KROLL

# 2025 Financial Crime Report

## AI and Geopolitical Uncertainty Fuel a New Wave of Financial Crime

# Table of Contents

# Contributors


**Thomas Bock**
Managing Director and
Head of U.S. Financial Crime
Advisory Practice
+1 212 277 0123
thomas.bock@kroll.com

**Howard Cooper**
Managing Director and Global Co-Head
of Financial Investigations Practice
+44 20 7029 5137
hcooper@kroll.com

**Oliver Stern**
Managing Director
Investigations, Diligence and Compliance
+44 20 7029 5157
oliver.stern@kroll.com

**John deCraen**
Associate Managing Director
Cyber and Data Resilience
+1 973 775 8303
john.decraen@kroll.com

**Richard Taylor**
Director
Financial Services Compliance
and Regulation
+44 20 7089 0928
richard.taylor@kroll.com

**Tarun Bhatia**
Regional Managing Director
and Co-Head of APAC
Investigations, Diligence and Compliance
+91 22 6294 8166
tarun.bhatia@kroll.com

**Laura Walster**
Senior Vice President
Financial Services Compliance and Regulation
+44 20 7029 5009
laura.walster@kroll.com

**David Lewis**
Managing Director
Investigations, Diligence and Compliance
+33 1 40 06 40 35
dlewis@kroll.com

**Dan Rice**
Associate Managing Director
Cyber and Data Resilience
+1 713 237 5308
dan.rice@kroll.com

**Tiernan Connolly**
Managing Director
Cyber and Data Resilience
+353 1 428 3125
tiernan.connolly@kroll.com

**Mark Turner**
Managing Director
Financial Services Compliance
and Regulation
+44  20 7089 0834
mark.turner@kroll.com

**Hannah Rossiter**
Managing Director
Financial Services Compliance
and Regulation
+97 144 496 733
hannah.rossiter@kroll.com

**Amanda Wood**
Managing Director
Investigations, Diligence and Compliance
+61 282 867 223
amanda.wood@kroll.com

KROLL

# Executive Summary

Authors

David Lewis

Thomas Bock

**From pivotal elections to advances in artificial intelligence (AI) to heightened geopolitical tensions, the events of the past year have only amplified the challenges of fighting financial crime. Our latest research—based on a survey of over 600 executives across the globe—can help leaders prepare for what's next.**

With AI-powered cybercrime disrupting businesses across industries and regulators imposing billion-dollar penalties for compliance failures, more than 70% of executives expect financial crime risk to increase in 2025—compared to 67% in 2023—yet only 23% believe their organization's compliance program is "very effective" in combating it.

These are among the key takeaways from Kroll's 2025 Financial Crime Report, which surveyed over 600 business leaders in the U.S., the UK, Europe, Asia Pacific, the Middle East and Africa. Respondents included CEOs, chief compliance officers, general counsel, and chief risk officers from leading financial services, accounting, insurance and legal services firms.

In addition to assessing financial crime expectations, concerns and readiness for the year ahead, the report examines how AI can fight—or enable—illicit activity and captures current sentiment around geopolitical threats, evolving regulations, supply chain risks and more.

### A Fast-Changing Financial Crime Landscape

In the coming months, new leadership across major economies could reshape financial crime regulatory and enforcement activity—with potentially significant consequences for how governments handle economic sanctions and anti-money laundering (AML) rules. These shifts come as the continued expansion of such requirements beyond the financial services sector deepens compliance pressures on regulated "gatekeeper" industries, from accountancy to legal services to gaming.

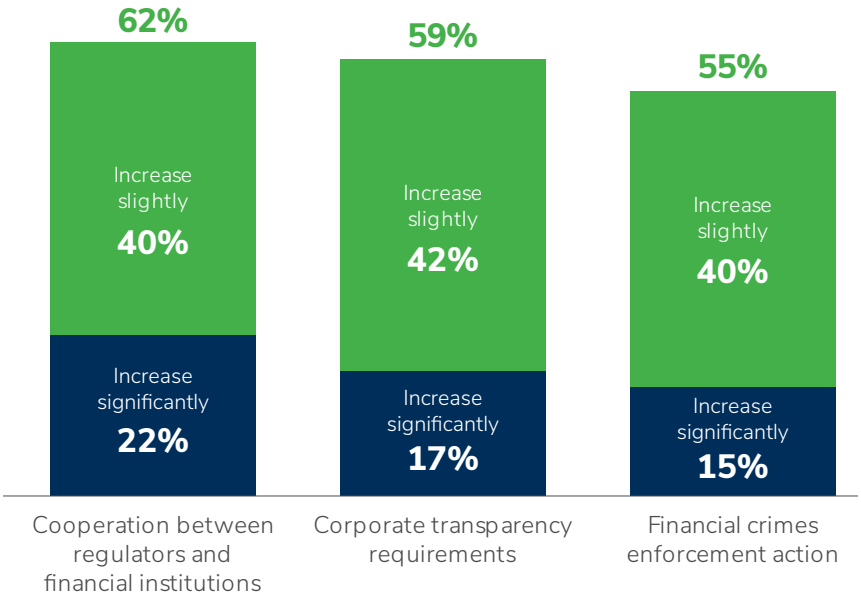
At the same time, swift advances in technology are deepening financial crime risk as organizations race to get ahead of bad actors. Cyberattacks and the increased use of AI by cybercriminals are the top two reasons why respondents expect financial crimes to increase in 2025. Respondents cite rapidly evolving technologies as the top hurdle causing governments to lose ground in the fight against financial crime.

Companies are also ramping up efforts to account for risk around digital currencies as cryptocurrency moves from the dark web to Main Street. Nearly 3 in 10 (29%) respondents accept, recognize or transact in crypto, and roughly another third (32%) are considering doing so—even as 59% of respondents say the financial crime threat it poses is a moderate or significant concern for their organization.

On the other hand, technology is an increasingly critical tool for fighting illicit economic activity. Fifty-seven percent of respondents believe AI will benefit their financial crime compliance programs, and nearly half expect to invest in both AI solutions and non-AI technology as part of their internal steps to tackle the expected increase in such risks.

Respondents are concerned about what may be on the regulatory horizon as well. Sixty-two percent expect cooperation between regulators and financial institutions to increase in the next 12 months, with similar forecasts for corporate transparency requirements and financial crimes enforcement action.

**Please indicate the extent to which you believe the following may change over the next 12 months:**




Meanwhile, persistent conflicts in Ukraine and the Middle East highlight the complexity of sanctions compliance, while escalating tensions between key economic powers fuel cyberattacks on private businesses and individuals. However, only 39% of respondents are “very confident” in their own financial crime compliance program’s sanction screening capabilities, and just a third say their programs are very prepared to address geopolitical issues over the next 12 months.

More broadly, our research revealed gaps in technology implementation, governance and sectoral readiness. This could pose significant problems for some industries in 2025, with our data showing real estate and legal services lagging behind accountancy, financial services, and insurance on some key aspects of financial crime preparedness.

### Preparing for What’s Ahead

There’s room for optimism, too. Seventy-nine percent of respondents expect their organization’s compliance function to take on more responsibility—and 8 in 10 respondents also say their organization is meaningfully committed to a culture of integrity and senior management supports the compliance function.

A significant percentage of respondents are taking steps to mitigate financial crime in 2025, whether they are investing in technology, increasing their cybersecurity budget (47%), assessing risk more frequently (41%), or implementing additional controls (39%).

In the following report, we’ll take a closer look at what our research reveals and provide actionable guidance to help leaders navigate the changes across today’s increasingly complex financial crime landscape.

# Methodology

The online survey was conducted in September and October of 2024. The 600+ respondents included CEOs, chief compliance officers, general counsel, chief risk officers and other financial crime compliance professionals. Half work in the financial services industry and the remainder are from other regulated industries, including accountancy, insurance, real estate, and legal services.

The survey also represents executives from key economic regions and financial hubs: the U.S. and UK, Western Europe (France, Germany, Ireland, Italy, Spain and Switzerland), Scandinavia (Norway and Sweden), Asia Pacific (Australia, India and Japan), Hong Kong, Singapore and the Middle East/Africa (United Arab Emirates and South Africa), as well as offshore financial centers—the British Virgin Islands, Cayman Islands and Jersey.

Survey responses were anonymous, and data was analyzed in the aggregate. Due to rounding and select multiple questions, data may not add up to 100%.

| Region | Country/Territory | Total |
|---|---|---|
| Asia Pacific | Australia | 75 |
| Asia Pacific | India | |
| Asia Pacific | Japan | |
| BVI, Cayman, Jersey | British Virgin Islands | 50 |
| BVI, Cayman, Jersey | Cayman Islands | |
| BVI, Cayman, Jersey | Jersey | |
| Hong Kong | Hong Kong | 50 |
| Middle East and Africa | South Africa | 75 |
| Middle East and Africa | UAE | |
| Scandinavia | Norway | 50 |
| Scandinavia | Sweden | |
| Singapore | Singapore | 50 |
| United Kingdom | United Kingdom | 50 |
| United States | United States | 50 |
| Western Europe | France | 175 |
| Western Europe | Germany | |
| Western Europe | Ireland | |
| Western Europe | Italy | |
| Western Europe | Spain | |
| Western Europe | Switzerland | |
| | | **625** |

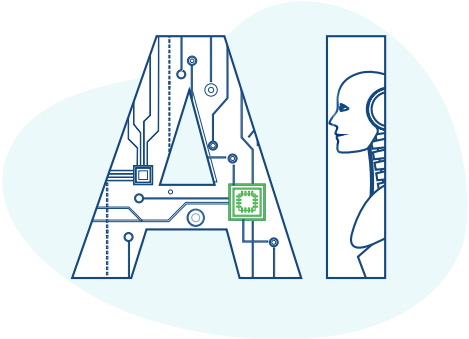
# Key Findings


**71% of respondents expect financial crime risks to increase in 2025—yet only 23% believe their organization's compliance program is "very effective". Potential reasons for ineffectiveness include:**

- **Lack of technology and investment.** Only 30% strongly agree their organization's financial crime compliance program is sufficient in these respects.
- **Weak governance.** Just 29% strongly agree that their organization has a robust governance infrastructure for overseeing financial crime.

**Cybersecurity (68%) and the increased use of AI by criminals (61%) are two of the leading catalysts for risk exposure in the coming year —with other factors including:**

| | |
|---|---|
| **38%** Increased incidence of predicate crimes | **34%** Financial pressure on individuals |
| **30%** Political instability | **30%** Geopolitical risk |

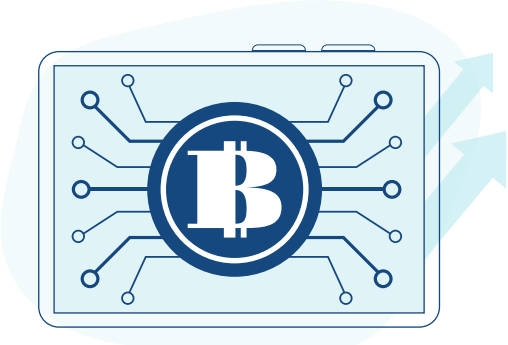


**As adoption of AI and machine learning advances, only 20% of respondents now exploring these tools see a "very positive impact" on their financial crime compliance frameworks—down from 37% in 2023.**

- Fifty-seven percent believe AI developments will benefit their financial crime compliance programs, while 49% agree AI poses a significant risk to compliance.

**Fifty-nine percent say the financial crime threat posed by cryptocurrencies is a moderate to significant concern in the coming year.**

- Thirty-one percent say their organization's financial crime compliance program caters to risks associated with cryptocurrencies; 23% say their program does not currently do so but there are plans to do so in the future.



**Only one-third of respondents say their financial crime compliance programs are "very prepared" to address geopolitical issues over the next 12 months, with the evolving sanctions landscape as one likely driver:**

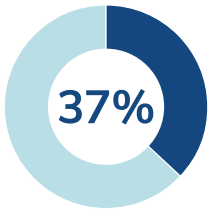
- Fewer than 4 in 10 respondents have high confidence in their program's sanctions screening capabilities.

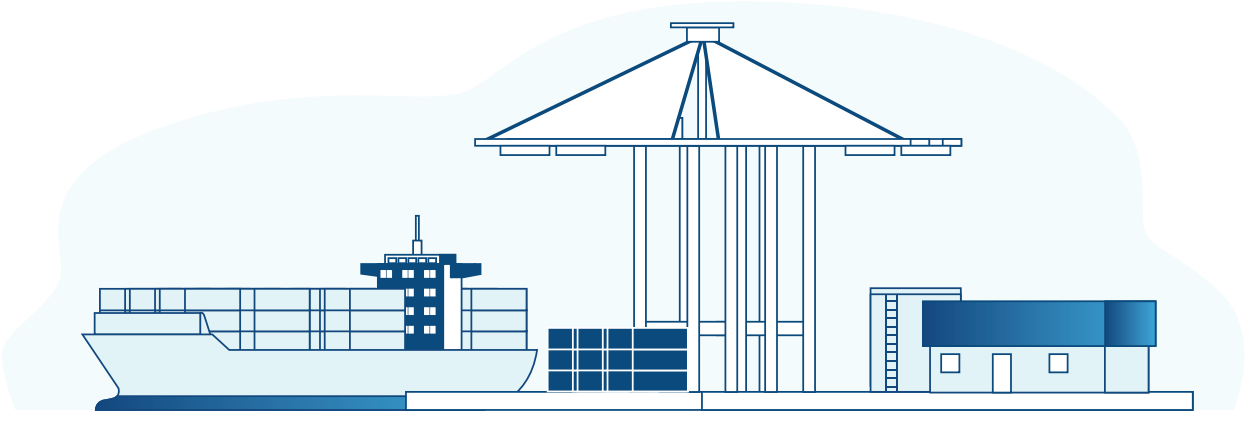
**Real estate and legal services lag behind accountancy, financial services, and insurance on some aspects of financial crime preparedness—a notable gap as expanding financial crime regulations increasingly put non-financial services organizations in the spotlight.**

- Respondents in those first two industries rank lower than their counterparts in financial crime compliance and prevention areas, such as having a robust governance infrastructure and sufficient technology and investment.

**Fewer than 4 in 10 (37%) are very confident in their financial crime compliance program's ability to evaluate supply chain threats.**

- The most prominent threats relate to cybersecurity (56%) and political instability (35%); only 38% say their financial compliance program is "very prepared" to handle such threats in the year to come.



KROLL

# How Geopolitical Tensions Fuel Financial Crime

Authors


Howard Cooper


Dan Rice

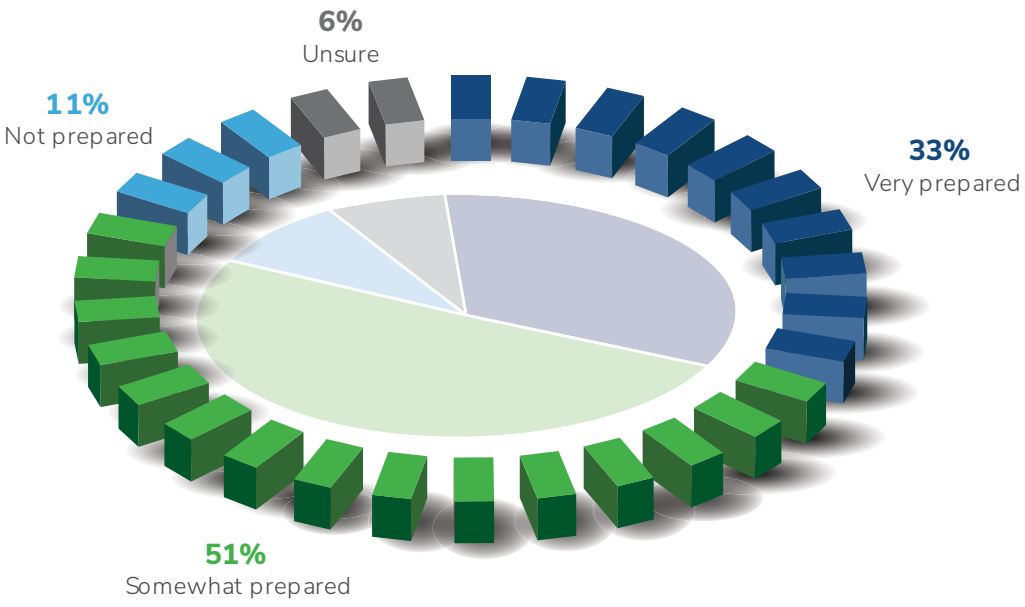

Oliver Stern

**Last December, amid ongoing conflicts in Ukraine and the Middle East—as well as potential turbulence stemming from the threat of higher U.S. tariffs and a deviation from U.S.-led free trade—the European Central Bank (ECB) made a timely announcement: In 2025, it would focus its supervisory work on geopolitical risks.**

**"Adverse geopolitical events are often not priced in by financial markets, which can lead to an abrupt repricing of risks if such events materialize," said Claudia Buch, the ECB's top supervisor.**

Geopolitical events create economic risk at the macro and micro levels. Less well reported, however, are the ways in which increased financial crime risk goes hand in hand with geopolitical tensions. The underrepresentation of such risk was reflected in our survey findings: Only a third of respondents said their financial crime compliance program was very prepared to address geopolitical issues in the year ahead, even as geopolitical risk and political instability were among the factors deemed most responsible for the anticipated spike in financial crime.

**Overall, how prepared is your financial compliance program to address geopolitical issues in the next 12 months?**

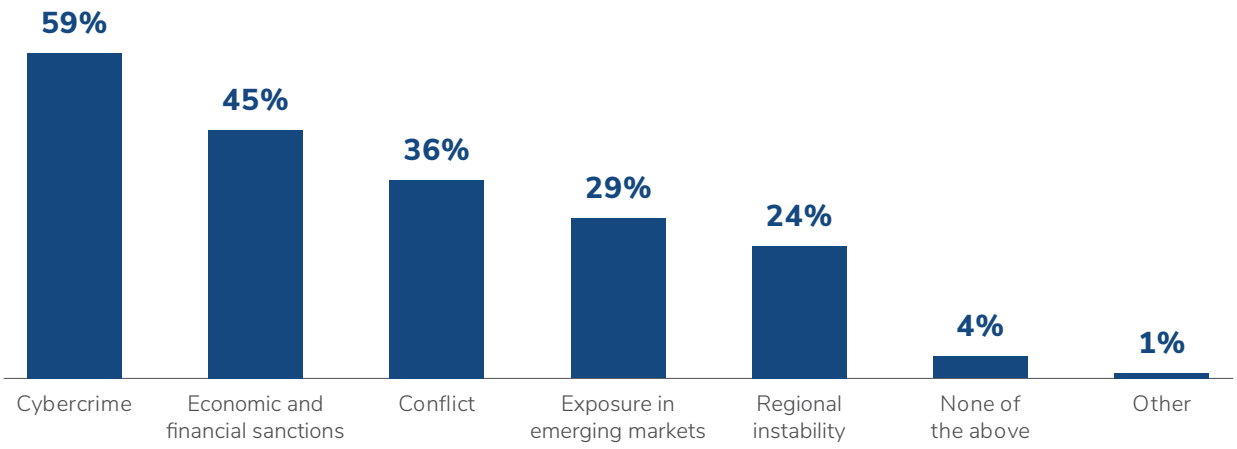


To manage geopolitically driven financial crime, businesses need to step up their compliance capabilities and increase cooperation with regulators around the world. Here's an overview of where companies currently stand and what they need to know moving forward.

## Emerging Geopolitical Risks and Organizational Readiness

Unsurprisingly, cybercrime is the top geopolitical threat to organizations' financial crime programs, selected by 59% of those who are less than "very confident" in their program's ability to scan and access such threats. Examples are everywhere—from Iran-based ransomware attacks on U.S. organizations and Israeli banks to Russian-backed distributed denial-of-service attacks related to the war in Ukraine. Such incursions are only amplified by artificial intelligence tools that have made sophisticated attacks more accessible to cybercriminals.

**Which of the following pose the greatest geopolitical challenges to your program over the next 12 months?**

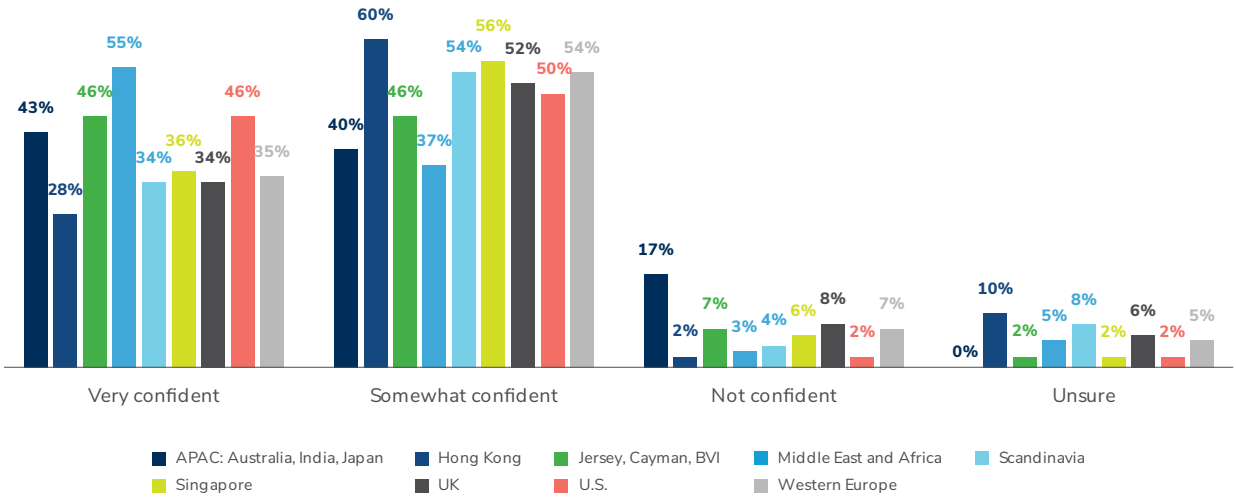



The risks here are far-reaching, as cyberattacks are specifically designed to disrupt and damage civilian infrastructure and the ways in which our societies function.

Economic and financial sanctions are also on executives' minds, selected by 45% of those respondents as the greatest geopolitical challenge. Overall, fewer than 4 in 10 respondents are very confident in their program's sanction screening capabilities, with only 35% from Western Europe expressing high confidence. The two biggest impediments in sanctions compliance: keeping up to date with changing regulations (49%, compared to 33% in 2023) and privacy protections (44%, up from 38% in 2023).

These blind spots could leave organizations vulnerable to financial crime. Where sanctions have been applied, organized crime groups and professional service providers will attempt to establish structures to move assets through the financial system and across borders—bypassing anti-financial-crime controls and processes as they do so.

**What is your current level of confidence in your own program's sanction screening capabilities?**

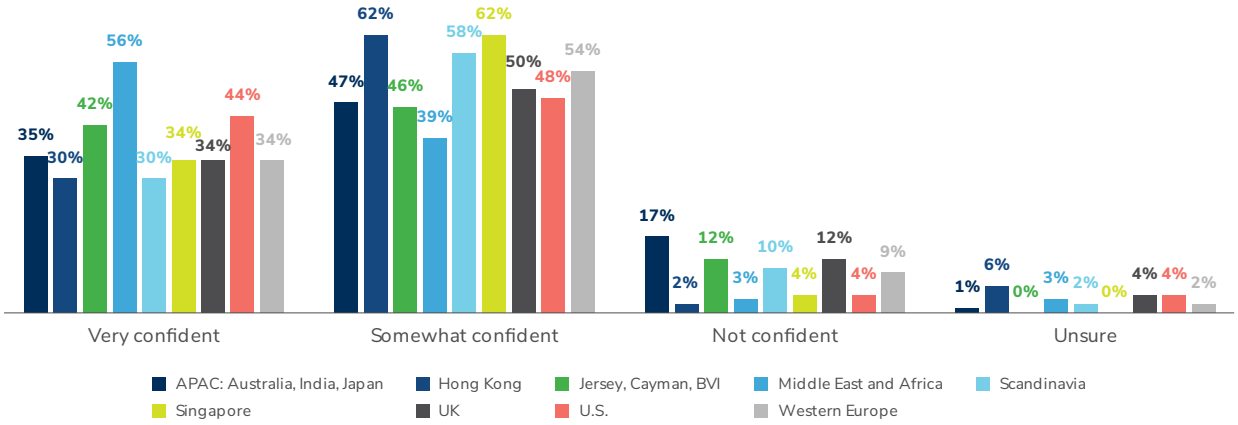



The increasingly interconnected nature of the global economy also creates opportunities for financial crime. States with limited access to regulated pools of capital can take advantage of less transparent jurisdictions to channel that money illicitly—even as these regions are bolstering their defenses against financial crime. In fragile and conflict states, meanwhile, the illegal trade of precious metals and stones enables regime continuity and fuels ongoing conflicts.

Other instruments are facilitating financial crime as well: Nearly 8 in 10 (77%) respondents, for instance, say cryptocurrency-related financial crime poses a concern for their organization in 2025.

Despite these obstacles, our survey reveals that only 38% of respondents are very confident in their financial crime compliance program's ability to scan and assess the geopolitical landscape for emerging threats. APAC (India, Japan, Australia) respondents are particularly concerned, with 17% saying they are not confident at all—perhaps due to uncertainties around the potential for an escalation of tensions between the U.S. and China and Taiwan's role in the South China Sea.

**What is your current confidence level in the ability of your financial crime compliance program's ability to scan and assess the geopolitical landscape for emerging threats?**




Automation, AI and other technology investments can help—and governments increasingly expect organizations to use these tools more effectively to prevent attacks. Nearly half of respondents say they are investing in AI solutions (49%) and other technologies (47%), as well as increasing their cybersecurity budgets (47%), to tackle the likely increase in financial crime.

## In an Increasingly Fragmented Geopolitical Landscape, Cooperation Is Needed

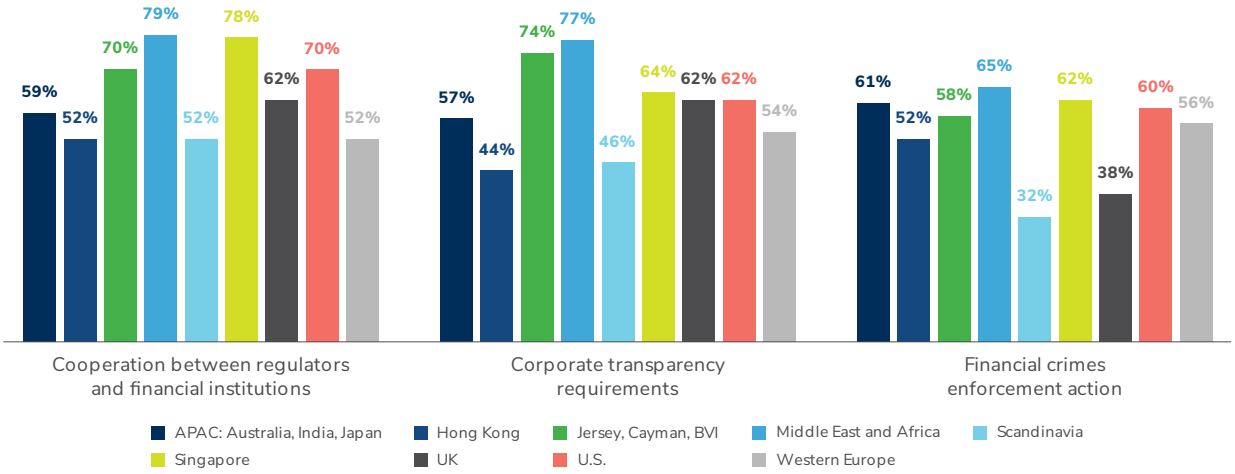
Those hoping to prevent, detect and respond to financial crime today are in something of a quandary. On the one hand, illicit economic activity is ever more global and digital. On the other, fragmentation and a breakdown of established norms in international affairs—coupled with the increasingly nationalistic stance of many governments—inhibits the cooperation necessary to combat this activity, hampering regulators and businesses alike.

For instance, data from the intergovernmental Financial Action Task Force illustrates low levels of effectiveness of AML systems around the world. Only about half of countries recently surveyed by the International Monetary Fund (IMF)—particularly in emerging markets and developing economies—had a national, financial-sector-focused cybersecurity strategy or dedicated cybersecurity regulations.

With that said, cooperative global initiatives are still advancing, including the IMF's AML/CFT (anti-money laundering/combating the financing of terrorism) Thematic Fund, which aims to strengthen countries' frameworks for fighting money laundering and terrorism financing, and the EU's recent agreement on a new regulation establishing a single AML and CFT rulebook.

Our survey reflects a mixed view on such efforts, however, with 62% saying cooperation between regulators and financial institutions will increase in 2025 and 30% saying there will be no change (30%) or that cooperation will decrease (9%). Only 52% of respondents from Western Europe believe it will increase, perhaps hinting at some skepticism toward recent initiatives.

**Please indicate the extent to which you believe the following may change over the next 12 months. ["Increase" responses shown]**




## Best Practices

What can organizations do to improve their ability to detect and prevent geopolitically related financial crime? Here are three high-level best practices to get started:

- **Access diverse sources of intelligence and information** to respond to geopolitical risks as they develop. Innovative approaches to monitoring policy direction in markets of interest and assessing civil society sentiment—in tandem with internally available information—better prepare firms as geopolitical events unfold. Effectively triaging risk triggers as they are identified allows organizations to stay on top of changing dynamics and remain flexible in navigating this complex terrain.

- **Implement effective supply chain management.** Supply chains can expose organizations to geopolitical threats they may not otherwise encounter. Diversification is important to avoid the vulnerabilities that come with a concentration of suppliers in one geographic area.

- **Focus on cyber resilience.** Organizations don't have to be sitting ducks for bad actors. Strengthening cyber resilience can help. Conduct periodic assessments of the cybersecurity landscape, improve controls and processes, and encourage data reporting and sharing.

## Uncertainties Abound

When it comes to the intersection of geopolitical risk and financial crime around the world, much remains unknown. How will the conflicts in Ukraine and the Middle East play out? What impact will a second Trump presidency have on current tensions? In which ways will the continued adoption of AI bolster organizations' and cybercriminals' capabilities? And how will regulators respond?

For now, executives have little choice but to embrace uncertainty. But that doesn't mean they can't lay the groundwork to develop stronger geopolitical and sanctions screening capabilities—plus heightened cyber resilience—in the year ahead.

# A New Era of Financial Cybercrime Is Here

Authors

Tiernan Connolly

John deCraen

**The IMF has called the mounting risk of severe cyber incidents "an acute threat to macrofinancial stability."**

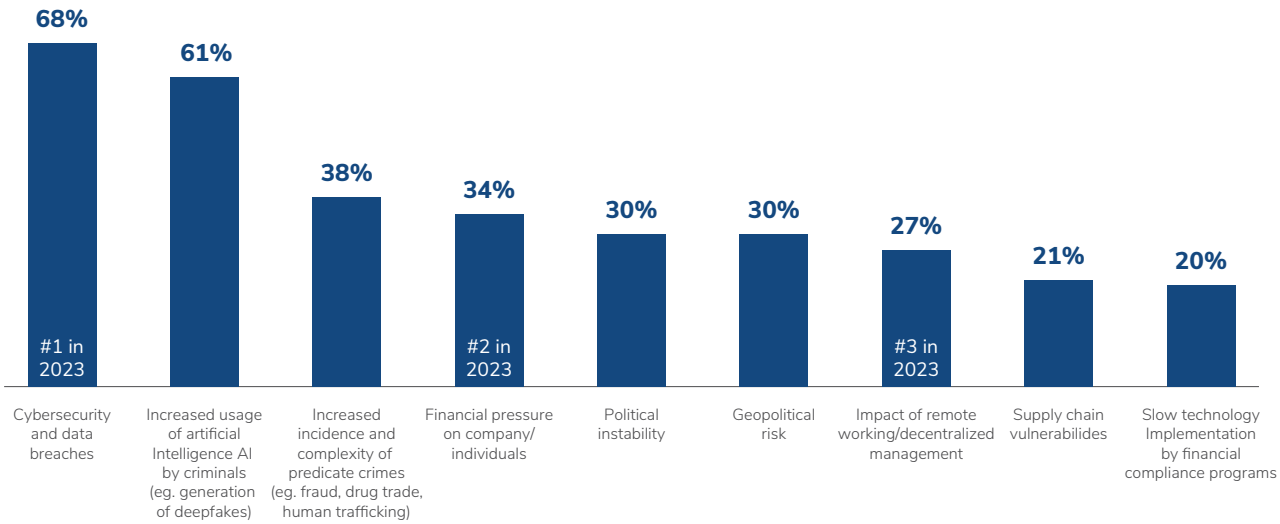
**It isn't hyperbole. Amid growing digitalization, heightened geopolitical tensions and a lack of international cooperation, cybercrime could cost the world more than USD 23 trillion by 2027. Extreme organizational losses from such attacks and other incidents have more than quadrupled since 2017 to USD 2.5 billion. The interconnected nature of today's financial systems means there could be severe collateral damage as well.**

Our latest survey fills out this troubling picture as it relates to financial crime, offering insight into pressing vulnerabilities, new regulatory developments and important security controls.

## Critical Cybercrime Vulnerabilities: Artificial intelligence (AI), Supply Chain and More

Our survey respondents are clear: Cyberattacks and data breaches are the number one factor behind the expected increase in financial crime risk, particularly for legal, real estate and insurance companies. Nearly 7 in 10 respondents selected this option, followed by the increased use of AI by criminals (61%).

**Which of the following factors are most responsible for this increased financial crime risk? [Asked to those who expect financial crime risks to increase over the next 12 months]**

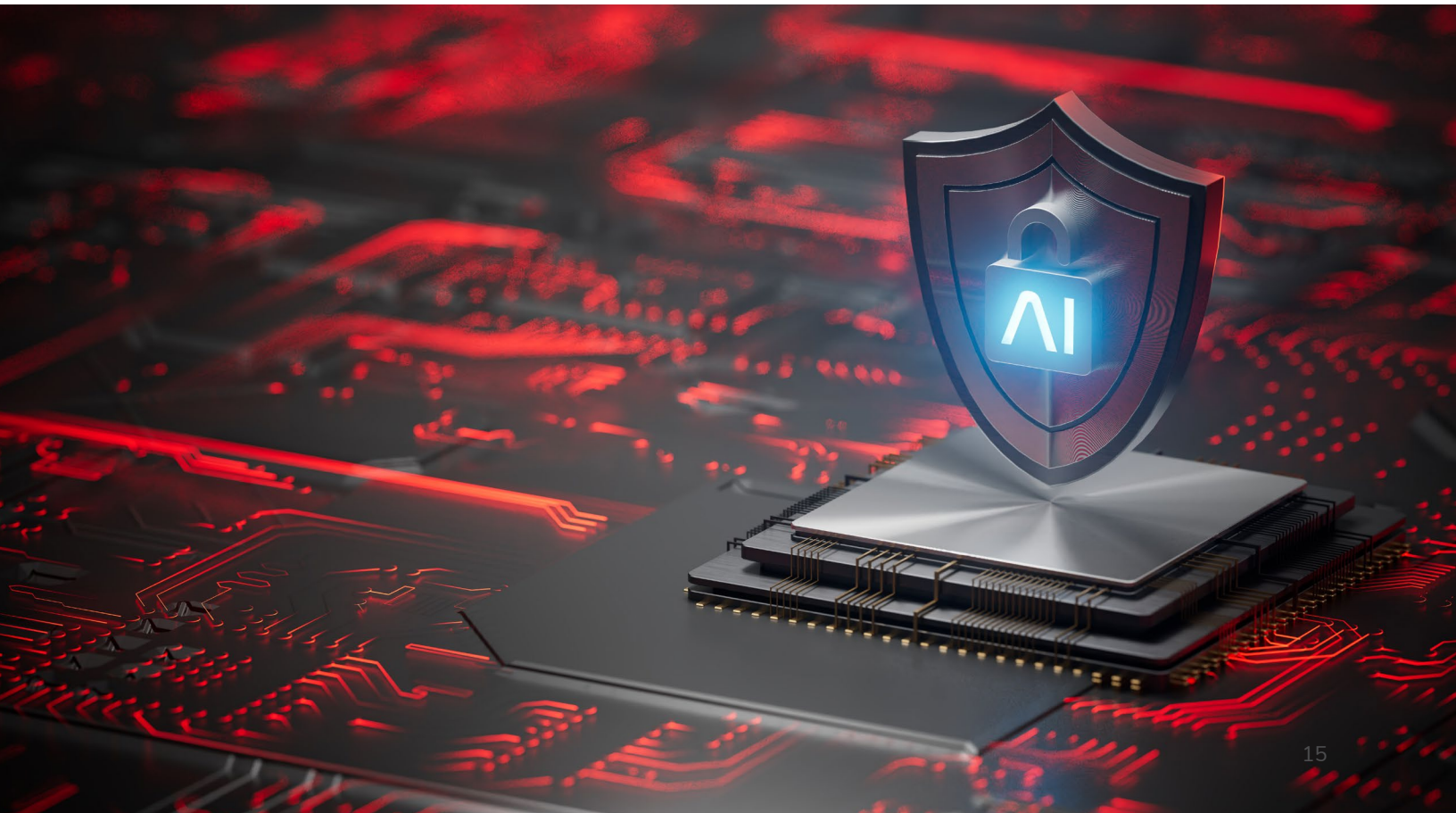


This shouldn't come as a surprise, given the above statistics. And as our AI article in this series illustrates, the rapid-fire adoption of AI tools can be a blessing and a curse when it comes to financial crime, providing new and more efficient ways to combat it while also creating new techniques to exploit the broadening attack surface—be it via AI-powered phishing attacks, deepfakes, or real-time mimicry of expected security configurations.

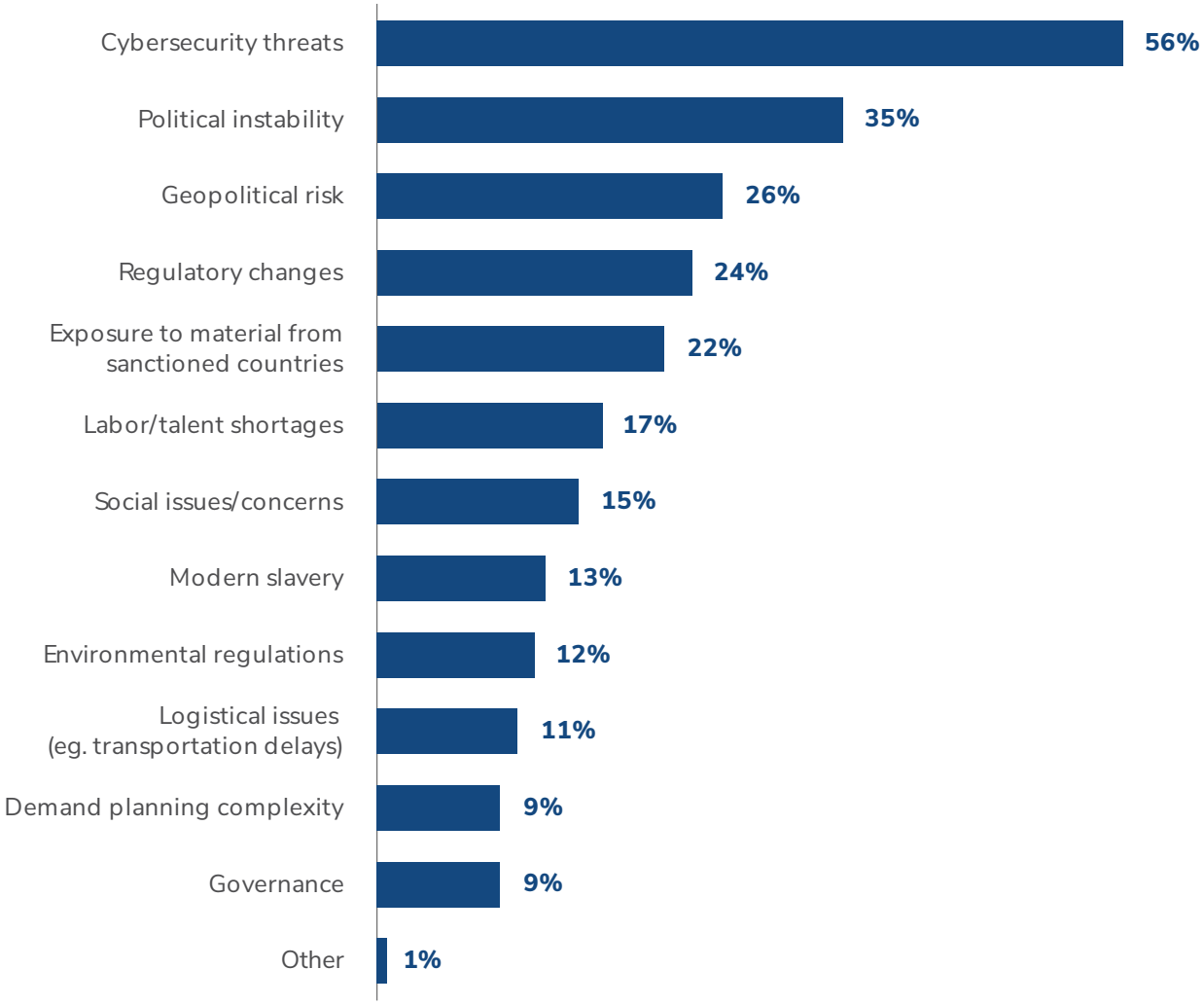
Attacks like these increasingly target and exploit weaker parts of an organization's supply chain, as evidenced in 2019's Solar Winds attack and the 2024 ransomware attack on software provider Blue Yonder, which disrupted payment and other operations at customers including Starbucks and two large UK grocery chains.

So-called "secret leaks"—unintentionally exposed passwords, encryption keys and other credentials—regularly provide attackers with access to endpoints along the supply chain. This risk is exacerbated by modern software development, which involves numerous third-party libraries, frameworks and tools, making it challenging to create unassailable, de-federated interchanges that manage secrets across these components. Rapid deployment cycles and the quick-fire adoption of new AI and machine learning (ML) tools generate additional vulnerabilities.

Many organizations still lack appropriate security controls to detect and prevent supply chain-related attacks. Just 37% of respondents said they were very confident in their financial crime compliance program's ability to assess supply chain threats, and a similar number (38%) said their program is very prepared to address these issues in 2025. That is problematic, since more than half (56%) of respondents who are anything less than "very confident" in their program's ability to detect supply chain threats say cybersecurity threats pose the greatest supply chain-related challenge to organizations' financial crime programs in the year to come—far and away the most-cited of any issue we asked about.



**Which of the following supply chain-related issues pose the greatest challenges to your program over the next 12 months? [Asked to those who indicated they were anything other than "very confident" in their financial crime compliance program's ability to assess supply chain threats]**



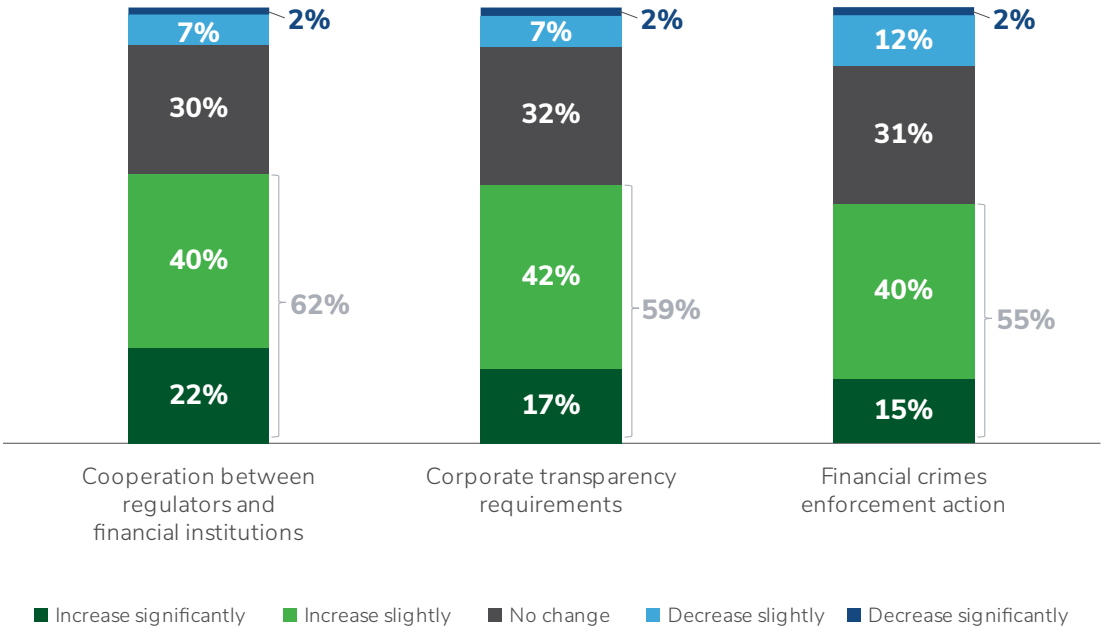

Business leaders from APAC (India, Japan, Australia) and the U.S. were particularly concerned in this regard. A primary contributor here may be the heightened geopolitical and economic tensions between the two jurisdictions, with the U.S. looking to limit its dependence on China. Overall, political instability and geopolitical risk are two key risk factors when it comes to the expected increase in financial crime, with each selected by about 30% of those respondents.

Finally, cybercrimes are being expedited by proliferating cybercrime-as-a-service offerings on the black market, which make it increasingly easy and cost-effective to carry out sophisticated attacks. Remote work also expands the attack surface. Twenty-seven percent of respondents cite it as being most responsible for the expected increase in financial crime risk, while external remote services and valid accounts are the methods most likely to be used by ransomware networks to get into organizations' systems, according to a 2024 Kroll survey.

## Track Regulatory Requirements—and Gaps

In addition to protecting against cybercriminals, organizations must stay up to date with an ever-evolving regulatory landscape, as 55% of respondents expect financial crimes enforcement action to increase in the year to come.

**Please indicate the extent to which you believe the following may change over the next 12 months.**




Those with operations in the EU will be most affected, given recent regulatory developments. The Digital Operational Resilience Act (DORA), for instance, came into effect this January, placing new burdens on financial institutions and critical information communications and technology providers. DORA's most extensive requirements focus on third-party risk management, raising the bar for financial institutions with operations in the EU.

Relatedly, 2022's Network and Information Security Directive (NIS2) set out cybersecurity standardization goals that must be achieved by organizations deemed "essential" or "important" in all EU countries, with each country required to transpose the NIS2 directive into national laws. And the EU's recent AI Act creates even more complications for those using these much-hyped technologies—with steep fines for non-compliance.

Other regulators around the world are expected to adopt and enforce similar requirements to DORA and NIS2, while in the U.S. a growing number of state and local data privacy laws—plus cybersecurity regulation from agencies like the New York State Department of Financial Services—are creating a complex patchwork of rules. This regulatory hodgepodge, and the resulting compliance complexity, may help explain why U.S. survey respondents are particularly concerned about the impact of cybercrime and data breaches on financial crime (81% of U.S. respondents named it as a key factor, compared to 68% overall).

Given the evolving regulatory landscape and the globally interconnected nature of financial cybercrime, cooperation between regulators and financial institutions is critical. While 62% of respondents believe there will be increased cooperation in the year ahead, this number is lower among

those from Western Europe and Scandinavia (52%), where, ironically, the most stringent regulatory regimes are being enacted. Still, progress is being made: As the IMF notes, the Financial Stability Board's model for incident reporting and its development of a common lexicon are important steps toward harmonizing effective information sharing.

## Cybersecurity Essentials

How can organizations prevent financial cybercrime? Here are some high-level best practices to get started:

- **Ensure effective credential and account management.** Business email compromise (BEC) and phishing attempts—in large part now powered by AI tools that can help with grammar, spelling and social engineering—prey on environments with poor credential and account management.

  When a customer signs into their online account, many organizations simply assume that that person is who they say they are. Organizations must be able to verify the bona fides of the individual: For instance, at Home Depot, tool renters are required to take a selfie that matches their driver's license as part of the sign-in process. But many organizations are reluctant to interrupt a seamless client experience by, say, requiring multifactor authentication.

  Relatedly, financial institutions (and others) often don't have the right processes and controls in place to prevent new accounts from weaponizing BEC to commit wire fraud. In the financial industry, for example, there are tools that assign reputations to each bank account based on its transaction history. These "reputational detectors"—coupled with additional threat intelligence—can go a long way toward improving account management security.

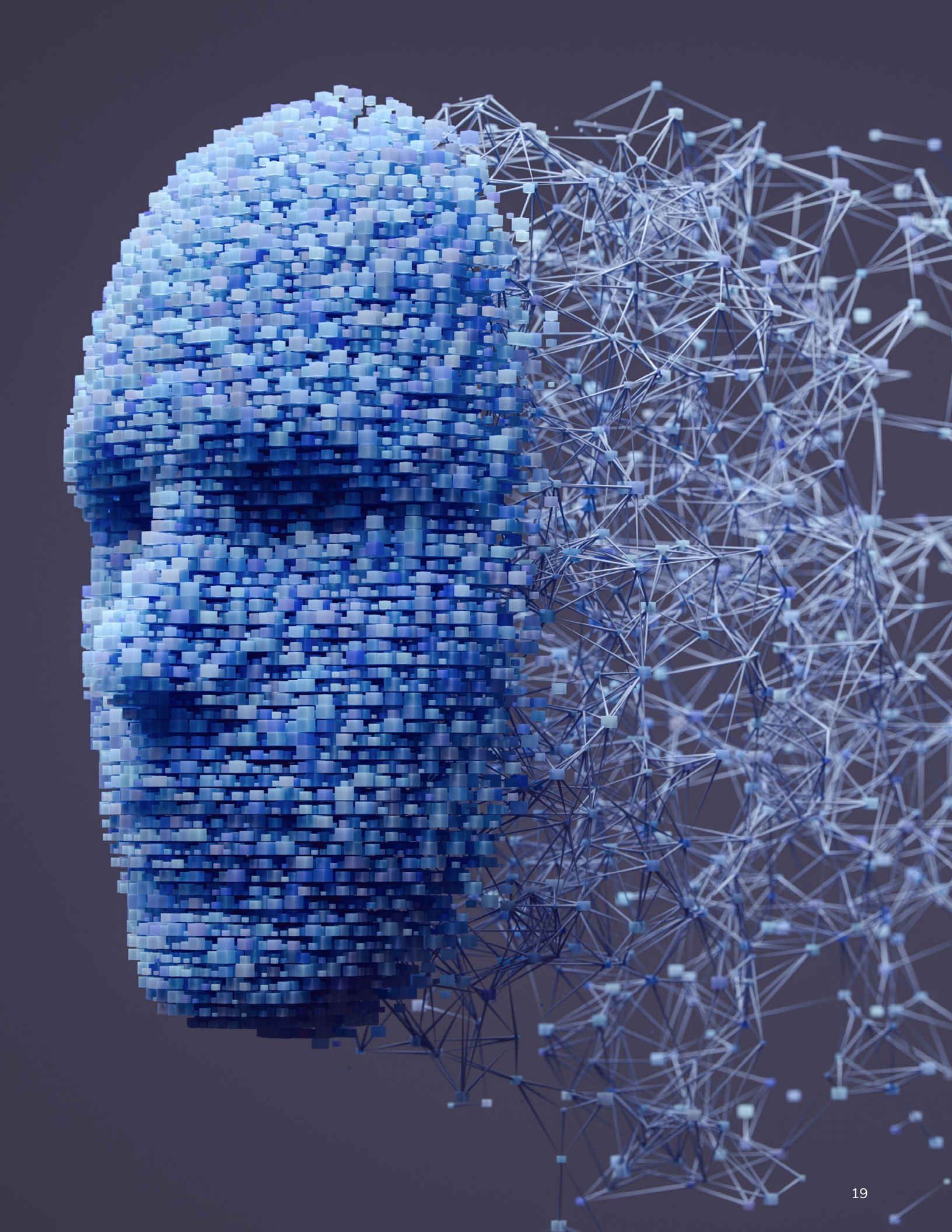
- **Implement control access policies.** Devices shouldn't be able to connect to your organization's network without any verification or controls in place. Organizations may want to ensure such endpoints have the latest operating systems and virus scanners in place, or that they don't come from a high-risk locale. Stepping up security in this arena is particularly important because threat actors can now impersonate device configurations to gain access to a system.

- **Focus on SaaS due diligence.** Software-as-a-Service (SaaS) applications are fast becoming an Achilles' heel for organizations trying to fight financial cybercrime. In 2023, businesses on average used 371 such applications, and many SaaS vendors are not forthcoming in allowing buyers to do adequate due diligence. Though they tend to share their SOC 2 audit information, many organizations don't realize this only provides a limited level of assurance; that is, the certificate being produced applies to only the corporate network and domain, not the customer environment.

## A Challenging Road Ahead

Financial cybercrime can (and likely will) happen to your business, whether it's a ransomware attack, a customer's hijacked bank account or an AI-generated phishing email that cracks open access to your organization's network. Nearly half of respondents (47%) say they are increasing their cybersecurity budgets next year to combat financial crime.

Yet whether organizations raise their budgets or not, foundational security controls and communicating the shared responsibility of good cybersecurity hygiene across the organization are crucial for today's business leaders—no matter what industry they're in.



# The AI Challenge

## AI is increasingly being used to combat financial crime—but it's also creating new hurdles

Authors


Dan Rice


Mark Turner


Richard Taylor

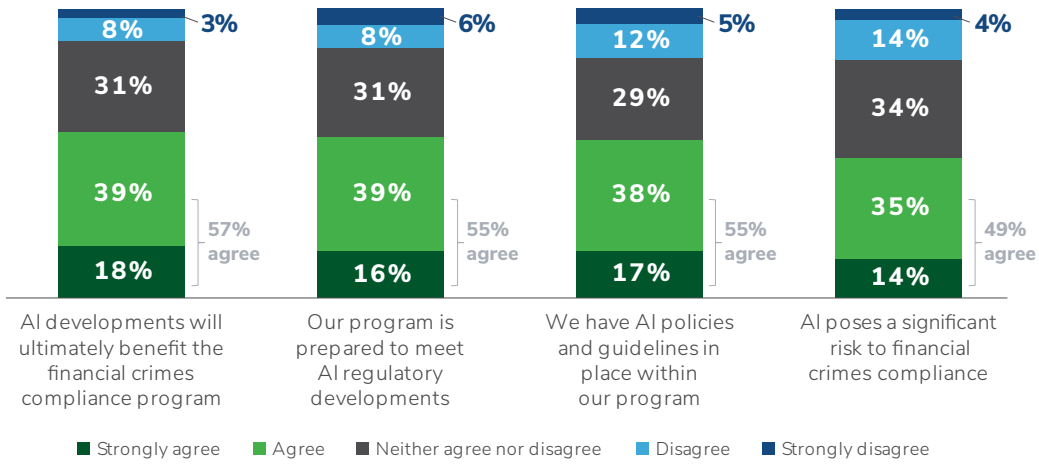
**Last November, the Financial Crimes Enforcement Network released a bulletin warning about an increase in fraud schemes using AI-generated deepfakes. According to FinCEN's analysis of Bank Secrecy Act data, criminals have leveraged generative AI to, for instance, create fake accounts that can receive and launder proceeds from other fraud schemes; impersonate executives; and instruct employees to transfer large sums of money to scammers' accounts.**

This, in part, is the world that proliferating AI has enabled—and the reason why 61% of survey respondents who expect financial crime risk to increase cite cybercriminals' increased use of AI., the second most cited factor, after cybersecurity and data breaches.

Yet AI is a double-edged sword: Even as bad actors use the technology to commit financial crime, organizations in industries from financial services to accountancy to insurance are using the technology to stop it. As then-Deputy U.S. Attorney General Lisa Monaco noted last year, AI "has the potential to be an indispensable tool to help identify, disrupt, and deter criminals, terrorists and hostile nation-states from doing us harm."

It's fitting, then, that 57% of respondents agree AI will benefit financial crime compliance programs, even as 49% agree it poses a significant risk. Both trends will likely accelerate as generative AI fuels the equivalent of an AI arms race.

**Please state your agreement with the following statements.**

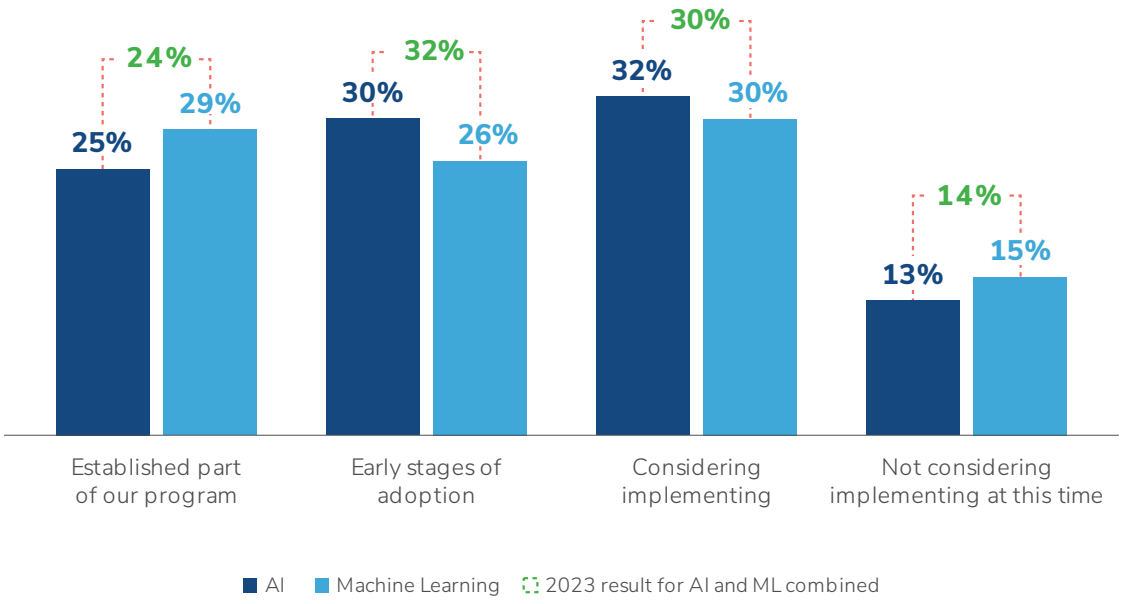


## AI Adoption Grows, but Organizations Struggle with Implementation

AI has been part of the financial crime prevention landscape for several years, aiding in everything from customer risk assessments and automated due diligence to transaction monitoring and data analysis. But as adoption of AI tools grows, so too does the awareness that they can be challenging to leverage effectively—whether the difficulty stems from bad data or missing employee skillsets.

Over half of all respondents to our latest survey are investing in AI solutions to fight financial crime. Twenty-five percent say AI is an established part of their financial crime compliance program, and 30% say they are in the early stages of adoption.

**Which of the following best summarizes your organization's current usage of AI and/or machine learning solutions as part of your financial crime compliance program?**




Taken together, the findings represent a notable rise in adoption from our 2023 report. Most who are already or considering using AI to fight financial crime are doing so to identify suspicious behaviors or patterns (63%), analyze networks (54%), identify risk signals (44%) and automate administrative tasks (41%).

This is not necessarily new ground. Back in 2022, the growing use of AI/ML in preventing financial crime even led *The Wall Street Journal* to report that regulators would start expecting banks to adopt such tools.

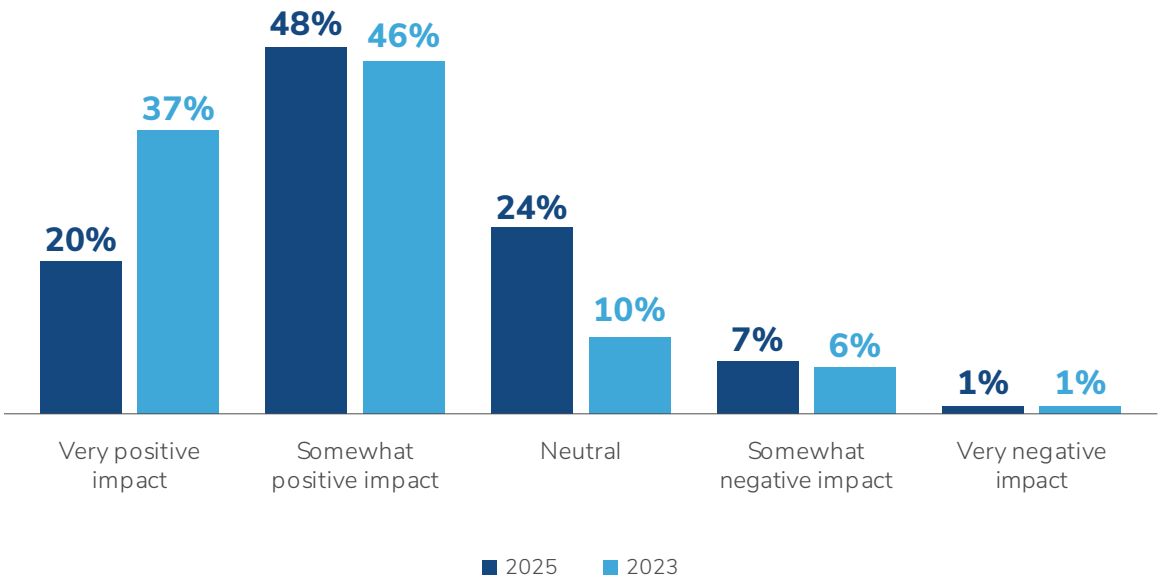
What remains an open question is how generative AI can be used to advance crime prevention tools like pattern recognition and data analysis to fight bad actors, who themselves will increasingly use large language models (LLMs) to generate fraudulent audio and text. Recent research has shown that LLMs can reduce the cost of the phishing process by more than 95%. Even more concerning: Nearly 80% of recipients in another study opened AI-written phishing emails—and 21% clicked on malicious content.

The latest technology offers benefits, too. Amid ongoing economic volatility and limited resources, generative AI embedded in financial crime prevention programs can help automate more mundane

tasks and guide employees to the right decisions in real time, overcoming an ongoing compliance challenge.

For now, however, as AI adoption rates increase, our survey reveals that positive perceptions of these tools' effects on financial crime compliance are *decreasing*. Only 20% of those currently using AI/ML say it has a very positive impact, compared with nearly 40% in 2023.

**What has been your perception to date of the impact of AI and/or machine learning on the financial crime compliance framework?**




On the one hand, the bar for entry has significantly lowered as the technology gets cheaper and easier to use. On the other hand, organizations still have a relatively immature set of policies and procedures when it comes to integrating these technologies—and many employees lack the sophistication to effectively oversee them. For instance, the European Banking Authority recently reported that roughly half of the 256 financial services companies fined in 2024 involved an "unthinking" reliance on new technologies, including AI.

These issues, coupled with some general disillusionment with much-hyped AI tools, can lead to disconnects between what businesses expect to get out of the technology and what it can actually deliver. AI could lead to a high rate of false positives when it comes to know your customer (KYC) reviews, or flag everyone of a certain gender without explanation for why it is doing so; alternatively, AI may not flag a transaction that it should have. As they get more familiar with AI, executives may also be discovering what they don't know—and that solving AI-related issues may not be as simple as they once thought.

At the root of many of these issues is a key organizational problem: bad data. Many might have thought that the AI itself would solve this issue when in fact it only exacerbates it.

## Regulatory Hurdles Mount

Just 55% of respondents agree (and only 16% strongly agree) that their financial crime compliance program is prepared to meet AI regulatory developments. For those in legal services and real estate, this percentage was significantly lower (30% and 40%, respectively).

This state of play is understandable given the emerging regulatory approaches currently underway around the world, like the EU's newly passed AI Act or a patchwork of U.S. state laws related to algorithmic discrimination, automated employment decision-making and AI bills of rights.

U.S. federal regulatory agencies have staked out positions on AI, too. The Consumer Financial Protection Bureau (CFPB), for instance, said in August 2024 that existing consumer protection laws—like the Consumer Financial Protection Act and Equal Credit Opportunity Act—also apply to new technologies, emphasizing that companies must "comply with crucial consumer protections that protect people from, for example, unlawful discrimination" and noting it may take steps to enhance oversight of algorithms used to inform lending decisions. Of course, these initiatives are poised to shift given the new Trump administration, which has already rescinded a Biden-era executive order aimed at establishing safeguards for AI use and ordered the CFPB to stop work.

So far, the UK is acting similarly to the U.S.—promising a less centralized, principles-based approach, at least for now—while China implemented Interim Measures for the Management of Generative Artificial Intelligence Services in August 2023. That said, the U.S./UK approach doesn't necessarily lower the compliance bar for businesses. These regulators are taking the stance that principles of good governance apply regardless of AI adoption and that regulated firms must be compliant with such rules if they go ahead with it.

Even the most prescriptive laws, like the EU's AI Act, apply more broadly than some might think, particularly for businesses that engage in highly regulated sectors like banking, insurance and healthcare. Having good governance structures and flexible, risk-based programs in place is the best way to ensure legal compliance —and avoid the steep legal, economic, and reputational risks of getting AI wrong.

Fortunately, 55% of respondents have AI policies and guidelines in place. That's just a first step, though. Executives will have to ensure they're evolving these policies year over year as today's hype matures into disciplined implementation and governance.

That may be a hurdle given the amount of documentation required for tech departments and third-party vendors, especially for organizations without the internal expertise to handle these risks and with a limited budget to expand teams. For example, the EU AI Act is heavy on technological documentation and requirements, while the EU's DORA, which went into effect this January, creates a binding, comprehensive information and communication technology risk management framework for the region's financial sector.

## Best Practices

How can business leaders successfully implement AI capabilities into their financial crime compliance programs while continuing to defend against the threats AI poses from outside? Here are a few best practices to keep top of mind:

- **Get the right team in place.** To manage the scope of AI-related documentation and governance, organizations must form cross-functional teams. Go beyond IT and cyber teams and involve those in

AML, compliance, legal, product and senior management. Achieving sound AI governance and implementation requires an all-organization approach to understand the use cases, risks and guardrails—and to communicate them effectively to regulators, customers and employees.

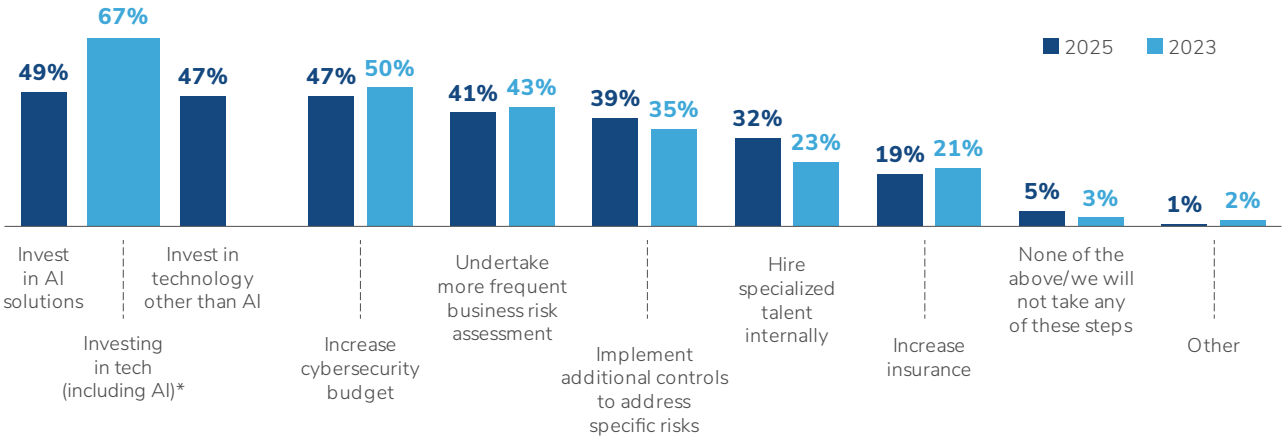
- **Frequent training, testing and education are key.** As suggested above, simply updating policies and expecting your workforce to abide by them isn't enough. There has to be focused, hands-on training with new AI tools. These trainings should be updated and repeated as the organization implements new AI capabilities and the regulatory and risk landscape changes. Firms should also undertake comprehensive testing before deploying AI and have sufficient monitoring in place to ensure it is working as intended.

- **To combat AI-related fraud, maintain a "back to the basics" approach.** Focus on fundamental human intervention and confirmation procedures—regardless of how convincing or time-sensitive circumstances appear.

## More AI to Come

In the year ahead, nearly half of respondents (49%) expect their organization will invest in AI solutions to tackle financial crime, and 47% say the same about their cybersecurity budgets. These investments complement one another, even as the mounting focus on AI may put added stress or pressure on cyber programs—particularly in a resource-strained environment.

**Which steps will your organization take internally in the next year to tackle the likely increase in financial crime?**




These and other findings from our latest survey reveal that organizations are headed in the right direction when it comes to AI use in financial crime prevention. However, obstacles remain, and business leaders must accelerate their organization's AI understanding, adoption and implementation. Bad actors will continue to innovate as new technologies become increasingly accessible. Those trying to stop them will have to as well.

*In 2023: Technology and AI were not separated.*

# Financial Crime Isn't Just a Financial Services Problem

## Here's what other industries need to know

Authors

Hannah Rossiter

Tarun Bhatia

**When it comes to fighting financial crime, there's a world of difference between the financial services sector and industries like real estate and legal services. Between stringent regulations—from the Bank Secrecy Act to KYC due diligence requirements—and steep penalties for non-compliance, it's no surprise that financial services organizations tend to be more advanced when it comes to financial crime preparedness.**

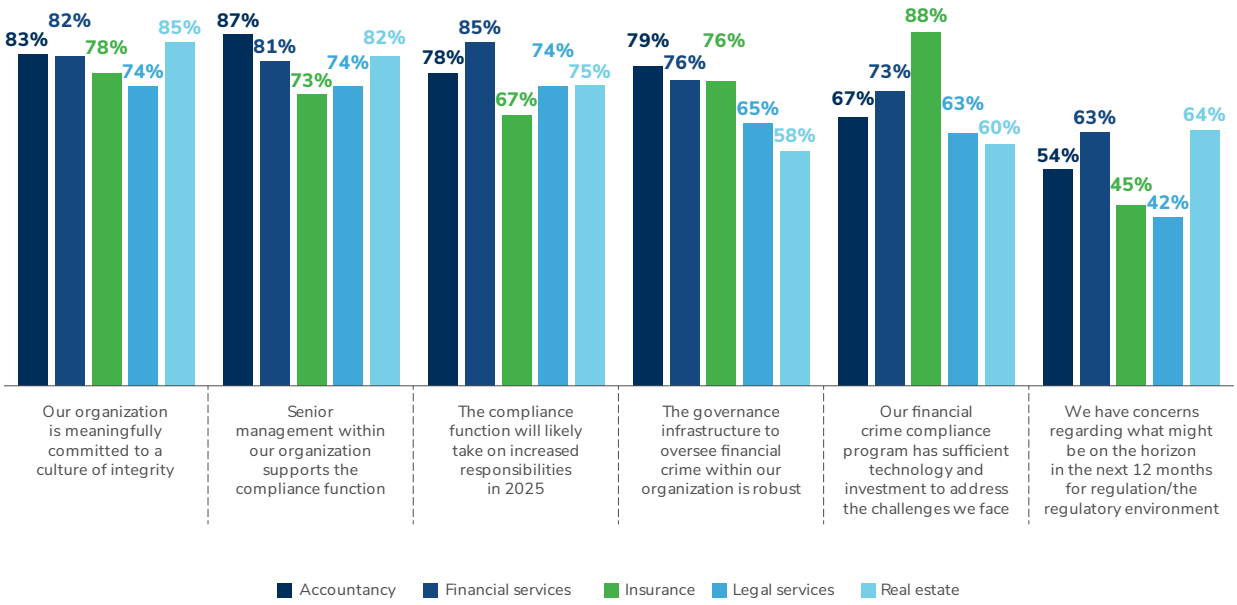
But as governments continue to extend anti-money laundering (AML) and other requirements beyond the banking sphere, other regulated industries that were previously subject to lower levels of scrutiny are now finding themselves in the spotlight. Efforts to close what some see as critical loopholes—for example, criminals who launder money by paying cash for residential real estate—demonstrate the urgency for non-financial services organizations to ramp up compliance programs and expertise.

That urgency will only deepen with the next round of evaluations of countries by the Financial Action Task Force (FATF), a global intergovernmental body that sets anti-money-laundering law standards. FATF is set to focus more on non-financial services entities, including the above industries as well as accountancy, dealers in precious metals and stones, casinos, and trust and company service providers.

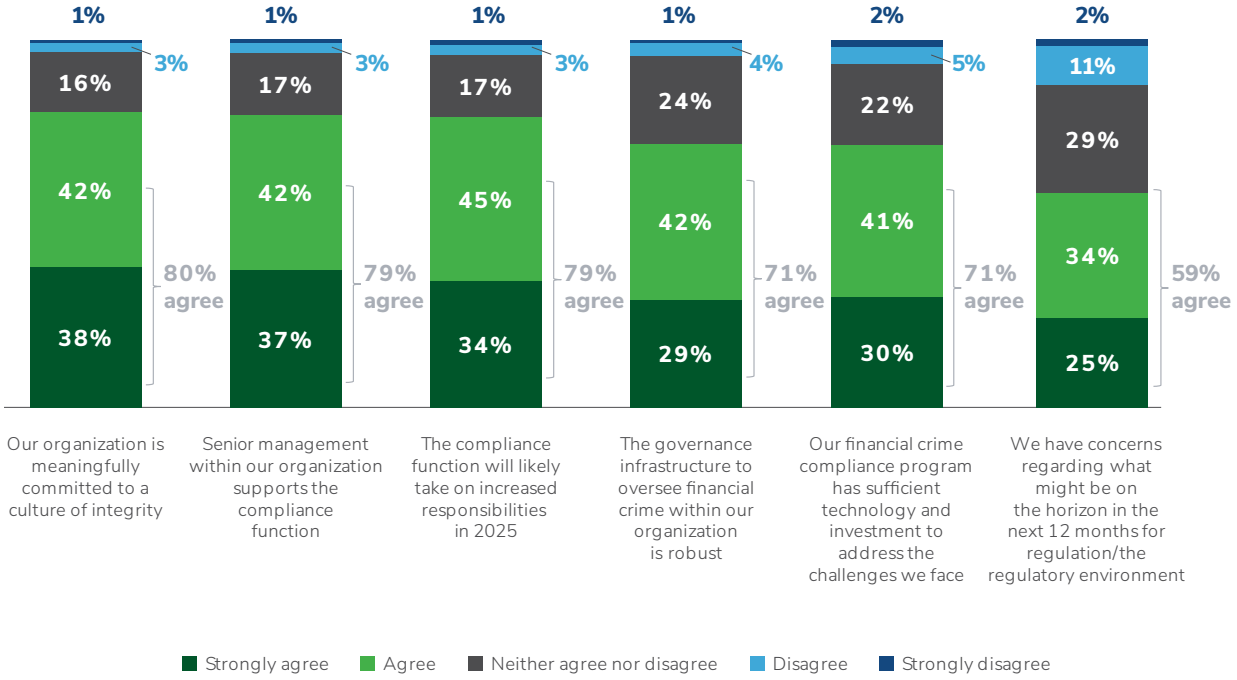
Our research indicates some industries have ample work ahead, from preparedness and technology investments to sanctions compliance. For example, real estate respondents were the most concerned of all surveyed sectors about what might be on the regulatory horizon. They also had the lowest degree of confidence in their organization's governance infrastructure for overseeing financial crime: 58%, compared to 79% of accountancy respondents and 76% of those in financial services and insurance.

The legal services industry has its own set of challenges, with 1 in 4 respondents suggesting that their firm was not meaningfully committed to a culture of integrity and only 63% saying their financial crime compliance program had sufficient technology and investment.

**Please indicate your agreement with the following statements (industry level). ["Strongly agree" and "Agree" responses shown]**




**Please indicate your agreement with the following statements.**




The maturity gap could expose some players to significant risk. Regulators are finding increased rates of non-compliance with AML and other financial crime rules—and levying penalties accordingly. In Hong Kong, the city's Insurance Authority recently imposed a record USD 2.9 million fine on a major Asia-based insurance company over technical issues with its AML oversight system. And the UK's HM Revenue & Customs fined estate agents more than GBP 1.6M over AML registration failures between 2023 and 2024.

In what follows, we'll delve into the challenges facing industries with less experience in financial crime compliance—and how they stack up against the financial services sector.

## Close Watch on Insurance and Accounting

In November 2024, a U.S. insurance mogul pleaded guilty to criminal money laundering and conspiracy charges spawned by an alleged USD 2 billion scheme to defraud policyholders—a headline-grabbing example of financial crime in an industry where the FBI estimates insurance fraud costs more than USD 40 billion per year.

Given those numbers, it's no wonder that insurance is a regulated financial activity, though it faces different compliance requirements and vulnerabilities than financial services organizations—the risk for insurers tends to be on the asset side, where money is invested on behalf of policyholders. But insurers are accustomed to a considerable degree of supervision and demonstrate substantial confidence in their ability to fight financial crime. Eighty-eight percent of insurance respondents say their compliance program has sufficient technology and investment to address the challenges they face.

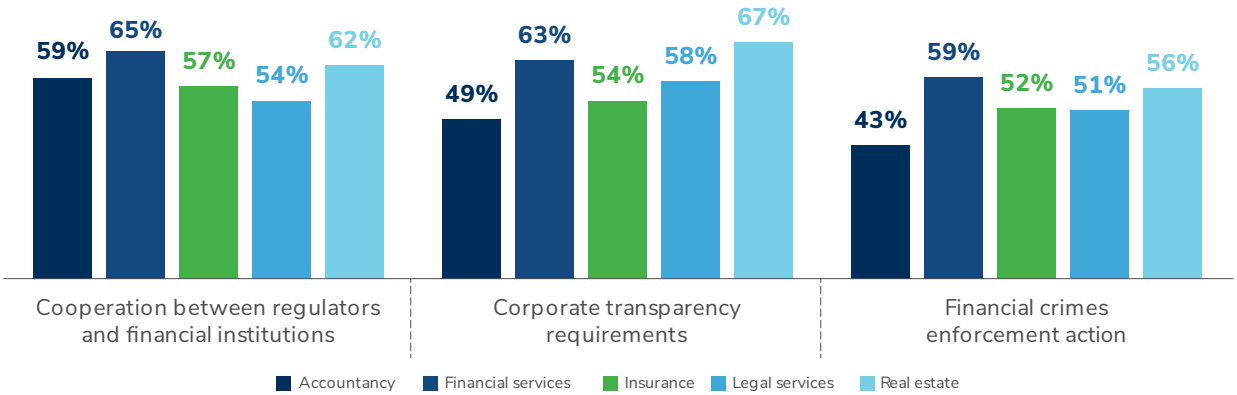
Similarly, large accounting firms are likely more familiar with AML and KYC requirements than, say, a real estate brokerage focusing on high-end residential properties. The majority of accountancy respondents (97%) report high levels of preparedness for conducting effective customer due diligence.

But it can be challenging even for sophisticated auditors to screen for and identify financial crime— in contrast to banks, where much of the liability is focused on customer deposits. Shortened audit windows compound the difficulty, as does the rapid evolution of clients' business models in a digital economy. The accounting scandal that brought down a prominent German electronic-payments company, for example, demonstrated the hurdles of auditing fintech and technology clients. And over the years, India has witnessed a series of corporate frauds where the role of accounting firms has been questioned.

Accounting firms are also under increased pressure to use a forensic lens while auditing, with many jurisdictions now obligating them to report fraud to authorities. In markets like Japan and India, auditors are expected to closely examine related-party transactions. Indian regulators also plan to overhaul the country's auditing standards, a move aimed in part at addressing financial crime. Existing rules—the Indian Companies Act 2013, the Companies (Auditor's Report) Order (CARO) and the Standards on Auditing (SAs)—already place reporting obligations on auditors to report fraud and suspected fraud to India's Central Government and its Board/Audit Committee.

Meanwhile, in the U.S., the Trump administration has said it won't enforce beneficial ownership disclosure requirements under the Corporate Transparency Act, a major law intended to tamp down on the use of shell companies by bad actors that imposes liabilities on accountants and other "gatekeepers". The shifting landscape may explain why accountancy respondents are the least sure of financial crime-related changes in the coming year when it comes to both corporate transparency requirements (49%) and financial crimes enforcement action (43%).

**Please indicate the extent to which you believe the following may change over the next 12 months.**



## Spotlight on Legal Services and Real Estate

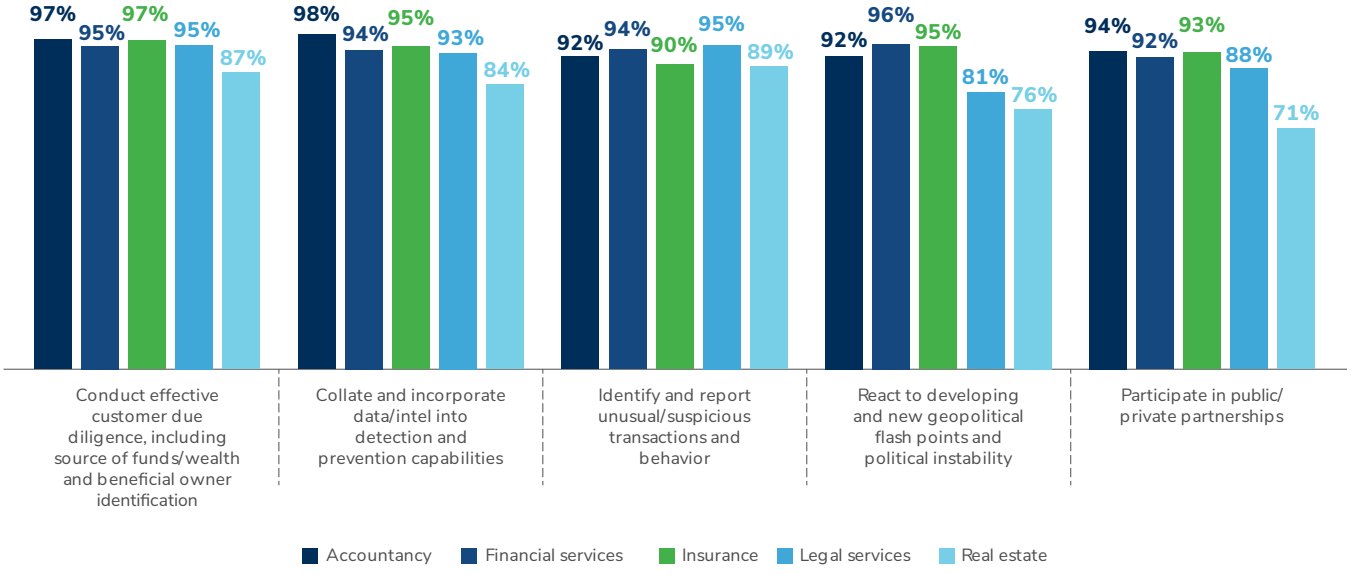
Financial crime prevention regimes are broadening. In addition to the new regulations noted above, real estate agents, art dealers and professional football clubs are among the entities in the EU now facing enhanced AML reporting obligations. In the U.S., proposed financial crime rules would require some investment advisors and real estate professionals to report suspicious activity. And Australia recently updated its AML law to obligate lawyers, accountants and others to undertake robust customer due diligence and report suspicious transactions.

Such expansions may present something of a shock to the system for industries like legal services and real estate. Big law firms routinely represent clients in economic crime cases and investigations, but they may not have the in-house expertise needed to safeguard their own organizations.

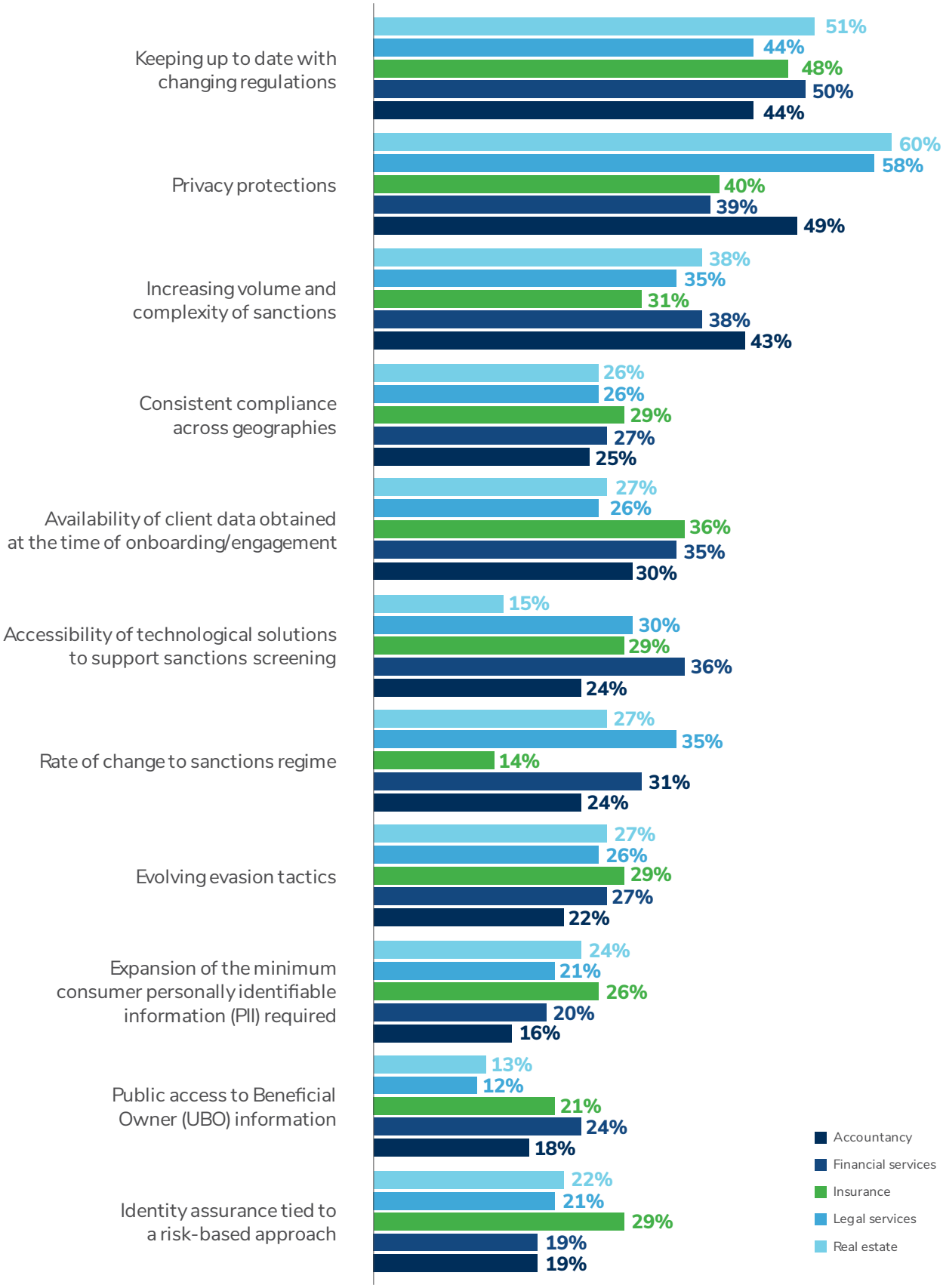
In the UK, the Solicitors Regulation Authority has fined law firms of varying sizes over AML failings. While some prominent cases have been dismissed, the reputational and financial risk is real, and it's clear that enforcement is on the upswing. Law firms in China and India may have fewer protections around client privilege than their U.S. counterparts, based on select instances of law firm premises being searched. However, information gathered in such a manner is unlikely to be used as evidence in a court of law.

Real estate may face the biggest hurdles among the non-financial services industries we surveyed. In addition to having little exposure to the types of client activities that put industries like banking or fund managers at risk, real estate indirectly benefits from financial crime by attracting funds generated by illicit activity. Our research found that at the industry level, real estate is the least prepared to take key preventive measures in addressing financial crime, from conducting effective customer due diligence to identifying and reporting unusual or suspicious behavior.

**How prepared is your organization to do the following.**



## Which of the following represent the most significant challenges in sanctions compliance?



Real estate and legal services also show differences from the other industries surveyed when it comes to navigating sanctions. Both are significantly more concerned about privacy protections as they relate to sanctions compliance (60% and 58%, respectively). This may be tied to the fact that more than half (54%) of legal services respondents and 47% of those in real estate conduct sanctions screenings entirely in-house—the highest share among industries we surveyed.

## Technology Investments

From risk analytics software to AI, technology can provide a critical compliance backstop for detecting financial crime. Our research shows the financial services sector is further ahead on some measures—though other industries are looking to catch up. More than half (55%) of financial services firms plan to invest in AI solutions in the coming year to tackle the expected increase in financial crime, followed by 52% in accounting and 45% in insurance. By contrast, only one-third of legal services respondents say the same—and just 26% of those in real estate.

Financial services is also in the lead when it comes to using AI and machine learning solutions to fight financial crime. Thirty-six percent say AI is an established part of their compliance program—15 percentage points higher than those in accounting and insurance, which had the next-highest levels of established implementation. Legal services and real estate report significantly lower penetration: Fewer than 10% in either industry say AI is an established part of their compliance program.

As technology tools proliferate and financial crime scrutiny expands, legal services and real estate respondents appear to be in catch-up mode, with 44% and 45%, respectively, considering AI implementation—the two highest shares by industry.

## Compliance Checklist

- **Education is key.** Industries playing catch-up with more highly regulated entities as scrutiny intensifies must engage in upskilling to ensure that staffers in a range of roles understand financial crime risks and best practices.
- **Targeted training.** Whether it's KYC standards or general training on AML measures, it's important for industries to understand the methods, tools and best practices for evaluating risk.
- **Consider outsourcing.** It takes time to build up internal expertise and muscle for spotting and fighting financial crime. Partnering with outside entities can help bridge the gap as organizations adjust to new requirements.
- **Avoid "off-the-shelf" solutions.** Programs should be tailored not just to your industry, but to your organization's specific activities and requirements. Avoid generic policies or applications that "check the box" but don't address root causes or require robust monitoring and engagement.

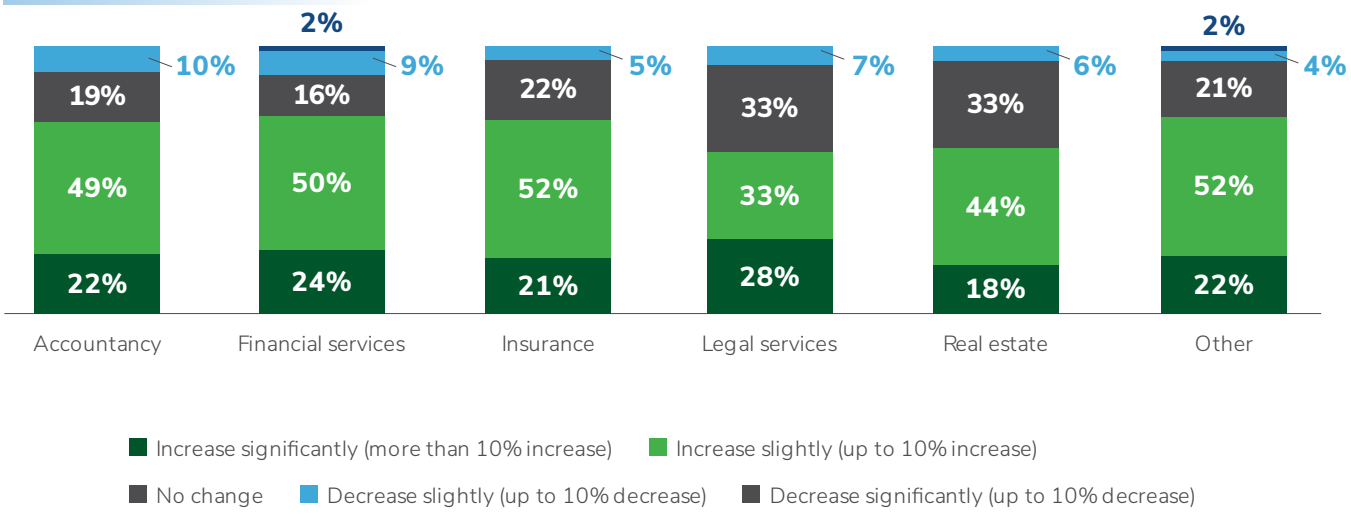
## Bracing for Risk Ahead

As industries move to implement compliance and meet new requirements, it's worth nothing that some of the biggest players in highly regulated industries still can miss the mark, as illustrated by the record fine and enforcement action last year on a major North American bank. Weak AML controls and due diligence at another big U.S. bank that was pushing to expand its wealth-management business, for example, demonstrate how even the largest banks can fall short of regulatory standards.

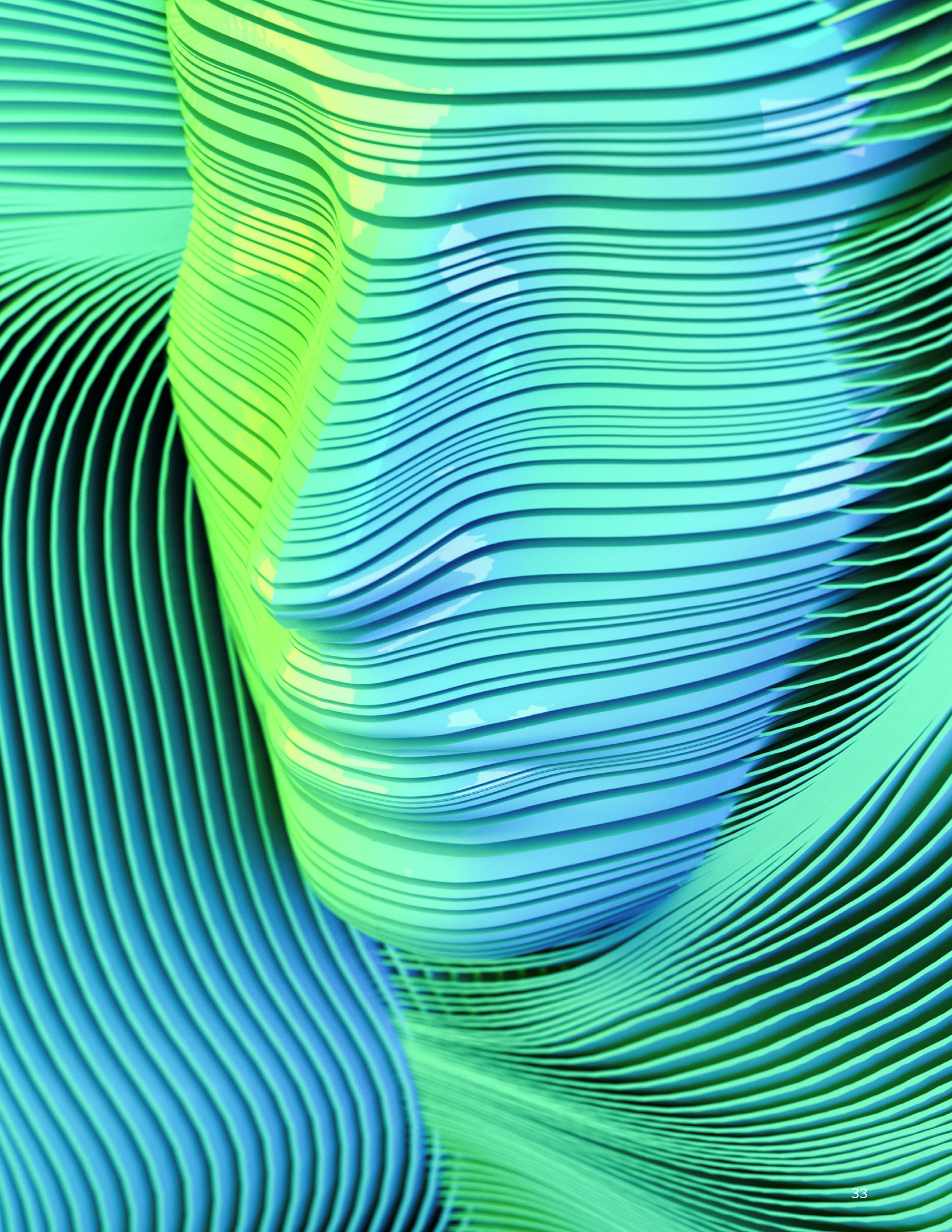
The industry's familiarity with both the impacts of illicit economic activity and the consequences for non-compliance may explain why financial services respondents lead in expectations of increased financial crime risk, with 74% forecasting an uptick in the coming year. Insurance (73%) and accountancy (71%) respondents were close behind, while the lowest expectations came from those in real estate (62%) and legal services (61%).

Meanwhile, other designated non-financial businesses such as gaming are facing increasing regulatory scrutiny, as illustrated by the monitorships imposed on some of the largest casino operators in Australia for AML/CFT failures.

**How do you expect financial crime risks to change, if at all, over the next 12 months?**




In an era of expanding financial crime regulations, industries facing new levels of scrutiny must adapt swiftly to meet rising compliance expectations. By prioritizing technological investments and leveraging best practices employed by the financial services sector, non-financial organizations can equip themselves to navigate the evolving regulatory landscape and fight financial crime.



# Confidence or Complacency?

## The evolving fight against financial crime

Authors


Amanda Wood


Mark Turner


Laura Walster

**Rising financial crime risk is casting a shadow over the global economy, as bad actors use the latest technologies to supercharge illicit activity and regulators expand AML and other compliance requirements across industries. Yet despite escalating threats and a higher bar for compliance, our research found a surprising degree of confidence within organizations about their abilities to combat money laundering and other financial crimes.**

Nearly three-quarters of respondents, for example, say their organization is either moderately (37%) or very (36%) prepared to identify and report unusual or suspicious transactions and behavior. More than 7 in 10 (71%) agree or strongly agree their financial crime compliance program has sufficient technology and investment to address the challenges they face. And 90% have some level of confidence in their program's ability to detect emerging geopolitical threats.

However, our experience working with organizations in financial services and other sectors suggests many entities may not be as effective as they think.

### Financial Crime Makes a Splash in 2024

Recent headlines highlight the gap between perceived capabilities and actual effectiveness in curbing financial crime by bad actors, both outside and within organizations.

Take the example of a large North American bank's USD 3 billion settlement with U.S. regulators in 2024. Prosecutors said the organization's failure to address "long-term, pervasive, and systemic deficiencies in its U.S. AML policies, procedures, and controls" allowed money laundering networks to transfer more than USD 679 million through the bank's accounts.

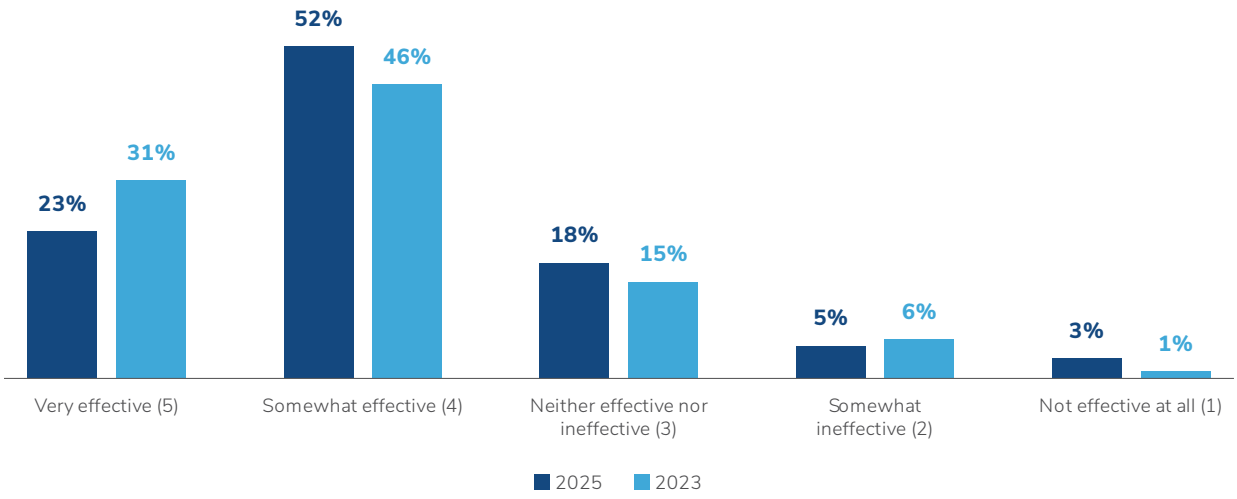
That same year, the UK's Financial Conduct Authority fined an online bank GBP 29 million for failings related to its financial sanctions screening framework; the bank's system had been screening new and existing customer names against only "a fraction of the full list of those subject to financial sanctions," the regulator said. In Germany, regulators fined a major bank USD 1.55 million in 2024 for breaching anti-money laundering duties.

Notable examples aren't limited to the financial services sector. In Australia, a large casino group agreed to pay an AUD 450 million penalty for AML failures that allowed organized criminals to infiltrate its casinos. And in the U.S., leaders of one of the largest-no fault insurance frauds in New York state history were sentenced to prison for their roles in a USD 40 million scheme targeting insurance providers that involved bribery, false healthcare billing and money laundering, among other crimes.

Such failures to halt financial crime—including among well-resourced and highly regulated institutions in industries with significant risk exposure—suggest that despite our respondents' strong levels of confidence in their financial crime compliance programs, such confidence may not be warranted.

There are signs that confidence may be slipping, too. Globally, only 23% rate their financial crime compliance program as "very effective," down from 31% in 2023. One likely reason: As organizations become subject to regulatory enforcement actions and more comprehensive compliance benchmarks, entities grow increasingly aware just how challenging it is to prevent financial crime—and how much work may lie ahead. These organizations are facing intense pressure to stay ahead as bad actors adapt their techniques—including deploying advanced technologies like AI-enabled deepfakes—to circumvent systems and controls at a much quicker pace.

**How would you rate the effectiveness of your financial crime compliance program?**




## Maturity and Expectations Gaps

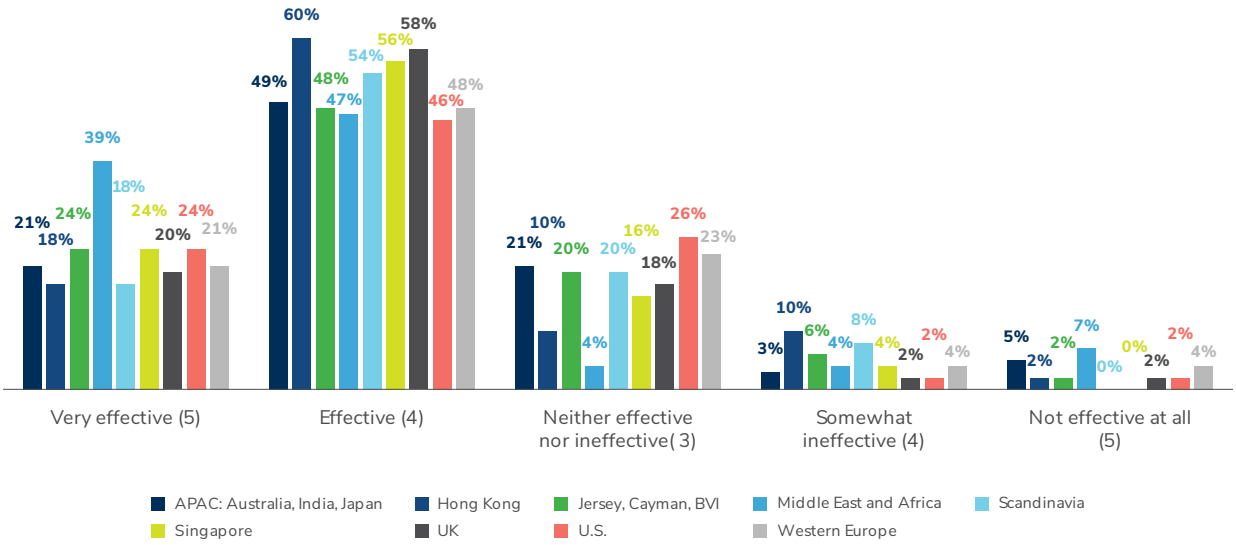
The survey findings revealed that confidence levels vary across different industries and regions. In our experience, this may stem from differences in financial crime maturity across different sectors and variations in expectations between different financial crime regulators across sectors and regions globally.

Respondents in jurisdictions with less advanced financial crime regulatory regimes, for example, may be a few years behind the curve, with compliance programs that may seem effective simply because they have yet to be fully tested. Those located in areas with more developed regulations and more forward-leaning regulators may have a more realistic view of their capabilities and/or potential exposure.

It follows, then, that nearly 4 in 10 respondents based in the Middle East and Africa rate their financial crime compliance program as very effective. That's nearly twice as many as the share of respondents from the UK, Western Europe and APAC (India, Japan, Australia) who say the same, and still significantly higher than those in the U.S. and Singapore.

Additionally, our work with global entities sometimes finds significant differences in financial crime prevention preparedness within organizations, depending on where firms within the group are located.

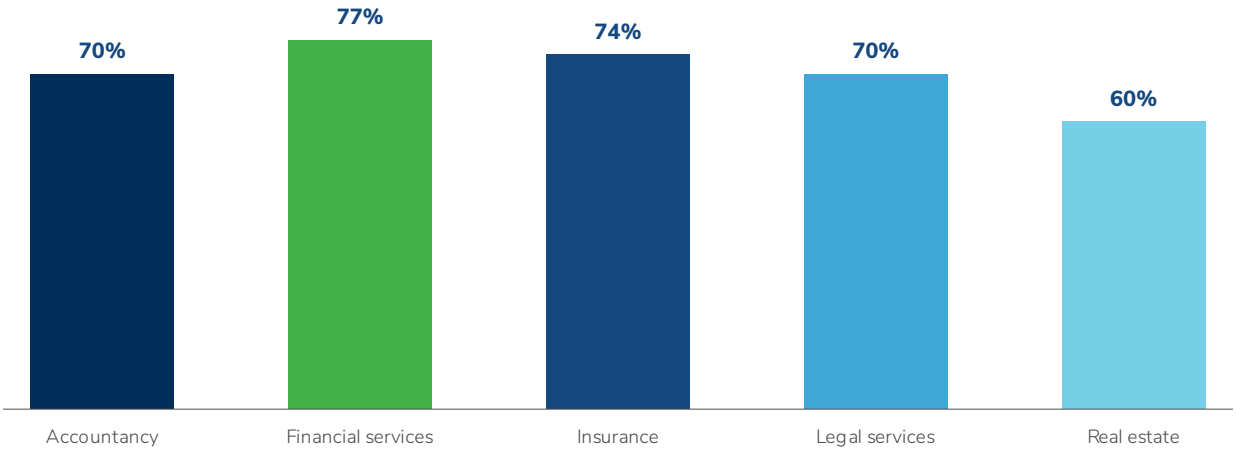
**How would you rate the effectiveness of your financial crime compliance program?**




Misplaced confidence in financial crime fighting programs could also stem from organizations—and at times the third parties they hire to support them—not adequately understanding or having an incomplete view of their financial crime vulnerabilities. To effectively respond to financial crime threats, entities need to understand their business's specific exposures to illicit economic activities, then implement appropriate controls to mitigate these risks. Often where we see deficiencies in financial crime compliance programs, regulated entities may be too narrow in their risk assessments, which makes it difficult to integrate the necessary controls or to evolve those controls to address new and emerging risks.

That lack of understanding creates particular vulnerabilities for non-financial industries—not just real estate and legal services, but also casinos and gaming—that are now experiencing heightened scrutiny in some regions. For instance, 70% of legal services respondents feel either very or moderately prepared to identify and report unusual or suspicious transactions; that's the same share as those in the more highly regulated accounting sector. Are law firms as prepared as they think to comply with expanding financial crime rules?

**How prepared is your organization to identify and report unusual/suspicious transactions and behavior? ["Very prepared" and "Moderately prepared" responses shown]**



## Technology and Data Mismatches

Technology is a critical area where overconfidence can expose organizations to significant risk. More than 9 in 10 respondents use technology, including AI, to screen for regulatory actions, fraud/bribery and corruption, and legal actions. But, while often helpful, investing in tech tools without robust integration and oversight doesn't always effectively fight financial crime—and bolting new solutions onto legacy technology may provide an unwarranted sense of security. It's essential that people understand not just how to integrate new technologies, but what to do with the data those systems generate and how to test and monitor their effectiveness.

Data integrity is paramount—compliance technology is only as good as the data you put into it. That's particularly true when it comes to AI, which 57% of respondents say will benefit their financial compliance programs. In addition to providing a flow of high-quality, well-structured data, organizations must also properly design and calibrate the systems into which that data flows to ensure they're detecting the right types of transactions and not capturing a disproportionate number of false positives.

Harnessed properly, technology can shine a light on where compliance is falling short, though careful implementation and ongoing monitoring are essential. Additional investment in such technologies may explain the eight percentage point drop in the share of respondents who consider their programs very effective since our last survey in 2023.

## Good Governance and Training Set the Tone

The fight against financial crime demands more than optimism—it requires careful planning and action. Organizations must bridge the gap between their perceived and actual capabilities by embracing robust governance, ongoing training, sustained investment in compliance frameworks, advanced technology and skilled personnel. The most successful organizations will target and maintain these efforts, tailored to their unique risks and vulnerabilities.

In a recent high-profile case, a bank's AML program failed to keep pace with expanding risks as the bank's business grew—with senior executives choosing "profits over compliance with the law—a decision that is now costing… billions of dollars in penalties," prosecutors said.

Effective financial crime compliance programs require buy-in across the entire organization, from the boardroom to customer-facing employees. People need confidence that reports of suspicious activities will be taken seriously by management, with clear lines of accountability and mechanisms to ensure that information makes its way up the chain to senior leaders. Training is essential, with programs that are engaging and tailored to organizations' specific needs and points of exposure.

By investing in these foundational pillars, organizations can evolve from misplaced overconfidence to well-founded readiness to tackle financial crime head-on in today's increasingly complex regulatory and criminal landscape.

KROLL

**About Kroll**

As the leading independent provider of financial and risk advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's global team continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at Kroll.com.

*M&A advisory, capital raising and secondary market advisory services in the United States are provided by Kroll Securities, LLC (member FINRA/SIPC). M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Kroll Securities Ltd., which is authorized and regulated by the Financial Conduct Authority (FCA). Valuation Advisory Services in India are provided by Kroll Advisory Private Limited (formerly, Duff & Phelps India Private Limited), under a category 1 merchant banker license issued by the Securities and Exchange Board of India.*

© 2025 Kroll, LLC. All rights reserved. KR25010160