



Global Compliance Outlook

Rising Ambition, Fragmented Reality

A survey of financial services compliance executives by the Harris Poll on behalf of MCO (MyComplianceOffice).



Table of Contents



Introduction..... 3

Executive Summary 4

Looking Ahead: The CCO Outlook in 2026 and Beyond 5

The Fragmented Landscape of Compliance Technology..... 10

The Varied Landscape of Compliance Risk15

Spotlight On: AI 21

Conclusion..... 26

Respondents and Methodology 29

About MCO 31

Introduction

MCO's Global Compliance Outlook, conducted in partnership with The Harris Poll, provides insight into the priorities, pressures and technology trends shaping financial services compliance today—and how leaders expect them to change over the next 12 months.

Compliance executives are navigating rising regulatory demands while fragmented systems and processes continue to make it harder to see and manage risk across the organization. The scope of compliance is expansive, increasing pressure on leaders to strengthen core programs, make better use of AI, data and technology, and support the business without adding further complexity.

As the compliance function becomes increasingly strategic, this research gives leaders a benchmark for assessing their own compliance programs and a clearer view of the decision points and trends shaping the industry's future.

—Paul Giardina, *Chief Marketing Officer, MCO (MyComplianceOffice)*



Executive Summary

Compliance leaders across the financial services industry are in the midst of another year of rising expectations and continued change. Budgets and technology investment are increasing as firms strengthen core areas of compliance and respond to a broad range of priorities, from financial crime and communications to digital assets and AI.

Investment alone, however, will not resolve the challenges facing compliance. Many firms are dealing with fragmented systems, providers, and processes. The focus moving forward is on using that investment to create a more integrated, data-driven compliance capability that can manage growing demands and play a more strategic role in the business.

The CCO role is becoming more strategic.

Compliance executives anticipate that their responsibilities will expand beyond regulatory interpretation to include a broader role as business advisers.

Compliance investment is set to rise with **93%** of respondents expecting budgets to increase over the next 12 months, and **89%** anticipating greater investment in compliance technology.

Compliance is mired in systems.

Organizations report using an average of **13.8** separate compliance systems. That complexity creates a **fragmentation tax** that makes integration and visibility difficult.

AI is already part of the compliance environment with **44%** of respondents already using AI in production for analytics or risk scoring. The challenge is how to operationalize AI with confidence, governance, and regulatory trust.



Looking Ahead:

The CCO Outlook in 2026 and Beyond

Compliance executives expect the demands on their function to grow, and they are preparing to invest accordingly. The findings point to higher budgets and technology spending, with KYC and AML, AI, and data management leading the priority list. Together, these priorities show firms strengthening core areas of compliance while investing in the capabilities needed for continued regulatory complexity and business growth.

The CCO role is evolving in response. Today, respondents most often associate the role with regulatory engagement and policy interpretation. In the future, they anticipate greater emphasis on being a strategic adviser, implementing data-driven compliance and embedding technology in compliance processes.



Compliance leaders are building a capability that can respond to regulatory change, make better use of data and support faster, more-informed decisions—and one that takes an increasingly strategic role in the business of the firm.



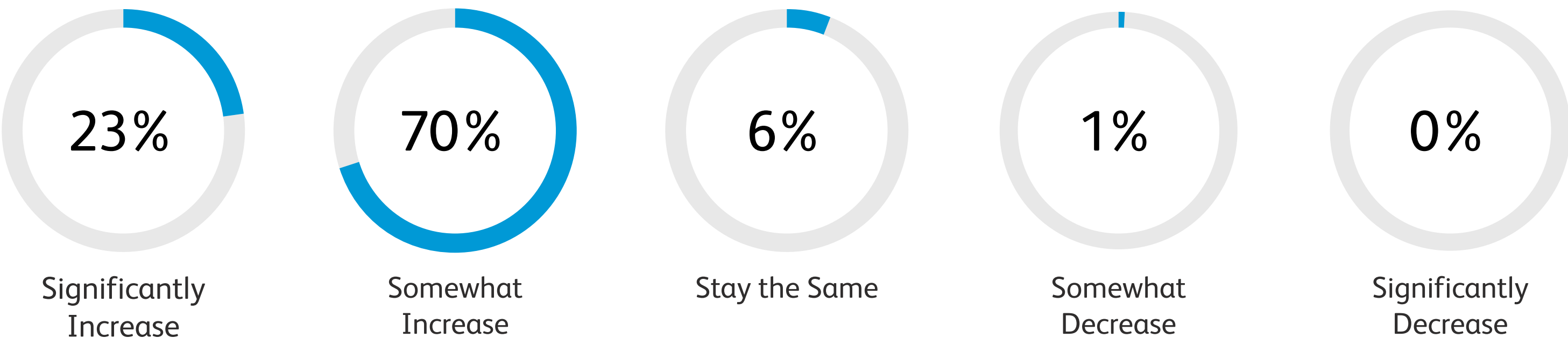


Compliance budgets are expected to rise

Compliance budgets are expected to increase for 93% of respondents over the next year.

This level of planned spending suggests that organizations see compliance as a continuing investment priority. The question for compliance leaders moving forward is how to direct that funding toward the areas that improve coverage, efficiency and decision-making across the function.

Over the next **12 months**, do you expect your compliance budget to...?

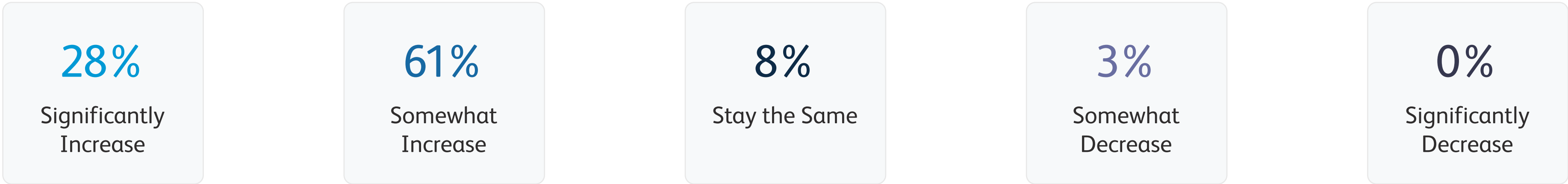




Technology is an investment priority for compliance leaders

Investment in compliance technology is expected to increase. That commitment comes as organizations already operate complex, multi-system compliance technology stacks. New investment will need to be evaluated not only on individual functionality, but also on how effectively it fits with the wider compliance environment.

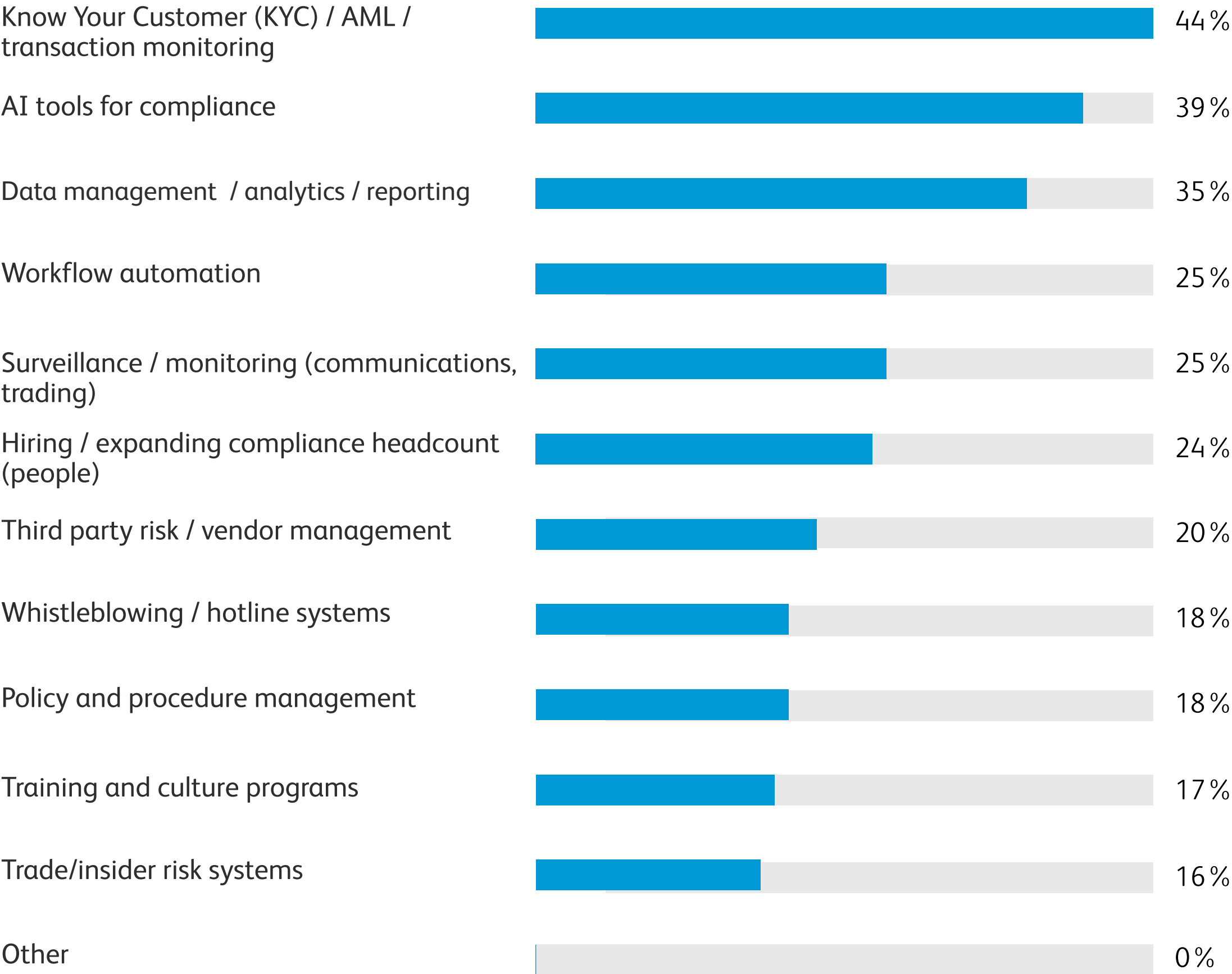
Over the next **12 months**, do you think your level of investment in compliance technology will...?



KYC, AI, and data management lead the investment list

KYC/AML is the leading investment priority for the compliance executives surveyed. AI tools, data management, and analytics and reporting follow closely behind. Viewed alongside the expected increases in compliance budgets and technology spend, the priorities suggest a focus on both the core areas of compliance and greater use of data and automation. Hiring and expanding compliance headcount remains important, but that sits alongside efforts to increase the capacity of the compliance function through technology.

Over the next 12 months, what are your organization’s top three investment priorities for compliance?



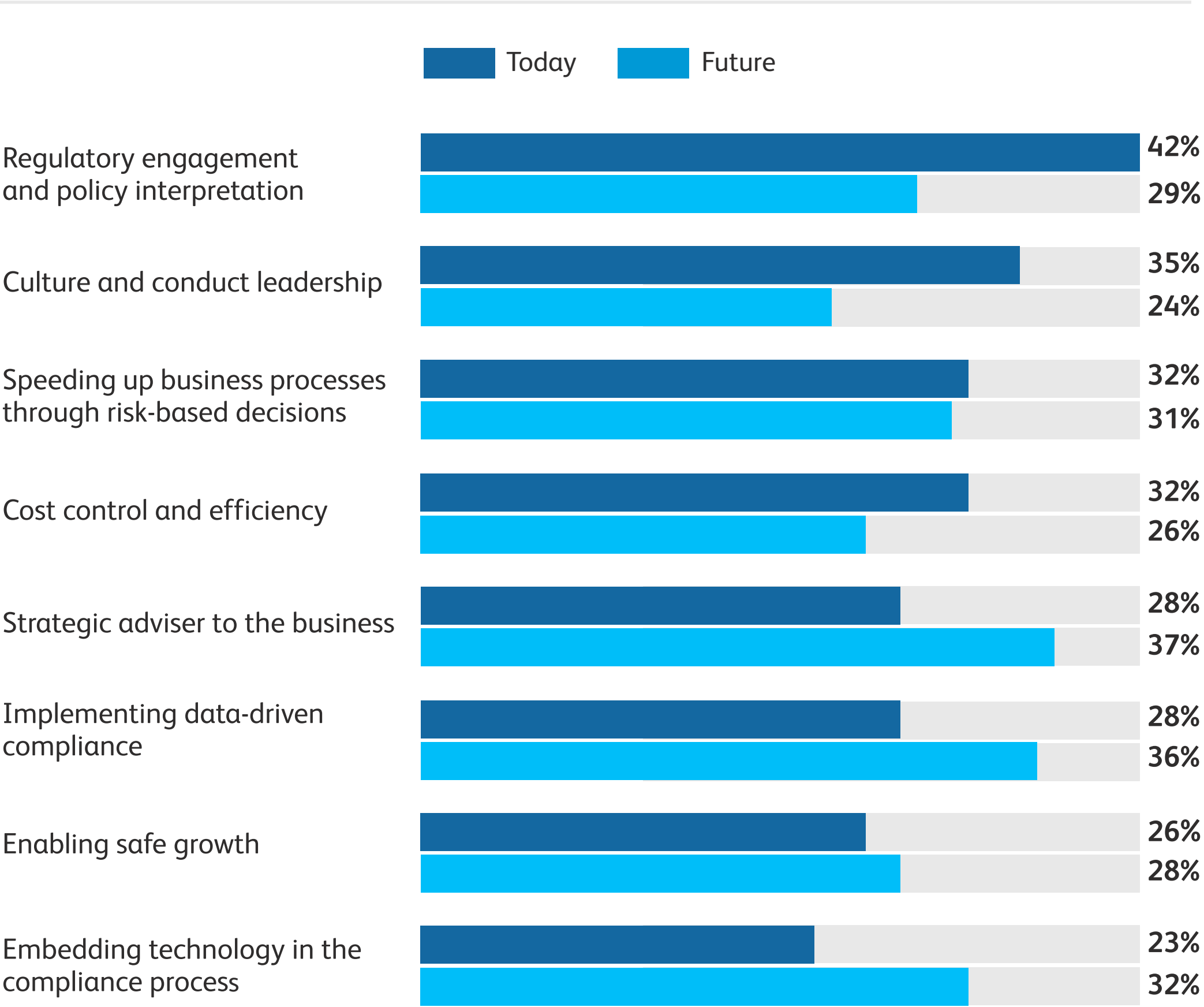
Respondents could select up to 3

The future of CCO is even more strategic, technology-focused, and data-driven

Today, compliance leaders most often define the CCO role through regulatory engagement and policy interpretation. Looking ahead, taking the role of strategic adviser to the business moves to the top of the list, while data-driven compliance and embedding technology also rank more prominently. Regulatory engagement remains important, but alongside greater emphasis on strategic advice and the use of data and technology.

Compliance leaders increasingly see their value extending beyond keeping the business within the rules to shaping its direction. The regulatory foundation doesn't go away — it becomes the base for a broader and more strategic role.

Thinking about the role of the Chief Compliance Officer (CCO) at your organization, please indicate what you think the role is today and what it should be in the future.



Percent of respondents

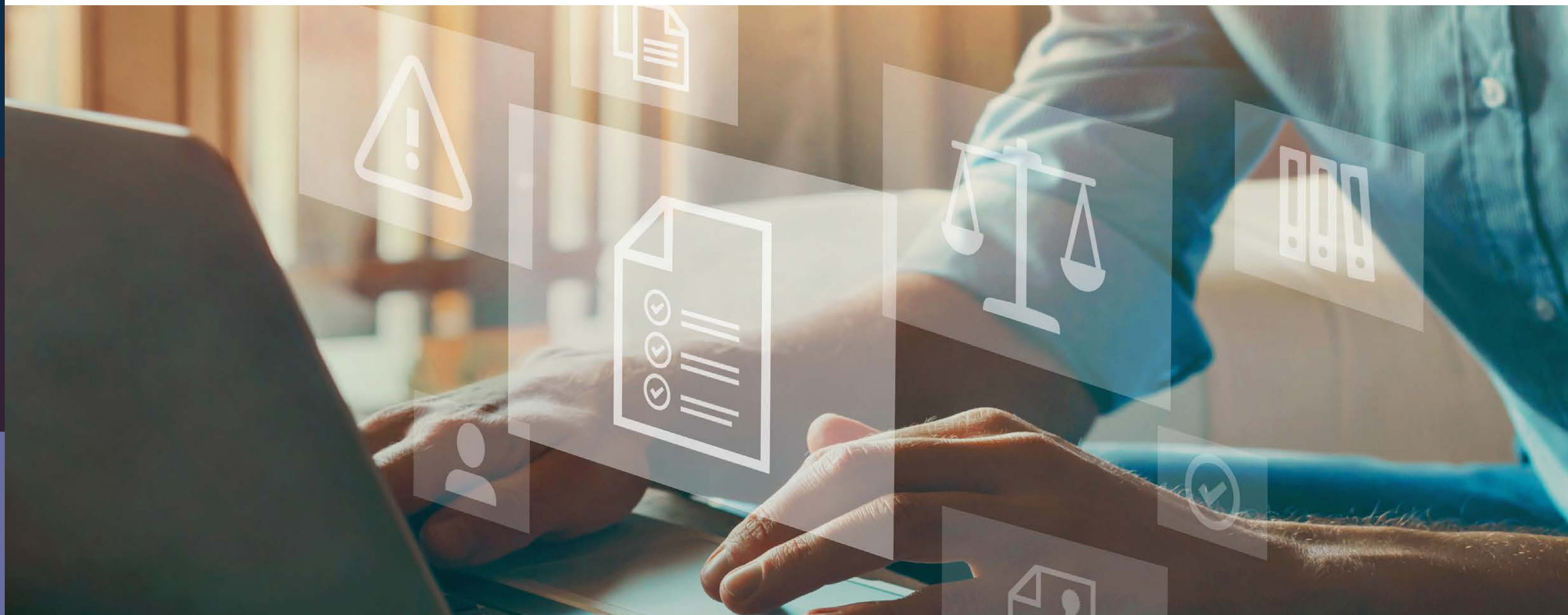
The Fragmented Landscape of Compliance Technology

The survey findings reveal a fragmented compliance technology environment. Organizations use an average of 13.8 systems and rely on a mix of vendor platforms, in-house technology, and manual processes across different areas of the compliance program.

Yet 65% of compliance leaders say their organizations still need more technology.

A large technology stack can reflect the breadth and maturity of the compliance program, but every additional system also introduces potential integration, data and workflow challenges.

The number of systems itself is not the issue. What really matters is whether the overall technology environment gives compliance teams a comprehensive view of risk across the firm.





The average organization uses nearly 14 compliance systems

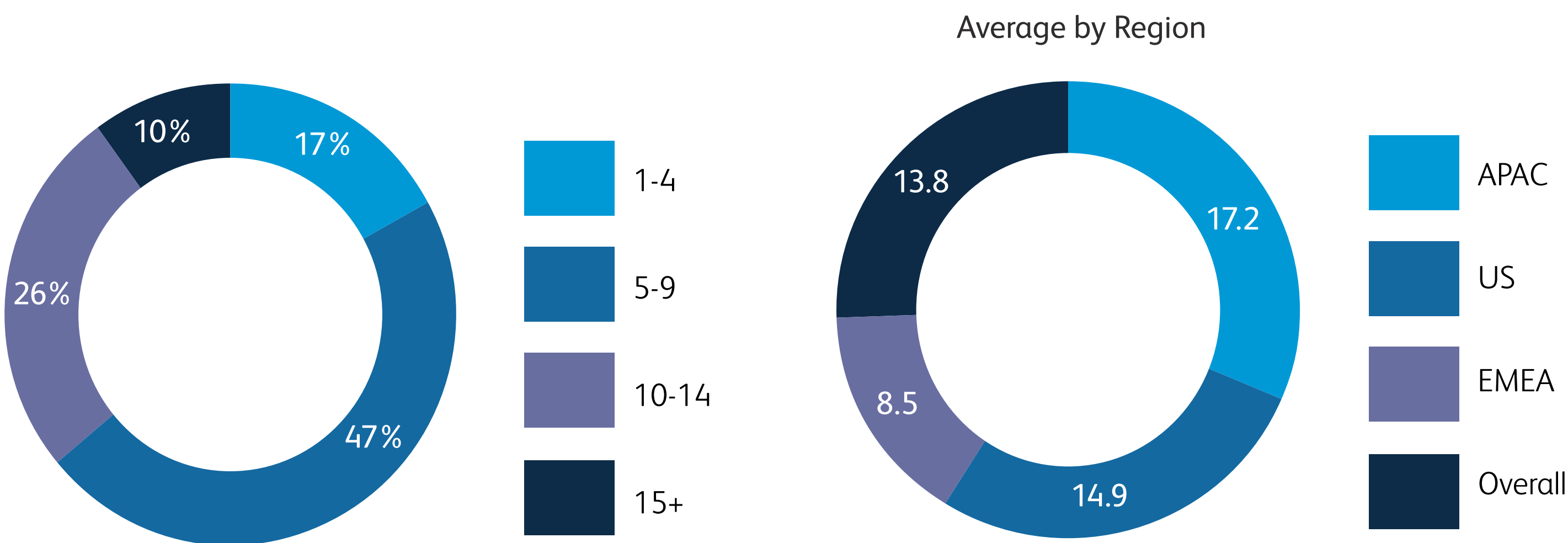
Organizations use 13.8 distinct compliance systems on average.

System sprawl varies by region

APAC respondents report the largest number of compliance systems.

The variation may reflect differences in organizational structure, market coverage, and regulatory demands. Across regions, however, the need is the same: organizations must be able to connect information and controls across the systems they use.

How many distinct compliance systems do you use across your organization?



The Fragmentation Tax

Firms are paying hidden operational and financial costs because surveillance environments remain fragmented.

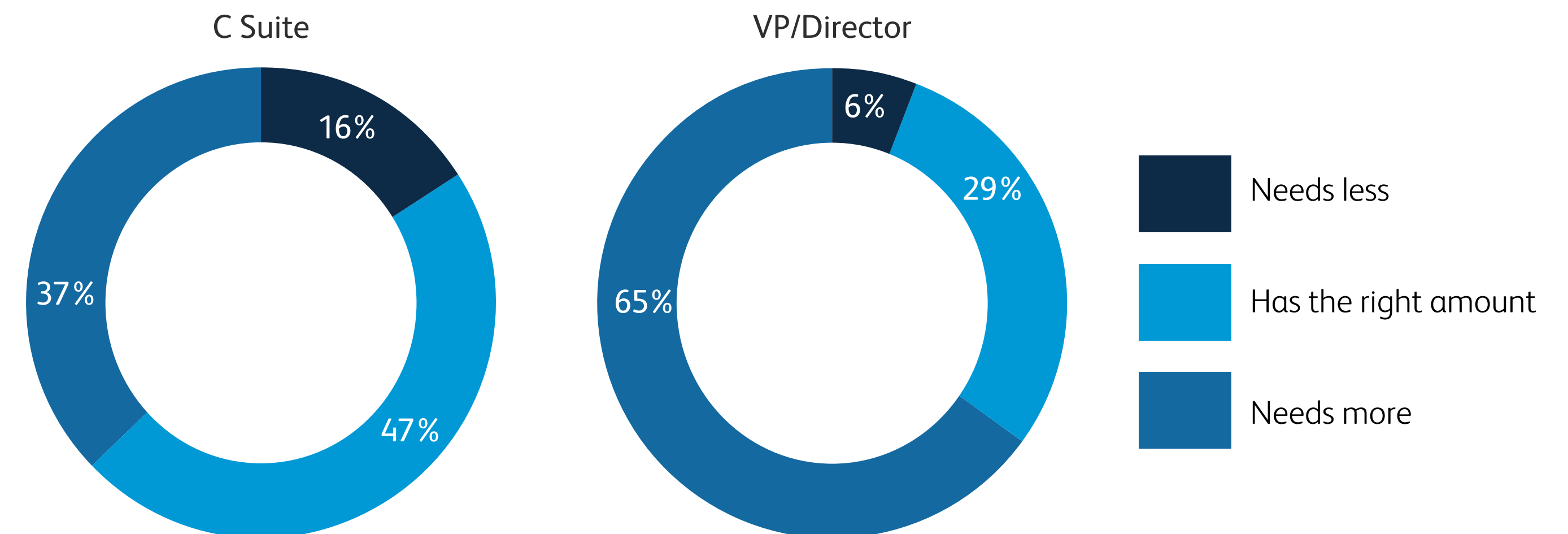
Fragmented systems impose a fragmentation tax: higher operating costs, duplicated effort and greater integration demands, alongside reduced visibility across the compliance program. The cost extends beyond licensing to data extraction fees, overlapping systems, functionality gaps, and the work required to connect technology and processes.

These demands absorb time and resources, complicate the consistent application of controls and make it harder for compliance teams to access a comprehensive view of risk.

Compliance leaders want more technology

Those closer to day-to-day compliance operations report technology gaps nearly twice as often as the C-suite, with 65% of VP's and directors saying their organization needs more compliance technology—and 47 % of the C-suite believing that the organization already has the right amount.

When thinking about your compliance technology, do you feel your organization...?

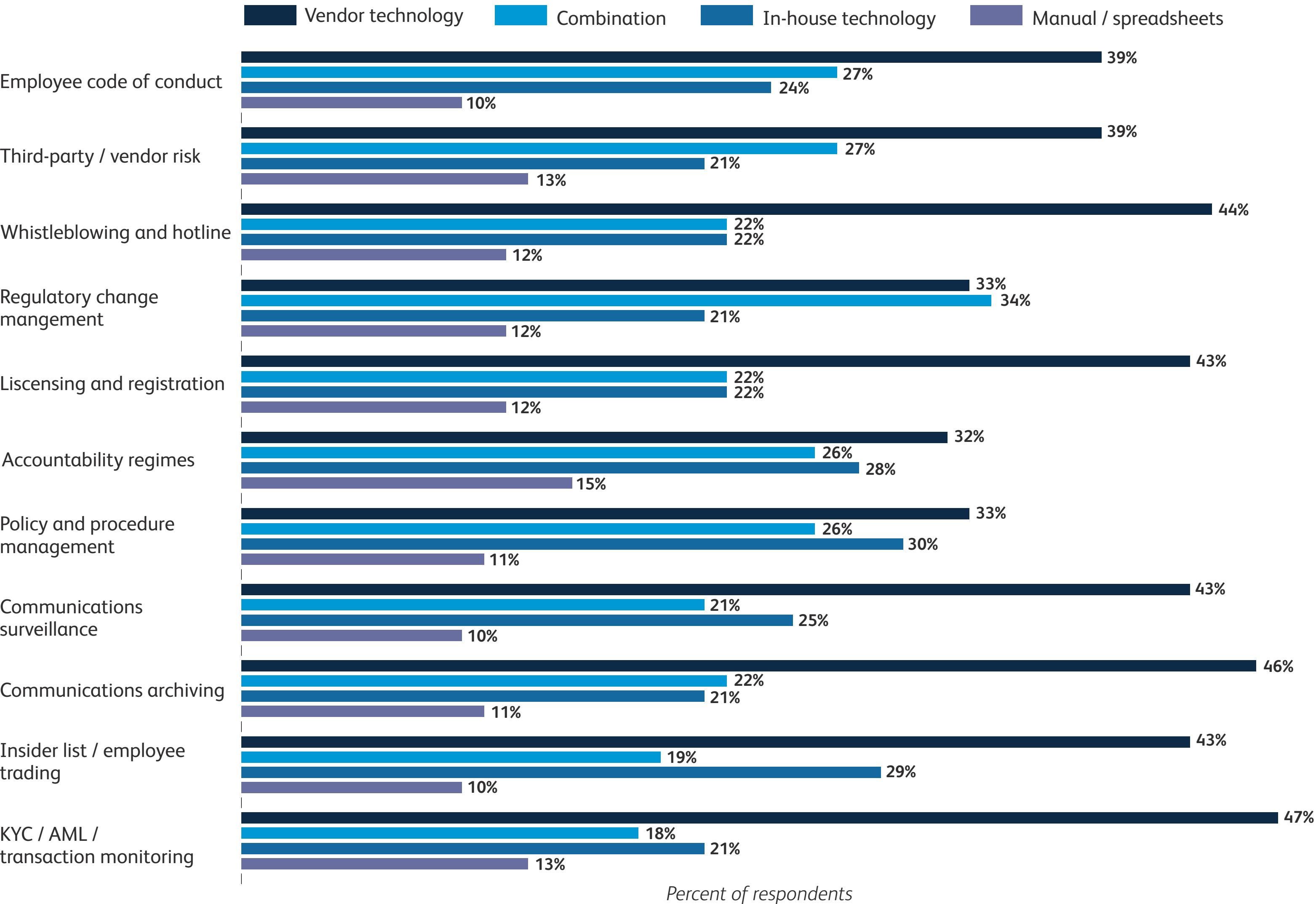


Compliance is being managed by a patchwork of technology

Vendor technology is the most common primary management model across most of the compliance capabilities included in the survey. Yet firms continue to use a wide mix of vendor and in-house technology, manual processes, spreadsheets and combinations of approaches across every area. The pattern remains consistent across types of firm, firm size, and regions.

The result is a fragmented mix of systems and approaches across the compliance program. Firms are juggling vendor platforms, internal tools, and manual workflows across all the different areas of compliance.

For the following capabilities, please indicate how they are primarily managed today



Percent of respondents

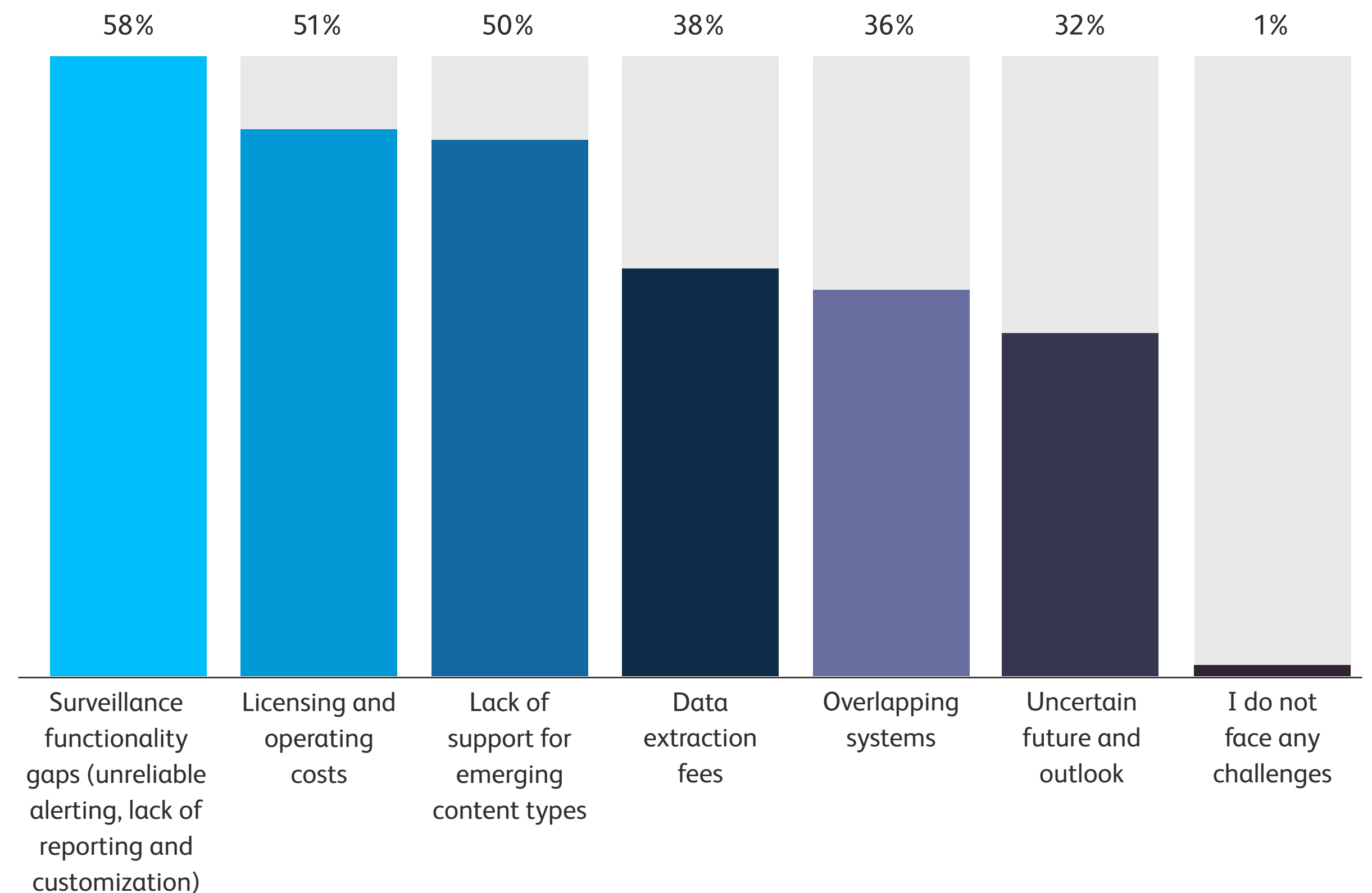
Surveillance is Fragmented

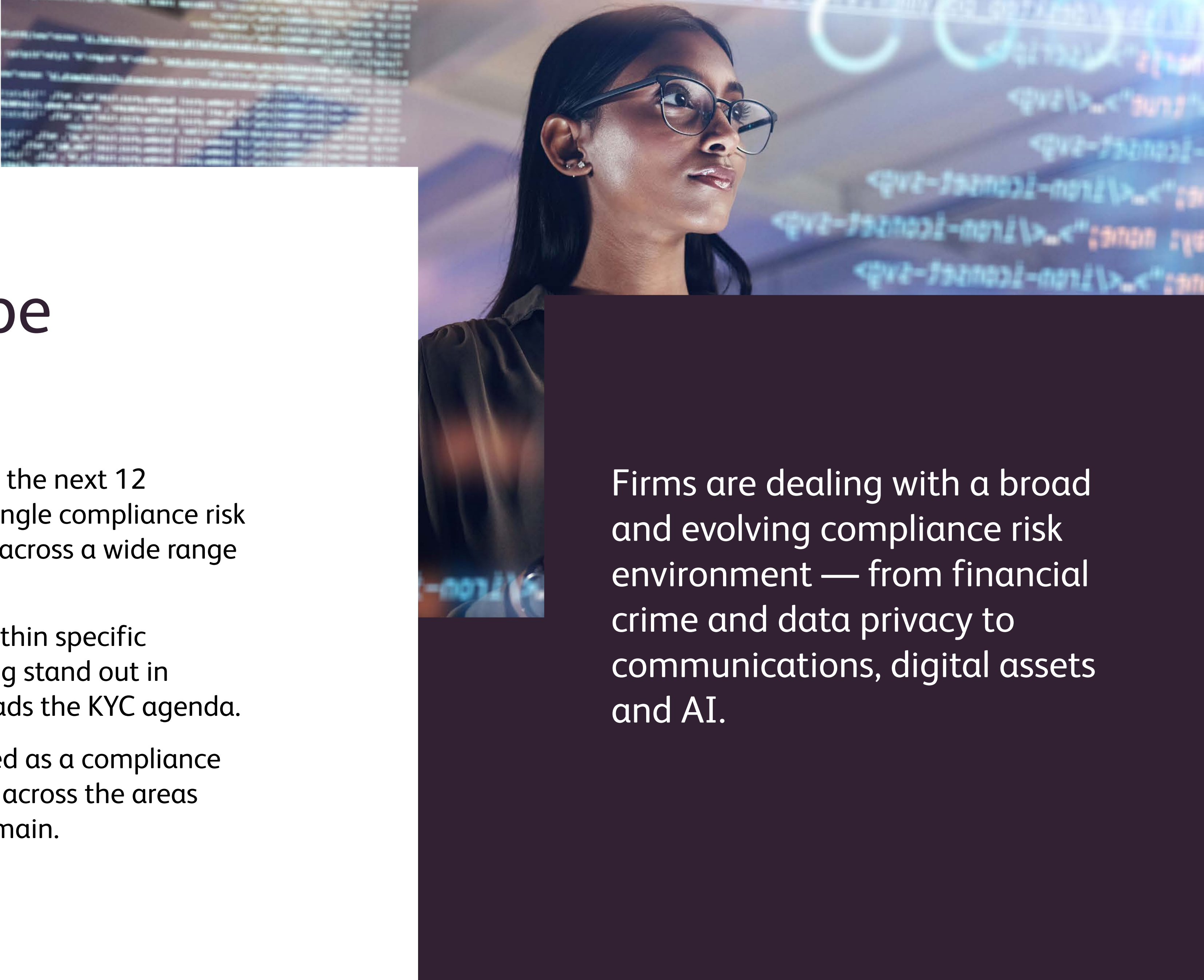
Respondents report a wide range of challenges with their archiving and surveillance providers. Functionality gaps—including unreliable alerting and limited reporting or customization—are cited most often, followed closely by licensing and operating costs and lack of support for emerging content types. Data extraction fees, overlapping systems and uncertainty about providers' future and outlook are also widely reported. With only 1% saying they face no challenges, these issues extend across nearly the entire respondent base.

Surveillance challenges extend across functionality, cost, content coverage, and data access.

Functionality gaps top a long list of surveillance challenges

What challenges, if any, do you face with your current archiving and surveillance providers?





The Varied Landscape of Compliance Risk

Regulatory expectations are set to increase over the next 12 months, according to 90% of respondents. No single compliance risk dominates, however, with responses distributed across a wide range of priorities.

The results also point to the leading priorities within specific areas of compliance. Chat and mobile messaging stand out in communications, while perpetual monitoring leads the KYC agenda.

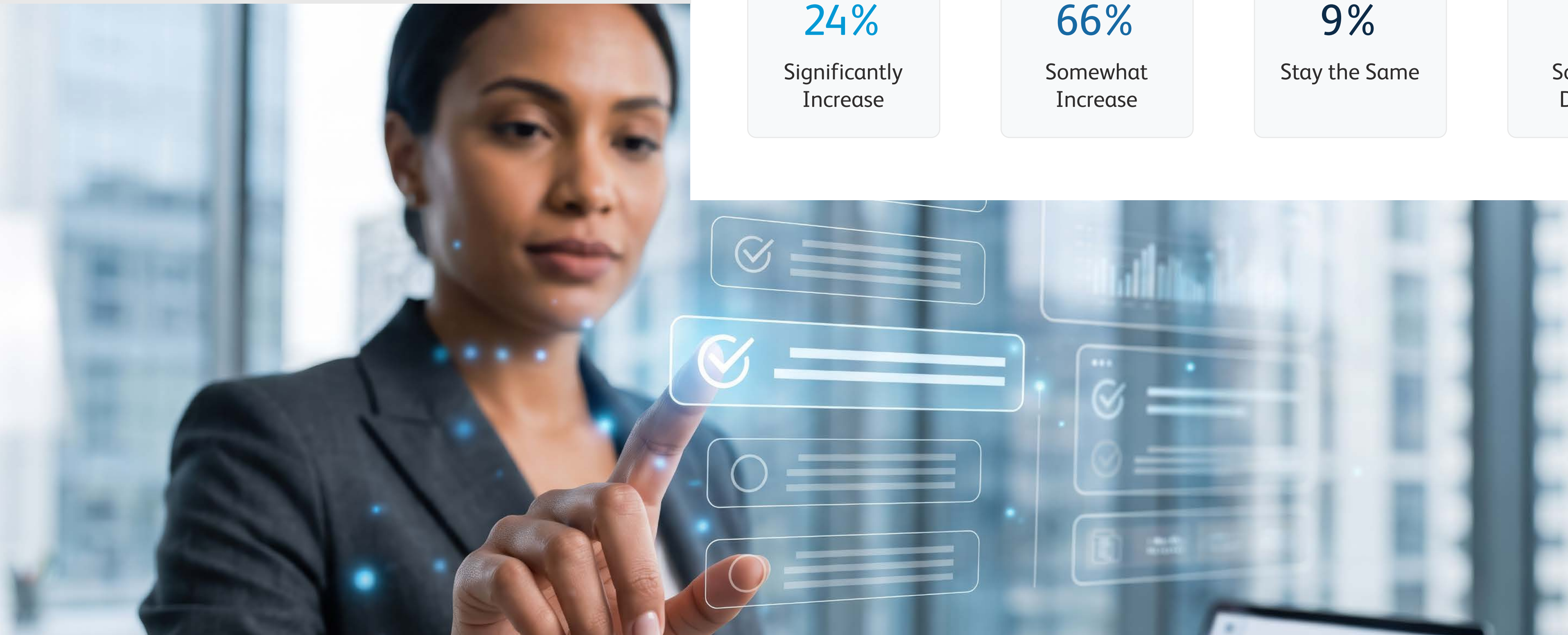
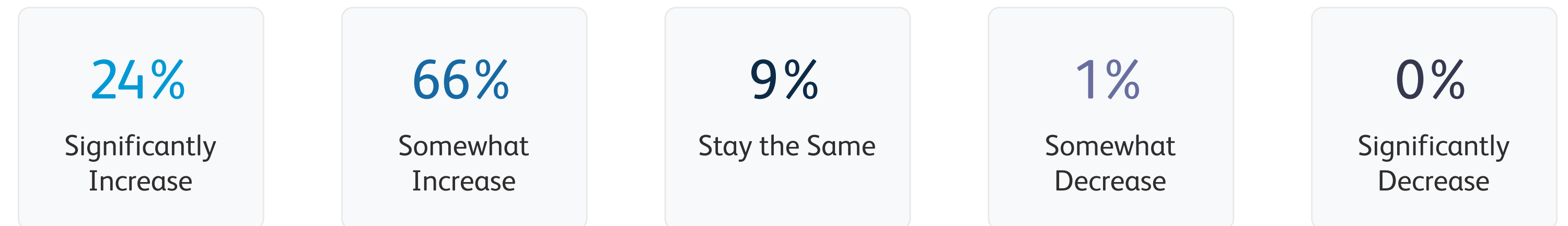
Digital asset compliance is also firmly established as a compliance priority. Most firms have some formal processes across the areas surveyed, but gaps and developing processes remain.

Firms are dealing with a broad and evolving compliance risk environment — from financial crime and data privacy to communications, digital assets and AI.

Regulatory expectations will continue to rise

Nine in ten respondents expect regulatory expectations to increase over the next 12 months.

Over the next 12 months, do you expect regulatory expectations for your organization to...?

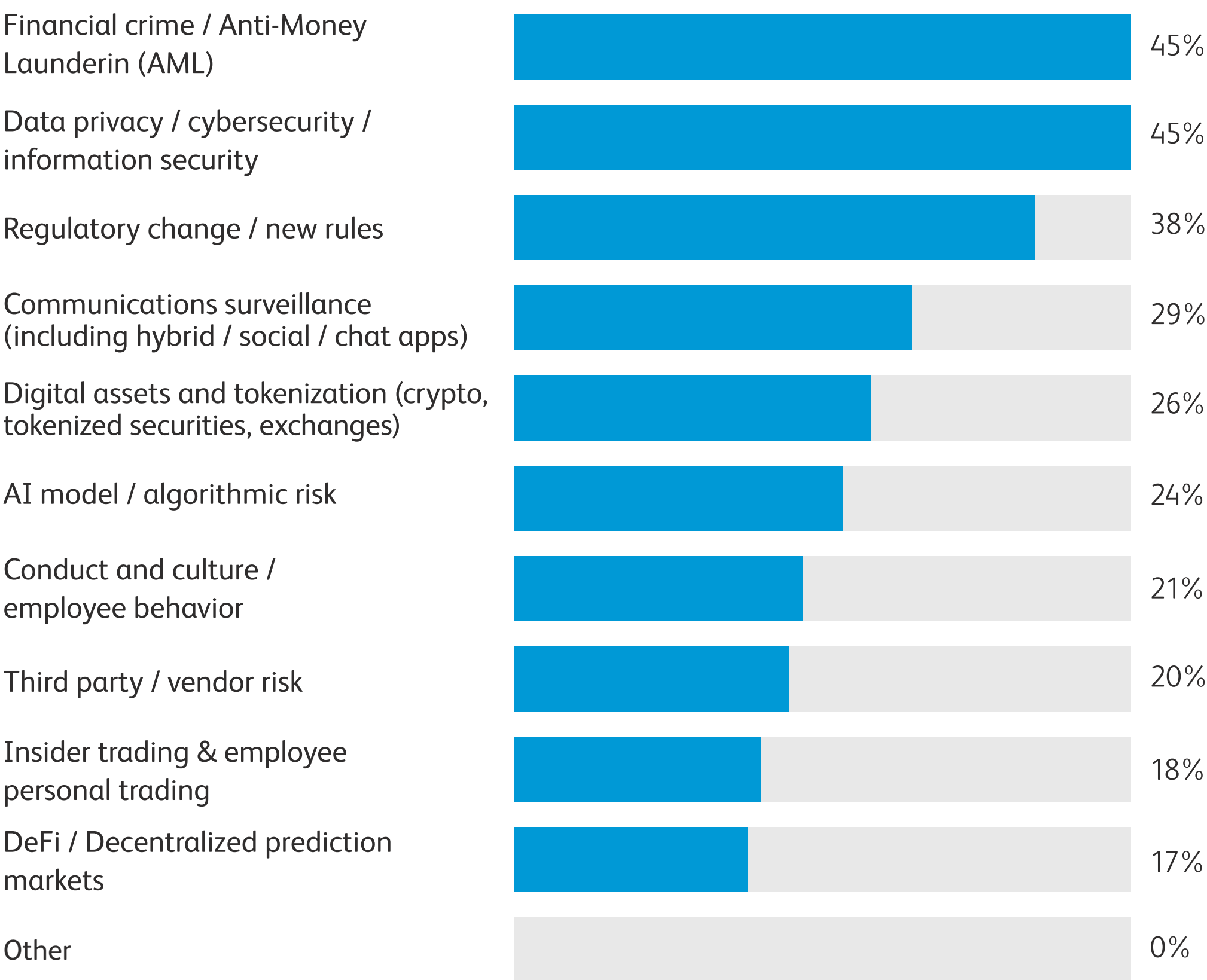


No one area dominates the risk agenda

Financial crime and information security concerns lead the way, each cited by 45% of respondents, but no single area defines the compliance risk landscape. The varied results point to the fact that firms are managing multiple compliance priorities at the same time, spanning regulatory change, communications, technology, employee conduct and third-party oversight.



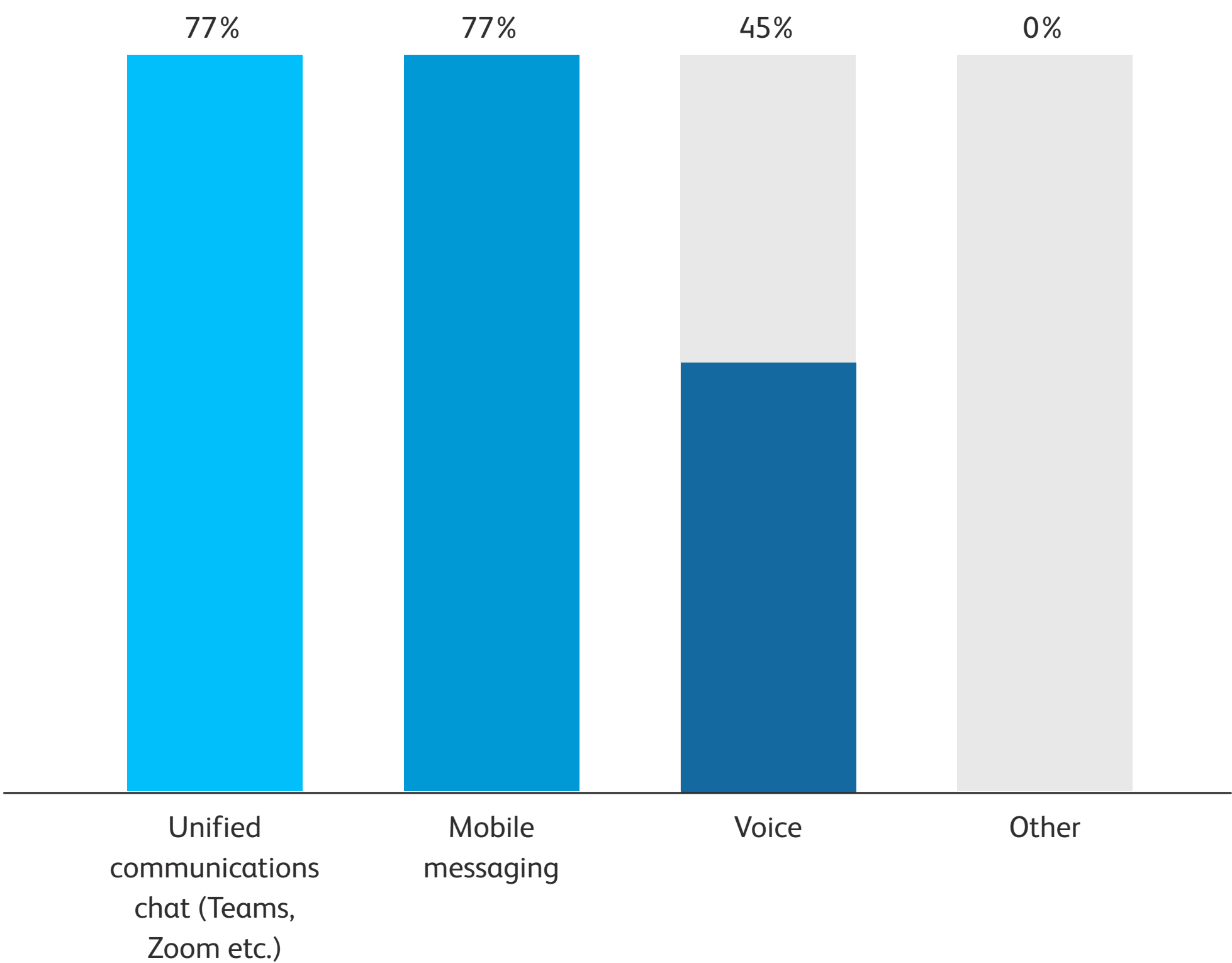
What are the three highest areas of compliance risk for your organization today?



Respondents could select up to 3

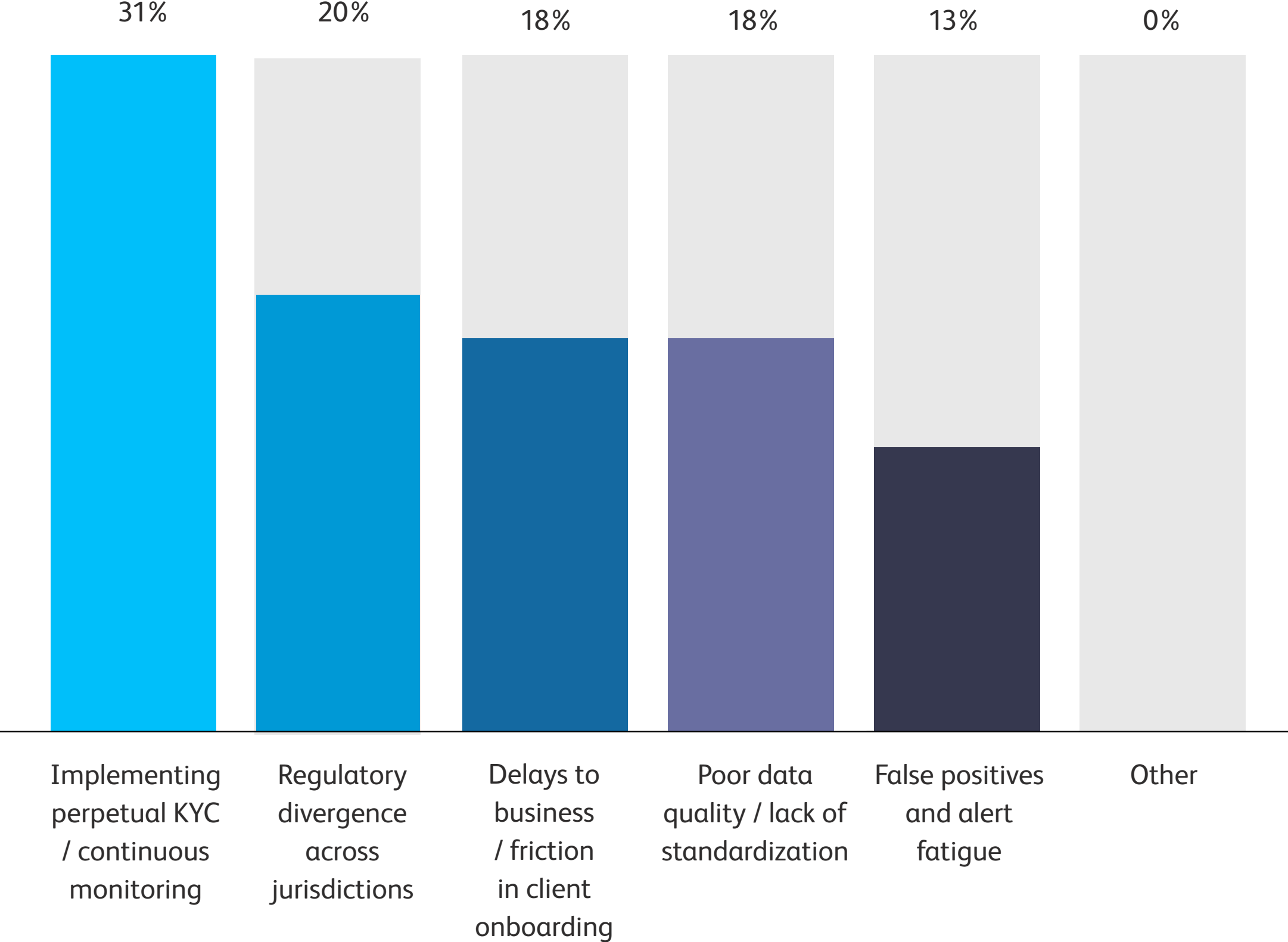
Chat and mobile are communications compliance priorities

Where do you expect focus on communications compliance to increase in the coming year?



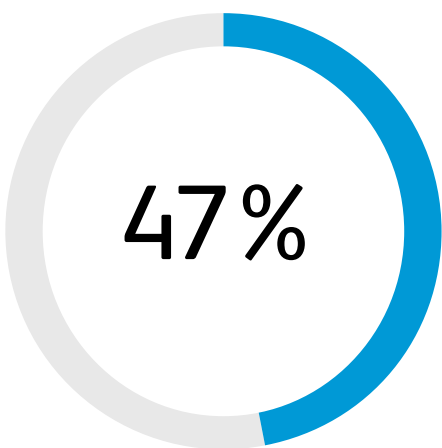
Continuous monitoring is the leading KYC concern

What is the biggest concern facing compliance today regarding KYC?

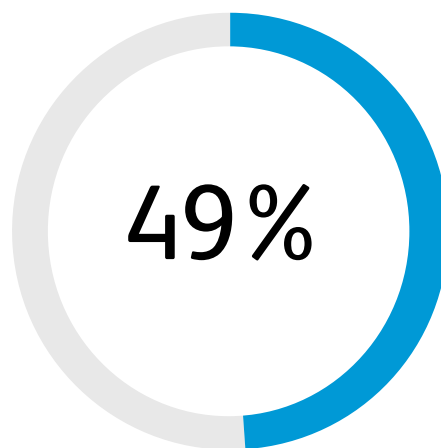


Digital asset compliance is now a mainstream priority

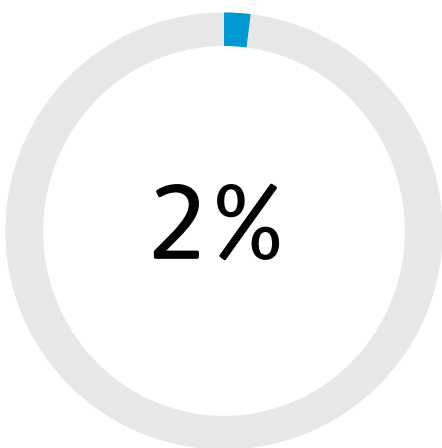
How important is managing compliance related to crypto/digital asset activities for your organization?



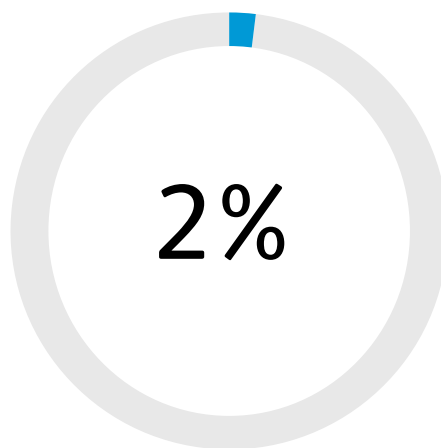
Very Important



Somewhat important



Not very important



Not at all important



Most firms have some digital asset controls in place—but developing processes and gaps remain

Does your firm currently have a formal process in place to manage the following areas related to digital assets?

				
	Yes	No, but in development	No	Not applicable
Employee outside activities / moonlighting in digital assets	68%	25%	7%	0%
Management of insider information regarding digital	67%	28%	4%	0%
AML controls for digital asset transactions	67%	30%	2%	0%
Employee personal trading in digital assets	64%	30%	6%	0%
Tokenized securities / custody & safekeeping	51%	41%	7%	1%

Spotlight On: AI

AI adoption is already broad, and investment is expected to increase, with respondents reporting pilots, enterprise tools, purpose-built vendor solutions and production use across analytics, surveillance and document review. Confidence is high, but so are concerns about explainability, auditability and regulatory uncertainty.

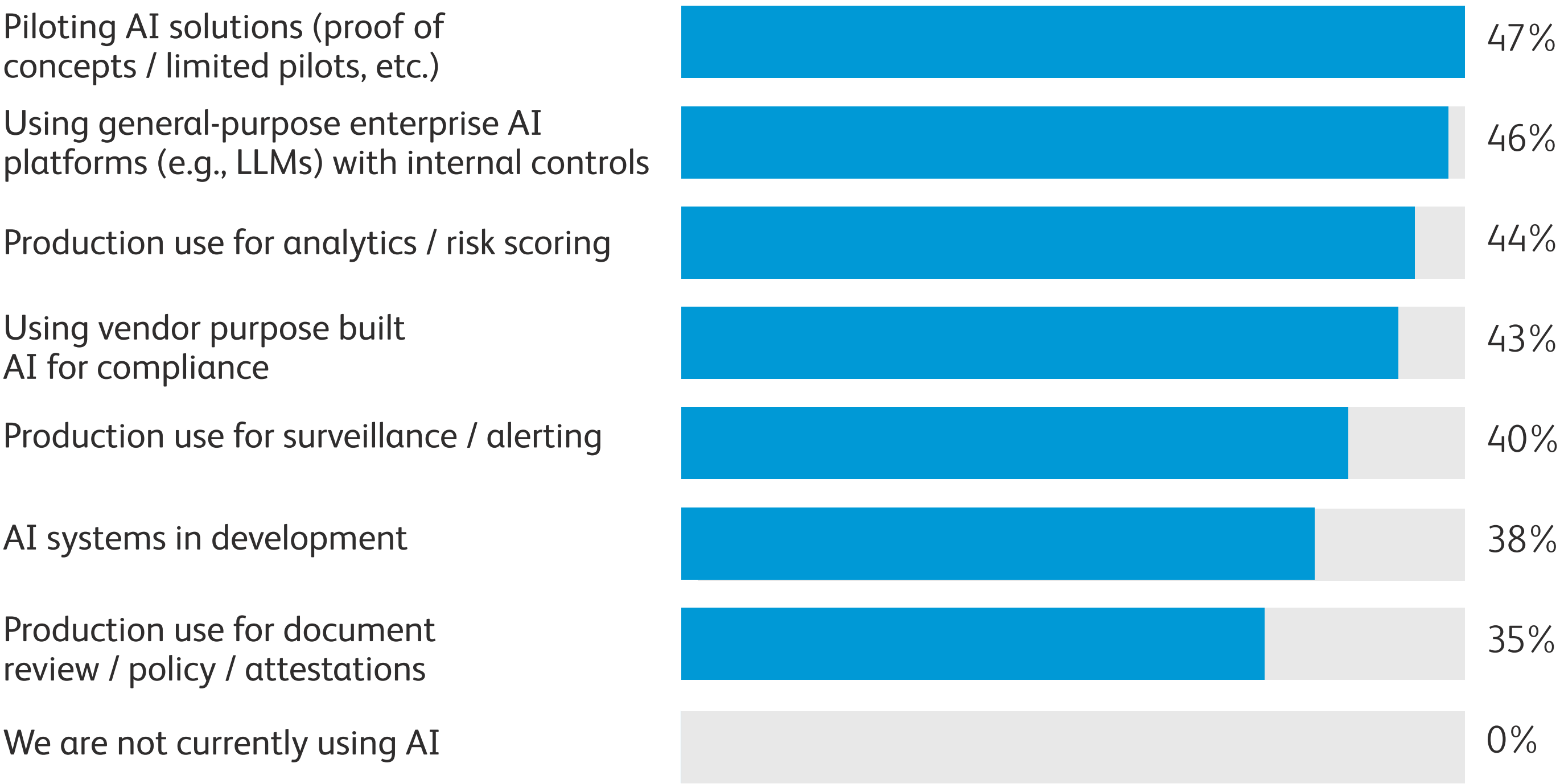
Piloting remains the most common form of use, showing that adoption is still at an early stage for many firms. The results of these pilots—considered with regulatory developments, governance requirements and confidence in the systems already in use—could influence which applications progress to wider deployment and how quickly they scale.

AI has moved beyond experimentation, with production use across analytics, risk scoring, surveillance and alerting, even as explainability and unclear rules remain leading concerns.

AI has moved into production across core compliance activities

AI use spans pilots, enterprise platforms, purpose-built vendor solutions and production applications. No respondents say they are not currently using AI.

How is your compliance program currently using AI, if at all?



Confidence is high —but risks remain concerning

How confident are you in the AI systems your organization is currently using for compliance?



Explainability and regulatory uncertainty are the leading AI risks

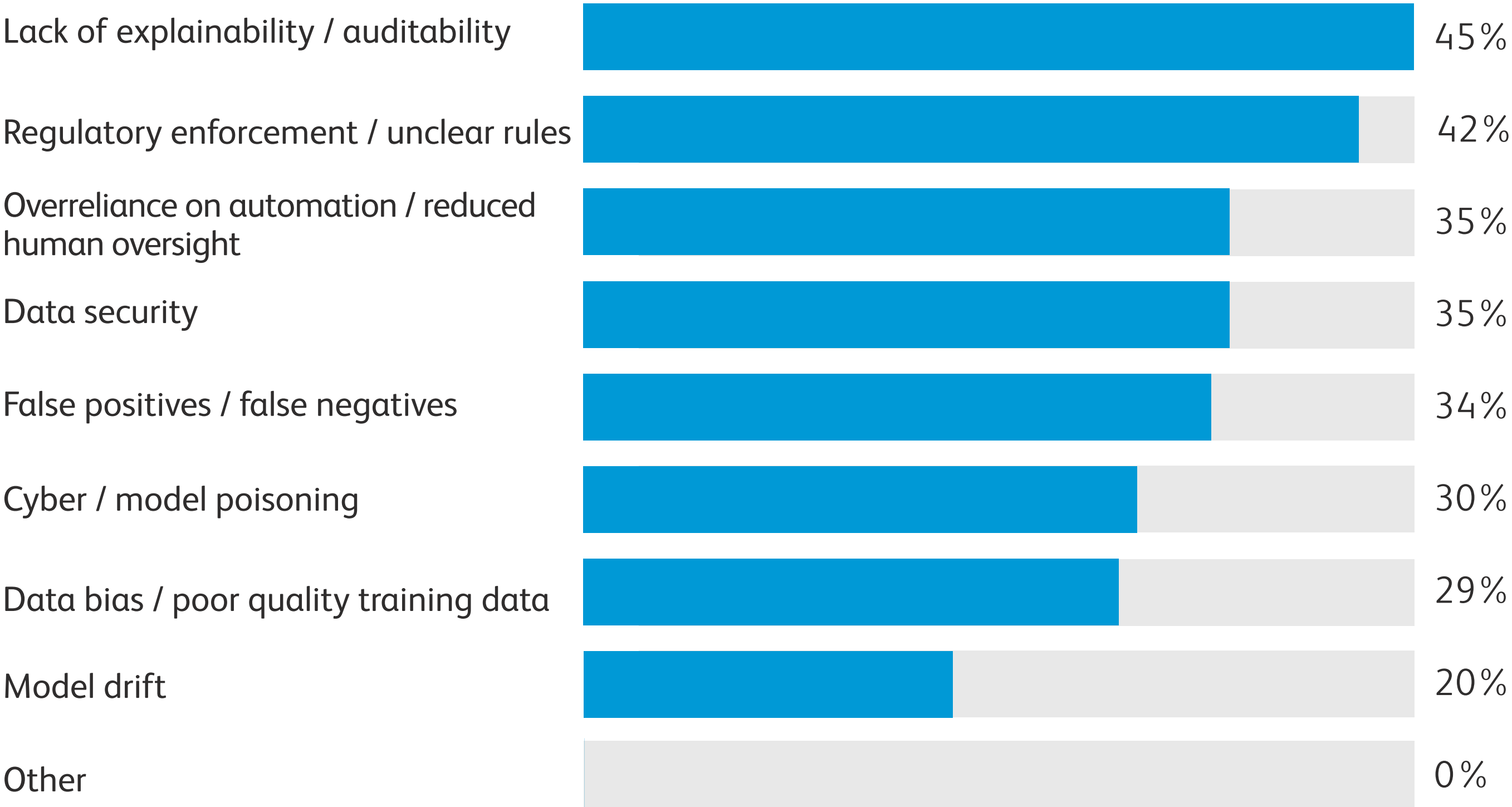
Lack of explainability and auditability is the most frequently cited AI risk at 45%, closely followed by regulatory enforcement and unclear rules. More than one third of respondents report concerns about overreliance on automation and reduced human oversight, data security, and cyber threats or model poisoning.

False positives and false negatives, data bias, and model drift add to the governance challenge. These concerns span the complete AI lifecycle—from data and design to deployment, monitoring, escalation, and review.

AI risk priorities vary by firm type. Capital markets firms are more likely than other financial services firms to cite regulatory enforcement and unclear rules, at 47% versus 33%. Other financial services firms place more focus on data bias or poor-quality training data, cited by 39% compared with roughly one quarter of banks and capital markets firms.



What is among the largest risk to your organization regarding the use of AI in compliance?



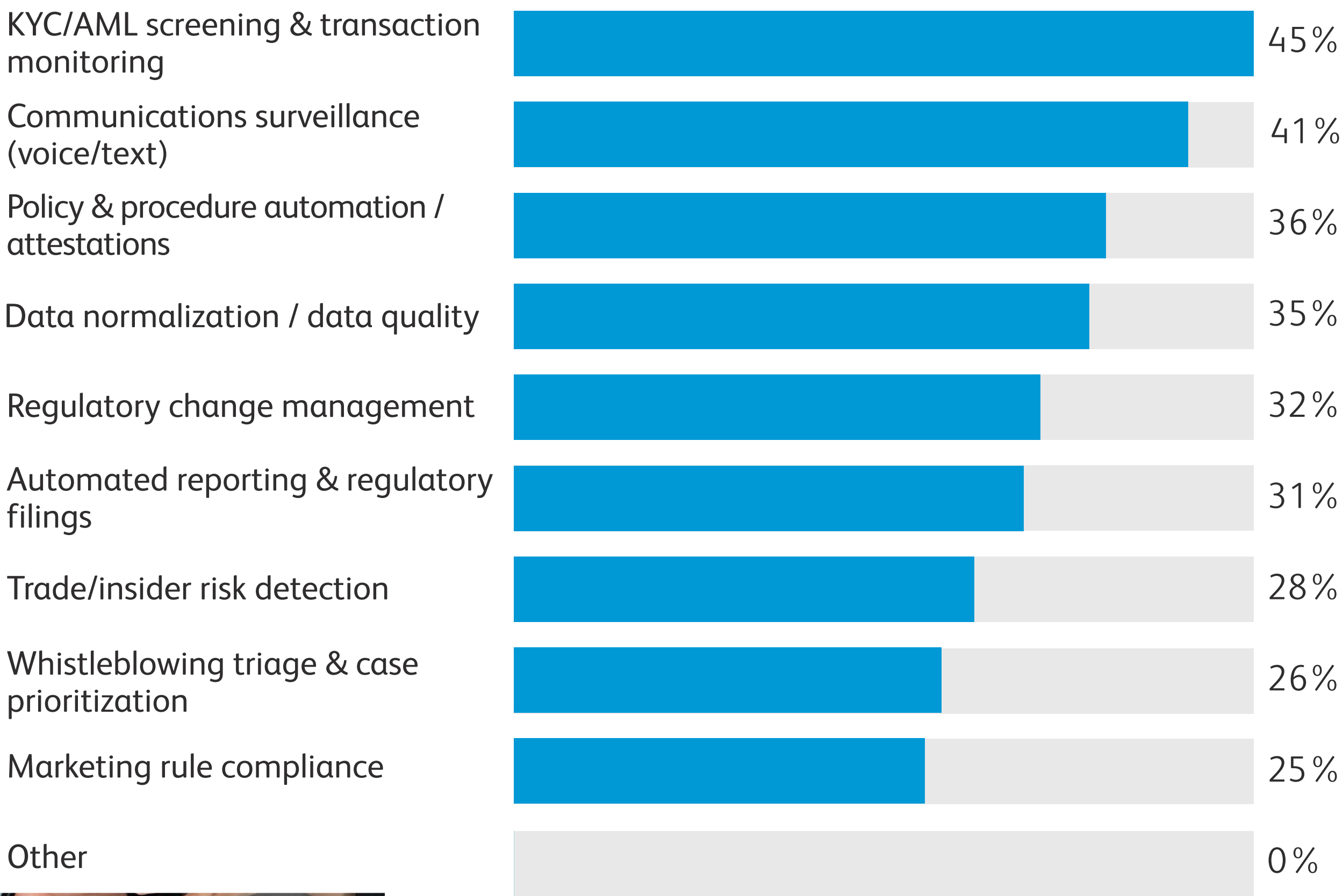
The highest-value AI applications address data-intensive compliance work

KYC and AML screening or transaction monitoring is the most valuable AI application, selected by 45% of respondents, followed by communications surveillance at 41%. Policy and procedure automation or attestations and data normalization or data quality are also among the leading applications identified.

The results point to value across several compliance activities, including monitoring, surveillance, policy management and data quality, that combine volumes of data with the need for prioritization and review.



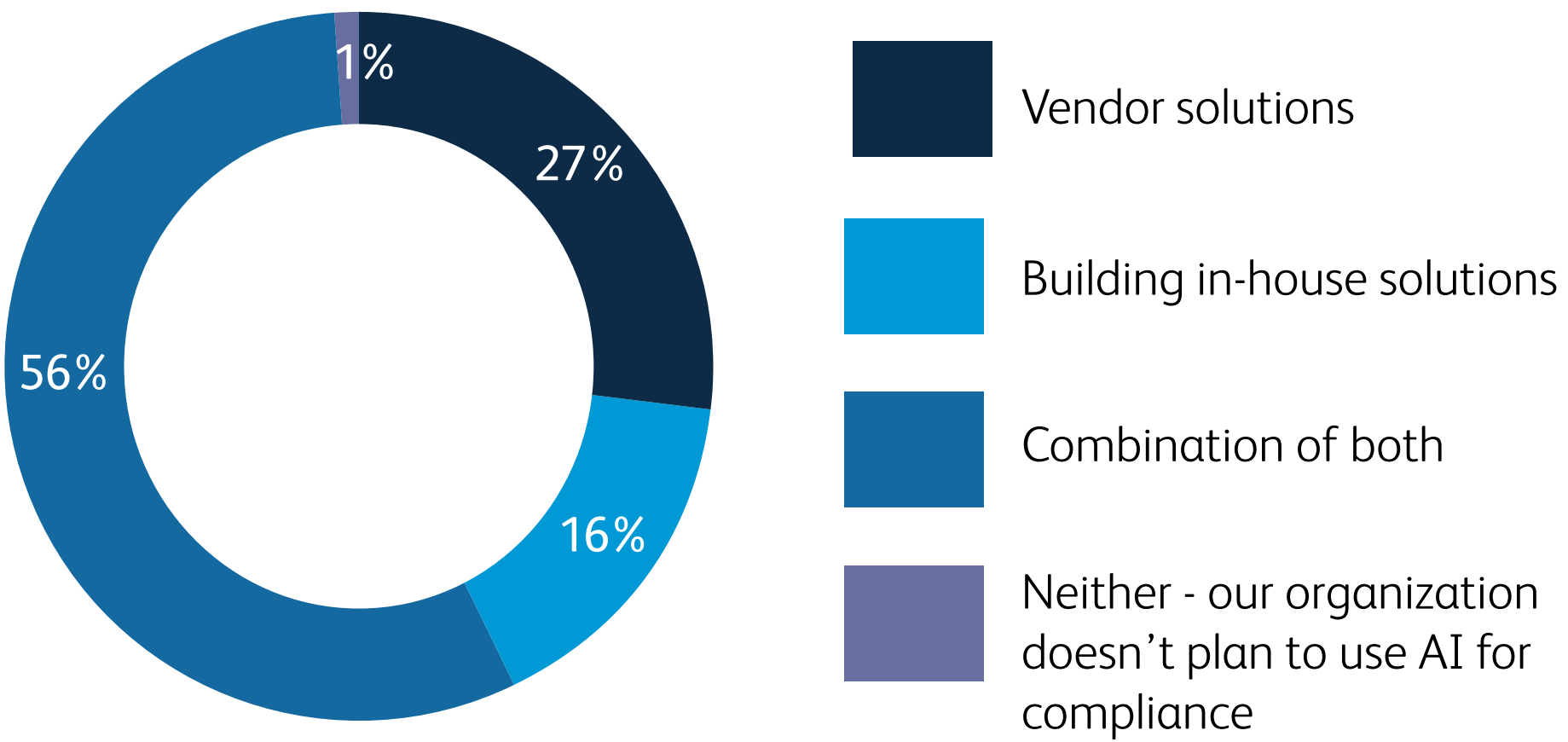
Which applications of AI do you consider most valuable for compliance in your organization?



Most organizations expect a hybrid AI strategy

A hybrid approach using both vendor and in-house technology allows firms to combine internal knowledge and control with specialist capabilities, but it can also add to the fragmentation tax across the compliance program.

When thinking about AI for your compliance program, does your organization plan to invest in...?



Conclusion

The executive outlook is one of continued expansion for compliance: higher expectations, more investment, a broader risk agenda and growing use of AI.

Compliance functions are not standing still. They are adding capabilities and preparing for a more strategic role in the business.

The central challenge is that growth in capability has also produced complexity. A compliance function operating across nearly 14 systems on average cannot improve simply by adding another point solution. Leaders need to consider how technology, data and workflows connect across the program—and whether each investment strengthens the whole operating model.

Priorities for the rest of 2026 and beyond

As you reflect on these priorities, consider how they apply to your own organization and where further discussion may be valuable.

1. Align investment to the future role of compliance. Direct budget toward the technology and data that help the compliance executive provide timely, risk-based advice to the business.

Questions to consider

- Are our investment priorities aligned with the future role we expect compliance to play?
- Which investments will create the greatest long-term value for both compliance and the wider business?
- How will we measure whether these investments are delivering the outcomes we expect?

2. Reduce fragmentation across systems and processes. Evaluate new capabilities in the context of the wider compliance environment, including integration, data access, reporting, and user experience.

Questions to consider

- Where are disconnected systems creating operational inefficiencies or limiting visibility?
- Are we simplifying the compliance operating model or increasing complexity over time?
- How easily can our teams access and trust the information they need?

3. Address the full cost of surveillance. Look beyond licensing to consider functionality gaps, overlapping systems, emerging content coverage, the cost of extracting and moving data, the potential risks that separate systems may fail to surface, and the ability to provide proof of compliance when regulators require it.

Questions to consider

- Have we assessed the total cost of surveillance beyond software licensing?
- Where do manual processes or fragmented data introduce hidden costs or unnecessary effort?
- Are our surveillance capabilities keeping pace with evolving technology and regulatory expectations?

4. Apply consistent and holistic controls across a broader compliance risk landscape. Connect oversight of communications, employee activity, financial crime, and other areas where information and behavior intersect.

Questions to consider

- Where are risks still managed in silos?
- How effectively are data and controls shared across compliance functions?
- Could a more integrated approach improve visibility and reduce operational risk?

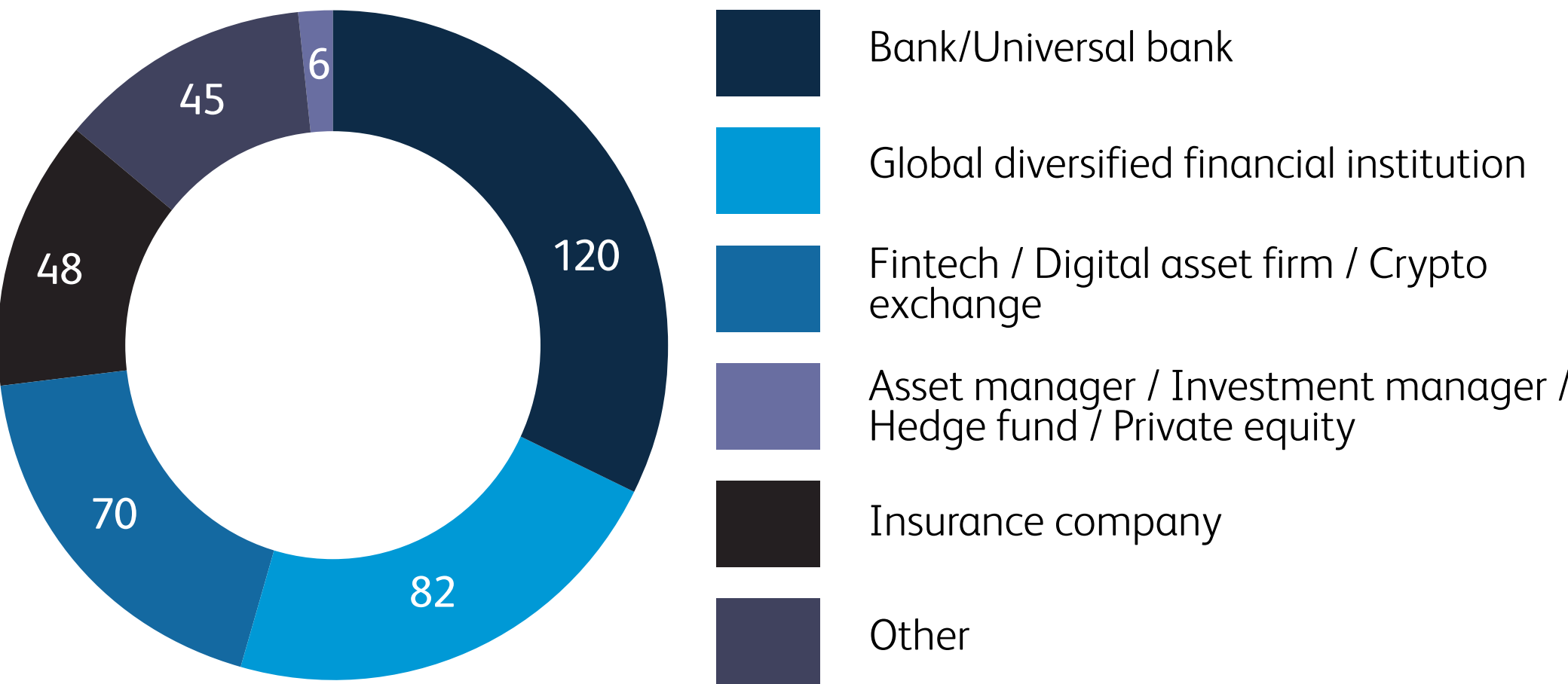
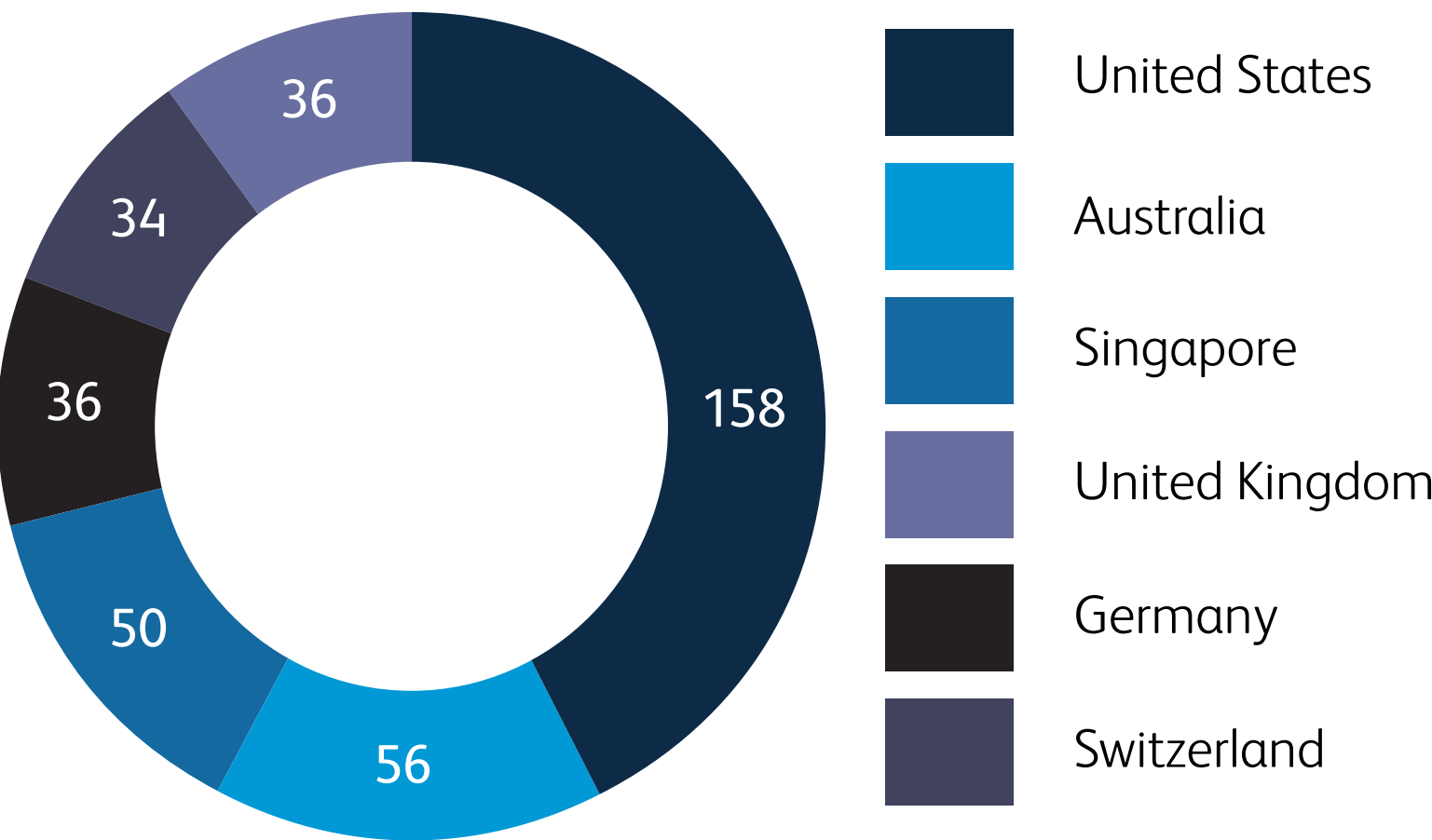
5. Establish accountability, explainability, auditability, human oversight and ongoing monitoring across vendor, in-house and hybrid AI models.

Questions to consider

- Do we have appropriate governance for every AI capability used within compliance?
- Can we explain and evidence how AI-supported compliance decisions are made?
- Are our governance frameworks evolving as quickly as our AI adoption in our compliance program?

Respondents and Methodology

Survey Participants



Method Statement



This research was conducted online by The Harris Poll on behalf of MCO (MyComplianceOffice) among 370 compliance professionals in three markets: the U.S., Europe (U.K., Germany, and Switzerland), and APAC (Australia and Singapore). Participants were aged 21+, employed full-time within the governance, risk, and compliance departments of financial services companies with at least 500 employees, and had at least a director title and some level of input in compliance-related decisions.

Data are weighted to reflect company size (based on number of employees) in line with their actual proportions within each of the three markets. Respondents are selected among those who have agreed to participate in our surveys. The sampling precision of Harris online polls is measured by using a Bayesian credible interval. The data is accurate to within + 5.1 percentage points using a 95% confidence level. This credible interval will be wider among subsets of the surveyed population of interest.

All sample surveys and polls, whether or not they use probability sampling, are subject to other multiple sources of error which are most often not possible to quantify or estimate, including, but not limited to coverage error, error associated with nonresponse, error associated with question wording and response options, and post-survey weighting and adjustments.

About MCO

MCO is a global leader on a mission to revolutionize how financial firms tackle compliance, making it simpler, smarter, and more effective. The MyComplianceOffice platform unifies compliance into a single, seamless view, empowering firms to monitor risks, identify conflicts, and maintain compliance across systems and departments.

MyComplianceOffice lets compliance professionals demonstrate they are proactively managing the regulated activities of the company, employees and third parties and provide evidence of regulatory compliance.

The MyComplianceOffice platform brings together key compliance functions, including employee compliance, communications compliance, transaction surveillance, third-party risk management, KYC/AML, and

compliance program management, on a single platform with shared data. By providing a consistent and integrated approach across compliance activities, MyComplianceOffice helps firms reduce operational fragmentation, improve strategic visibility into risk, and demonstrate compliance across the enterprise.

The organizations best positioned for the next phase of financial services compliance will align their technology investments to create a more data-driven and centralized compliance function—one that can meet regulatory expectations while enabling compliance executives to strategically move business the forward.





MCO (MyComplianceOffice) provides compliance management software that enables companies around the world to reduce their risk of misconduct and effectively oversee regulatory obligations.

Our powerful platform lets compliance professionals demonstrate they are proactively managing the regulated activities of the company, employees and third-party vendors and provide evidence of regulatory compliance. Available as a unified suite or à la carte, our easy-to-use and extensible SaaS-based solutions get firms up and running quickly and cost-efficiently.

mycomplianceoffice.com | © 2026 MCO (MyComplianceOffice)® | advance@mycomplianceoffice.com

