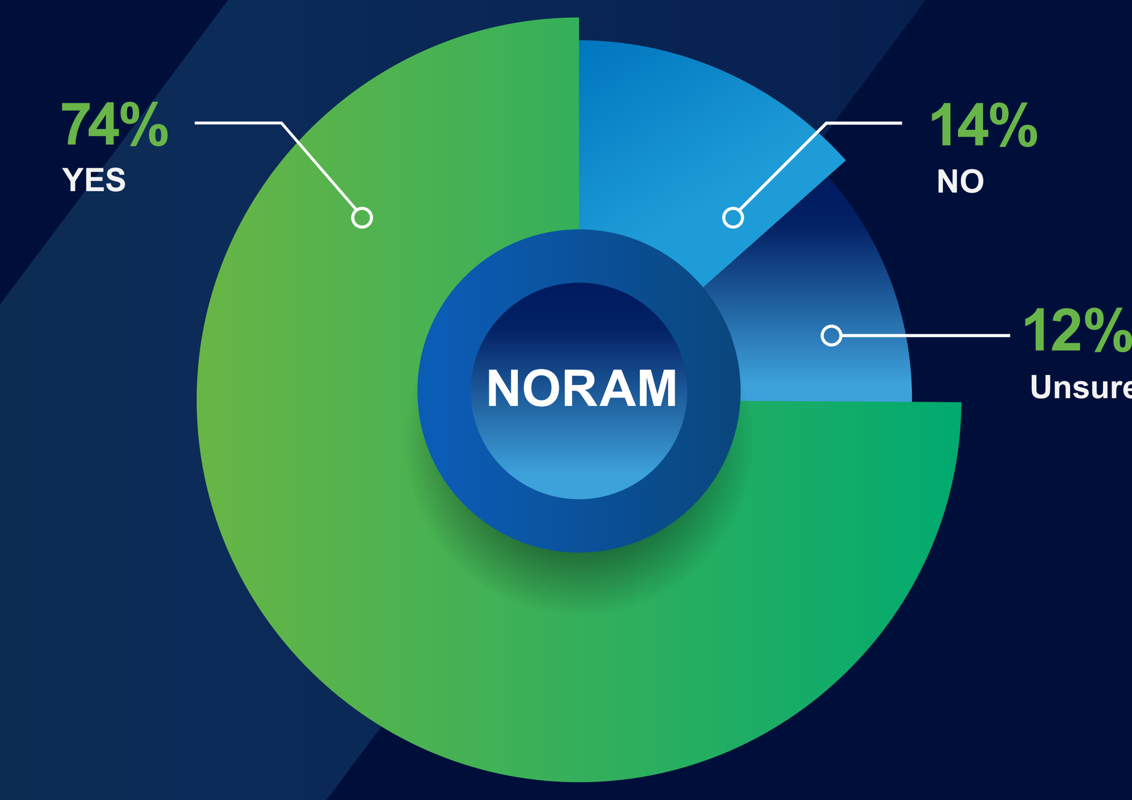


Organizations across all regions are shifting to a RiskOps approach. The APAC region reported a higher level of organizational silos. This is likely due to the large number of countries that make up this region, each with a wide variety of fraud and AML program maturity.

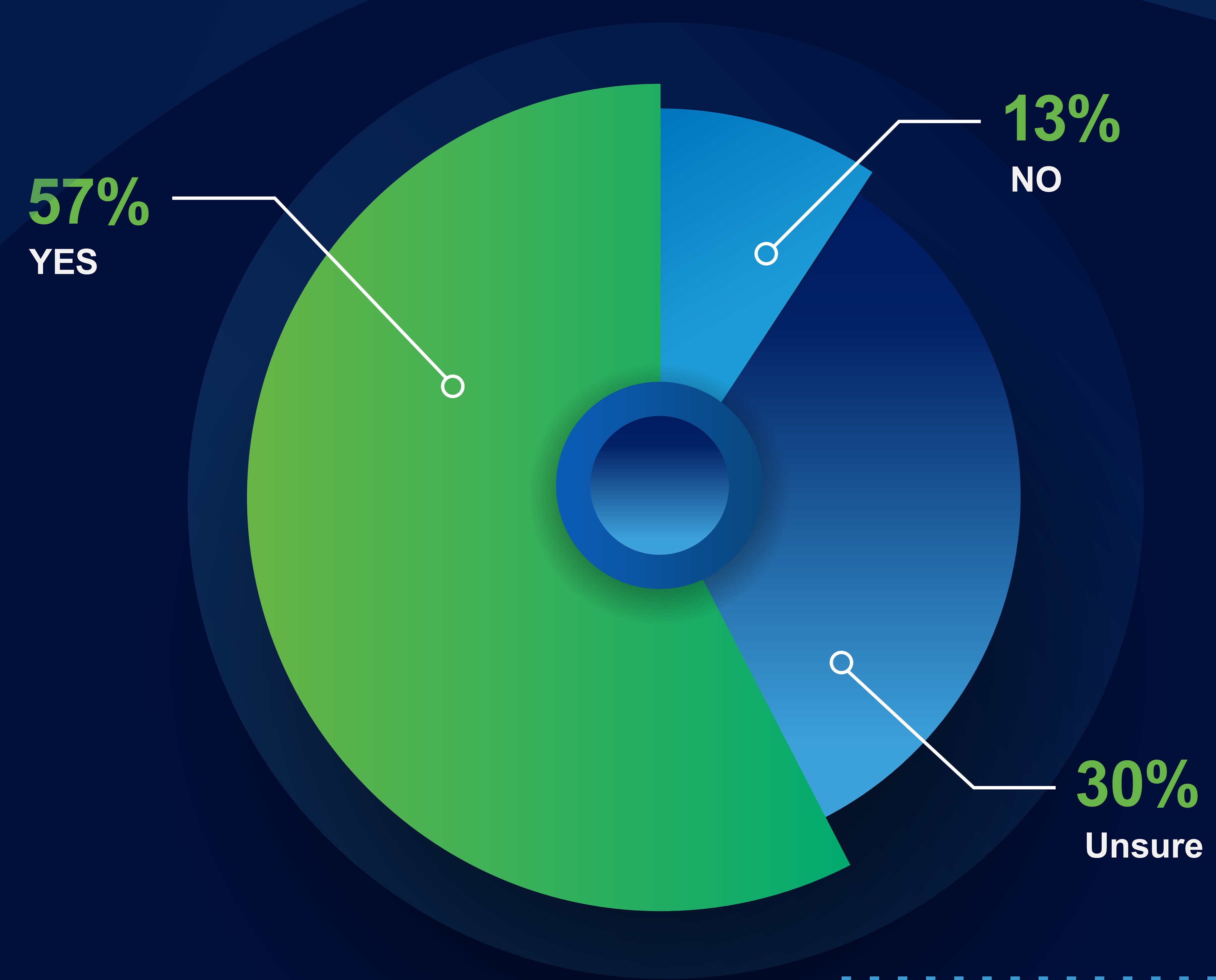








If your firm does not share information and data across fraud and AML teams, do you want them to?



Conclusion

In times of economic uncertainty, money launderers increasingly recruit money mules into their schemes. Most of these mules are unwittingly drawn in by fake job offers that promise quick payouts for little effort. Using multi-customer, cross-wallet payment activity to move funds between different accounts is an effective typology for avoiding detection and keeps mule schemes hidden.

Crypto exchanges are popular tools in mule schemes. Yet only 26% of respondents said they were investigating and evaluating their cryptocurrency risk exposure. This highlights a significant gap in AML compliance teams' priorities when addressing emerging risks. No wonder cryptocurrency is one of the top two pain points for AML professionals.

Cryptocurrency is not the only area where FIs aren't fully aligned on how to address their top AML priorities. For example, 61% of respondents believe enhanced automation that collates data from multiple vendors will be a top AML/KYC trend over the next five years. Half of respondents said using a RiskOps approach for data sharing between FIs will bolster anti-money laundering efforts. However, most respondents named implementing pKYC and reducing false positives as their main goals for 2022. Creating a single customer view that combines all data points lagged behind these initiatives.

Internally, some team members aren’t aligned on whether or not they take a RiskOps approach to share data. For example, 59% of fraud and AML analysts say they do not allow data sharing between fraud and AML teams. At the same time, 53% of managers said they do. This highlights a disconnect over how AML compliance teams can tackle the issue of data sharing if management doesn’t see the issue in the same light.

Respondents named increased regulatory expectations as the most challenging AML compliance issue and the top market challenge AML teams face in the next two years, followed closely by crypto and blockchain. Developments like Russian sanctions, 6AMLD, and the FATF's rules only add to their challenges. Though it lagged behind these two categories, staffing challenges were another top concern for respondents. This highlights the industry's challenge in addressing the "silent issue" of AML compliance staffing.

Usage of social media - or in some cases, the non-usage of social media - is another silent issue facing the industry. Roughly one-quarter of respondents said they don’t use social media to review a potential client’s background - despite this being a voluntary source of information.

AML compliance professionals frequently use yesterday's technology and tools to address tomorrow's money laundering challenges. Making more innovative usage of data, enabling smoother data sharing between teams, and doing more to address the challenges of cryptocurrency are all top concerns for AML compliance teams to demonstrate their effectiveness and root out money mule activities.

Many AML compliance teams may feel like they are constantly catching up to address the latest financial crime patterns. Taking a RiskOps approach to money mules and other money laundering activities provides a path forward for AML compliance and fraud prevention functions.

AML Survey Methodology

We received 636 responses (331) as not everyone answered each question. These represent 77 companies around the world. Beyond basic demographic information, we asked a total of 19 questions and analyzed the responses through a system of four categories:

Overall

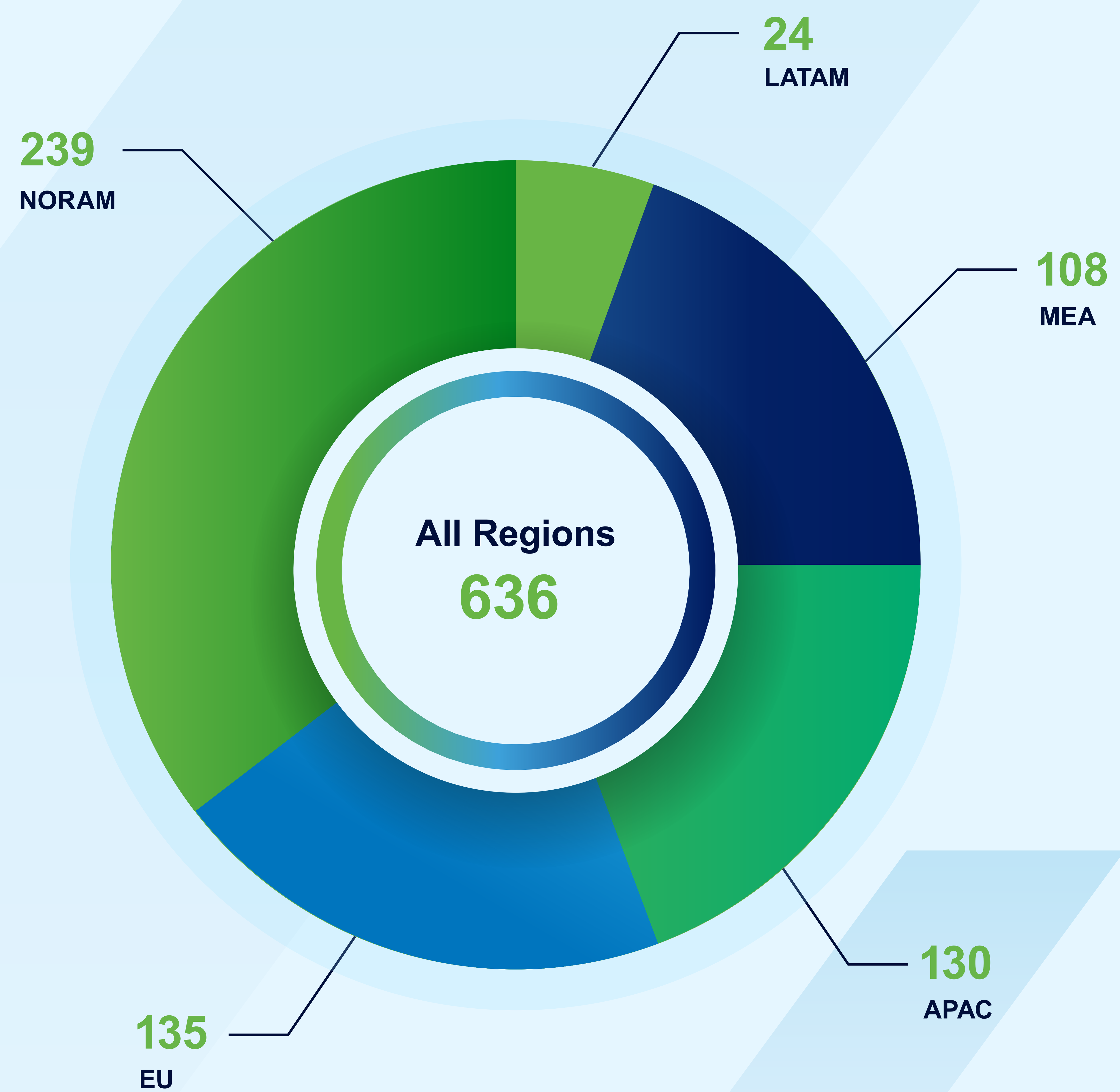
This is the total response regardless of region, role, or industry. If responses from roles or regions differed from the overall results, and there were at least 10% of respondents from a particular role or region for that question, we reported those findings as well.

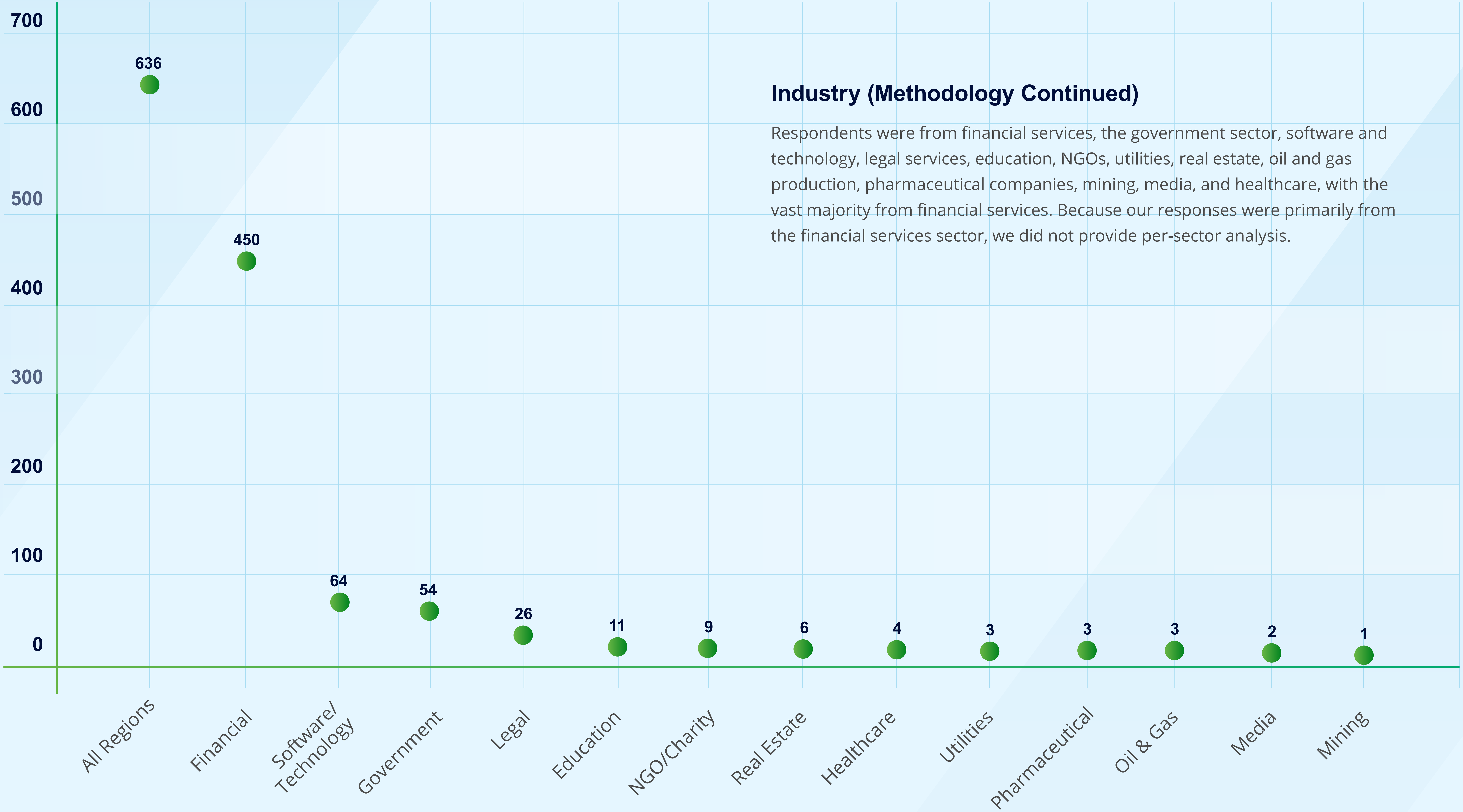
Role

Respondents were categorized as analysts, managers, or executives based on their titles.

Region

Regions were categorized as Asia Pacific (APAC), Europe (EU), the Middle East and Africa (MEA), North America (NORAM), and Latin America (LATAM). Note that while we did receive responses from the LATAM region, we did not receive enough responses to allow us to produce a statistically significant analysis. Here is a general breakdown of responses by region. However, not all respondents answered all the questions.





Industry (Methodology Continued)

Respondents were from financial services, the government sector, software and technology, legal services, education, NGOs, utilities, real estate, oil and gas production, pharmaceutical companies, mining, media, and healthcare, with the vast majority from financial services. Because our responses were primarily from the financial services sector, we did not provide per-sector analysis.

feedzai

Anti-Money Laundering Suite

Transaction Monitoring | Customer Screening | Payment Screening | KYC/CDD

Learn how Feedzai's Anti-Money Laundering Suite provides end-to-end, unified, and scalable solutions to identify money laundering and reveal unknowns hidden in terabytes of data. Our off-the-shelf risk strategies provide faster time to value. Schedule a demo today. https://feedzai.com/contact-us/request-a-demo/

Feedzai.com | info@feedzai.com | sales@feedzai.com