Survey Results

2025 AI Benchmarking Report

Contents

Introducing the 2nd Annual AI Benchmarking Survey

> AI adoption across the financial services landscape has accelerated dramatically over the past year.

The pace of AI adoption across the financial services landscape has accelerated dramatically over the past year. From research and investment diligence to compliance monitoring and oversight, AI is reshaping how firms operate and compete. Yet, despite the momentum, many organizations remain uncertain about how their peers are applying AI, the challenges and risks it introduces, and how these tools may improve efficiency and effectiveness.

To address this uncertainty and provide guidance to the industry, ACA and the National Society of Compliance Professionals (NSCP) conducted our second annual AI Benchmarking Survey. Gathering responses from compliance leaders across the financial services industry, this year's survey offers a deeper, more nuanced view on how strategies have evolved in the past year. The findings of our survey reflect both growing maturity in the use of AI tools, and opportunities for firms to improve their risk management and compliance practices regarding AI. It also speaks to persistent challenges, particularly around model transparency, data governance, and talent acquisition.

Ultimately, this report aims to provide a practical reference point for firms seeking to benchmark their own AI journeys. Whether leading innovation, managing compliance, or shaping strategic direction, the insights in this report can help inform decision-making and foster a more forward-looking dialogue across the industry.

Carlo di Florio

President
ACA Group

About the Survey

The results in this report are based on responses from 244 individuals to ACA's online AI Benchmarking Survey. Data was collected in September 2025 from firms that are either ACA clients or members of the NSCP. Most respondents represent financial services firms, particularly those in asset management firms and private markets. Additional respondent details are provided in the Appendix.

Throughout this report, you will also see references to the **2024 ACA and NSCP AI Benchmarking Survey**. That survey, conducted in July 2024, includes responses from 219 individuals, with a demographic profile closely aligned with the 2025 survey data.

Defining AI

For the purposes of this survey, respondents were asked to use the following definitions for AI and AI-related technologies.

Artificial Intelligence (AI) – Technology that enables computers and machines to simulate human intelligence and problem-solving capabilities.

Generative AI (Gen AI) – A type of AI that uses machine learning techniques to generate new content that appears like the data it was trained on. These tools can be used to create totally new text, audio, and images that will mimic the underlying patterns of the dataset.

2025: The Year of Accelerated AI Integration

In just one year, financial services firms have dramatically shifted their approach to AI, from cautious exploration to rapid, formal adoption of AI tools and technologies. Between 2024 and 2025, the number of firms using AI jumped by 20 percentage points, with 71% of firms now reporting formal AI use. This surge in AI adoption is likely due to a variety of factors, including greater availability and comfort with AI-powered tools and technology, and shifts in regulatory focus and priorities. AI adoption creates a wide range of opportunities for firms to operate more efficiently than ever before, while also introducing new risks that must be managed.

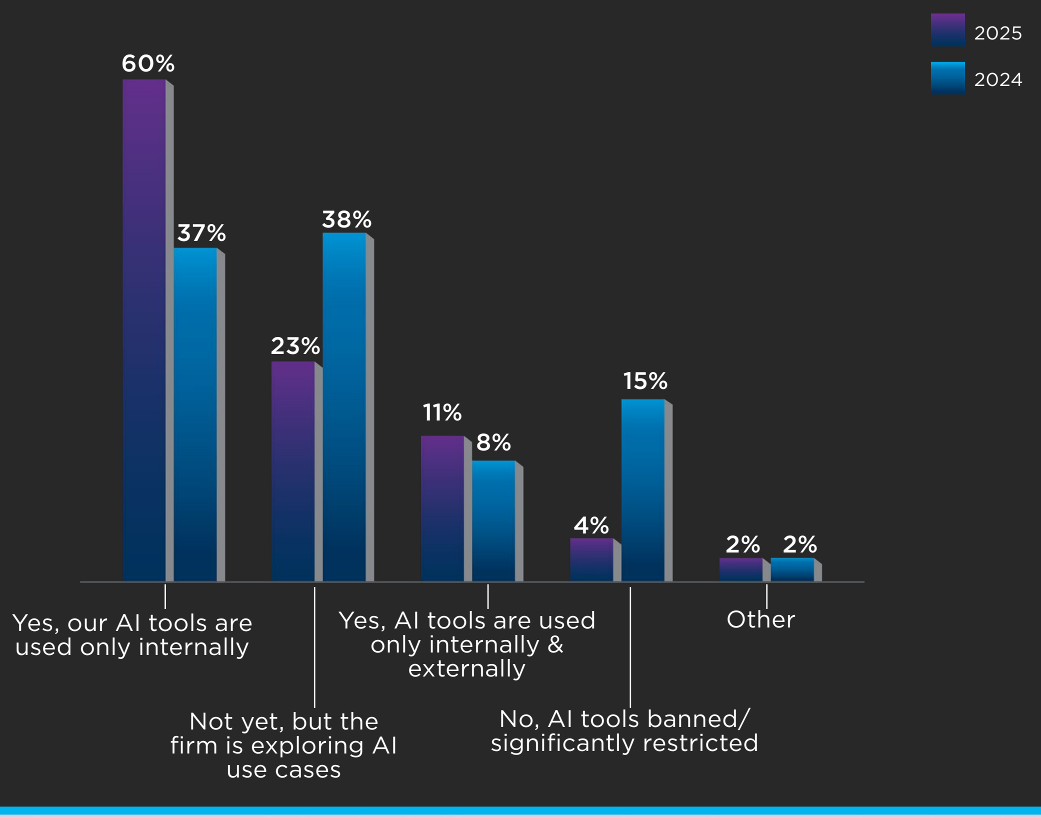
In this chapter, we examine how financial services firms have expanded their use of AI tools and technologies over the past year, including the most common use cases across the firms and within compliance, as well as how much firms are typically investing in AI tools.

From Exploration to Implementation

During 2024, financial services firms were in the early stages of AI adoption and exploration, with 38% of firms exploring AI use cases and 37% using it for internal use cases only. Within a year, AI use by financial services firms had expanded dramatically, with a significant increase in the number of firms that use AI for internal use cases (60%) as well as firms using AI for both internal and external use cases (11%).

Firms are becoming more comfortable with AI tools, as the percentage of firms that had imposed bans or significant restrictions has dropped to just 4%.

Does your firm use AI?



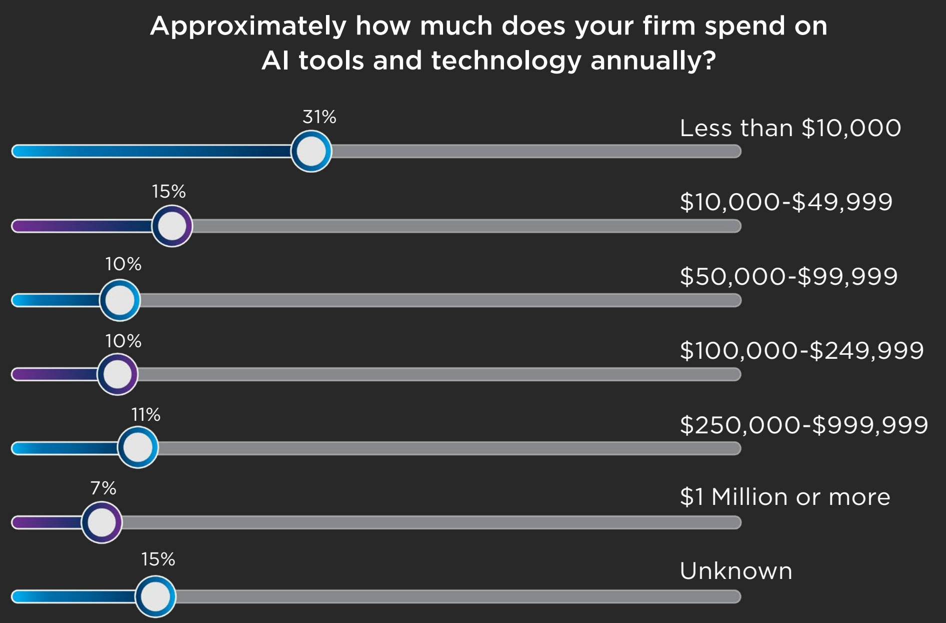
While firms are getting more comfortable with AI use, similar to 2024, only a small percentage of firms use it in client-facing interactions. While this has increased slightly from 2024, firms are still hesitant to use AI to directly interact with clients, likely due in part to limited regulatory guidance around these tools.

It is also worth noting that a firm's size has an impact on the firm's AI adoption decisions.

Firms that manage under $1 billion (USD) in AUM have the lowest rate of AI adoption with only 42% of firms formally using AI for internal use cases, 10% using AI for internal and external use cases, and 13% of those firms banning AI tools. In contrast, firms with between $20 billion and $50 billion in AUM have the highest rate of AI adoption, with 78% of firms using AI for internal use cases, and another 14% using AI for internal and external use cases, meaning that 92% of firms of this size are formally using AI.

A firm's decision to formally adopt AI tools and technology will vary based on the risks and opportunities the firm associates with this technology. These differences in adoption rates are likely due, in part, to larger firms feeling more confident taking the risk and/or seeing the potential upsides of AI outweighing these risks. Additionally, larger firms often have the practical advantage of being more willing or able to bring additional resources to help with AI for adoption. From additional budget to more staff with the technology skills to maximize the value of AI tools, larger firms are better positioned to adopt AI technologies.

As the next graph demonstrates, the amount firms are spending on AI tools and technology varies significantly. While firms spending less than $10,000 annually is the most common (31%), the percentage of firms spending between $10,000 and $49,999 annually is very similar to the percentage of firms spending between $250,000 and $999,999 annually.

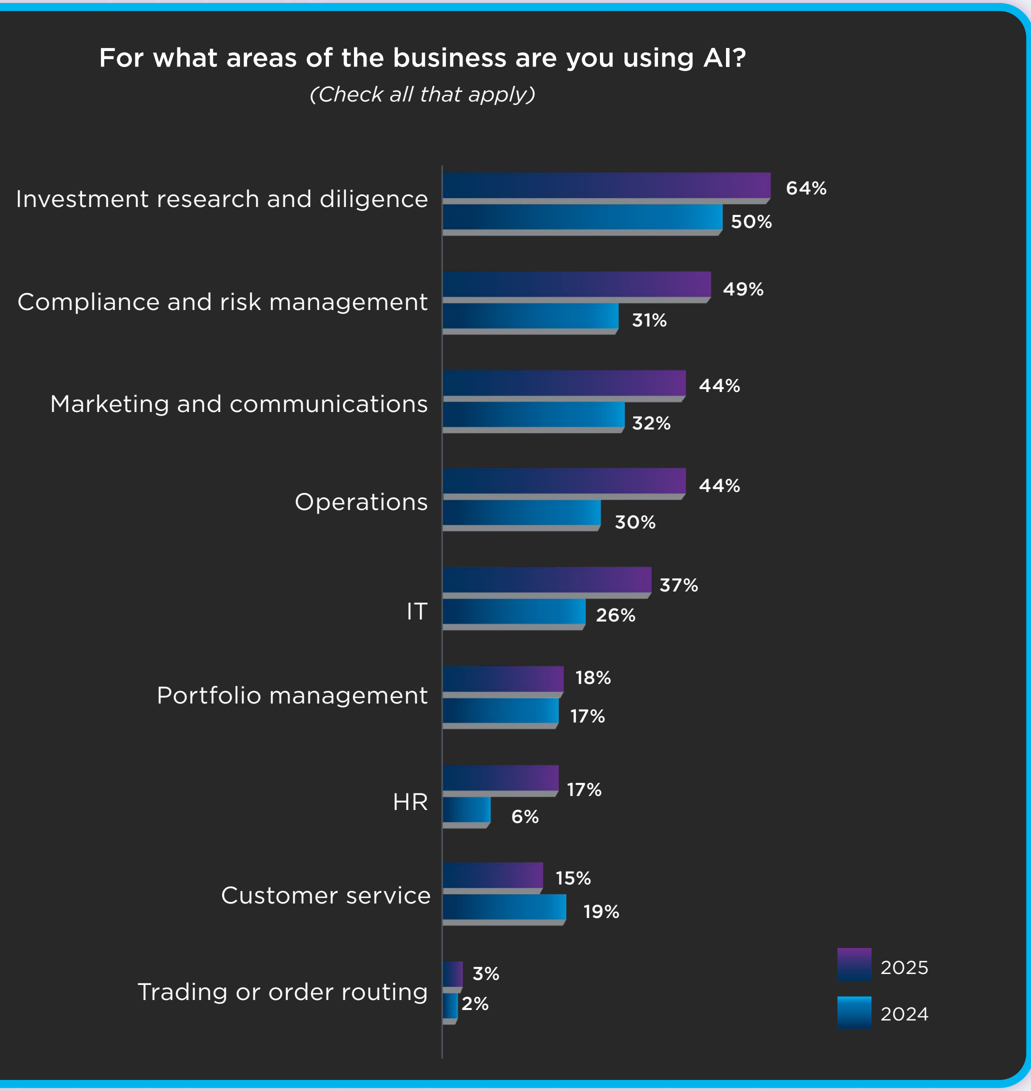


It is important to note that this data excludes firms who have not yet formally adopted AI and respondents were asked to include all costs associated with AI tools, including costs associated with AI tool purchases and licensing, AI tool development, and AI monitoring and oversight.

When this data is again segmented by the firm's AUM (again, excluding firms that have not formally adopted AI), we see that larger firms are much more likely to have higher AI-related spending than smaller firms. 63% of firms under $1 billion in AUM spend less than $10,000 annually on AI, significantly lower than the overall average and much lower than firms with larger AUMs. In fact, for firms with more than $10 billion in AUM, only 6% spend less than $10,000 annually on AI.

Common AI Use Cases

Not only has the volume of firms formally adopting AI increased since 2024, so has the number of tasks that firms are using AI-powered tools to complete.



Aside from customer service, all AI use cases included in our survey are more common in 2025 than in 2024. Use cases related to investment research and compliance and risk management have seen significant increases in the percentage of firms using AI to assist in this work, a 14-point and 18-point increase, respectively.

For compliance leaders, AI is helping them engage in activities that often require manual work or significant amounts of time to complete. These include:

- Developing policies and procedures (53%).
- Monitoring and testing activities (48%).
- Employee communications and training (46%).
- Employee surveillance (41%).

Beyond these use cases, a small percentage of firms are using AI tools for compliance work that falls outside typical automation or repetitive tasks (e.g., investigations, discipline). These areas generally require human oversight and review to ensure accuracy and sound judgment.

Conclusions

As financial services firms continue to embrace AI, the pace and scale of adoption reflect a broader shift in their comfort with these tools. While firms in 2024 were cautiously exploring AI, 2025 shows that firms are rapidly integrating the technology. While larger firms are leading the way in terms of investment and implementation, the growing comfort with AI tools across the industry signals a maturing landscape. With use cases expanding and spending increasing, firms are not only unlocking new efficiencies, but also confronting new challenges around oversight, governance, and risk. These challenges, which will be addressed further in the report, need to be actively managed by firms, and as the 2025 AI survey data indicates, firms are making meaningful strides addressing these challenges.

The Evolution of AI Risk Management

The rapid adoption of AI tools across the financial services industry has provided firms with new opportunities to work more efficiently and effectively. However, AI technologies also bring unique risks and challenges that firms must manage. From information security and privacy risks to hallucinations and model drift, AI tools present chief compliance officers (CCOs) and cybersecurity and technology leaders with a wide range of risks that must be addressed.

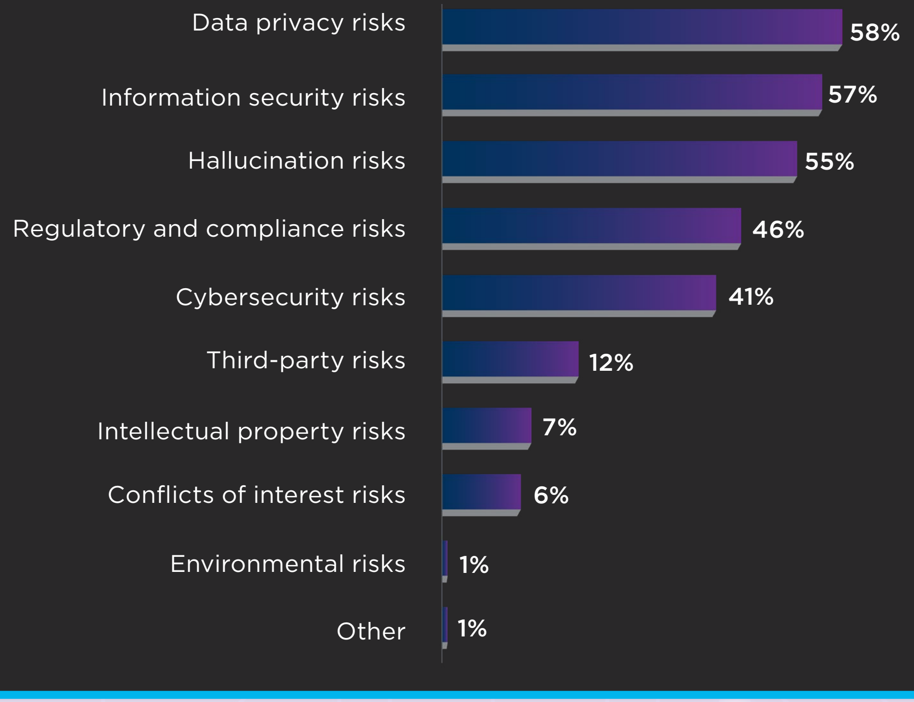
The following insights reveal the risks and challenges that are seen as most urgent for the financial services industry, the steps firms are taking to meet these challenges, and what opportunities remain for firms to improve their AI risk management practices.

Our Top AI Concerns

As firms integrate AI into their workflows, they are encountering a mix of risks and challenges that are familiar to any new technology as well as concerns that are unique to AI.

Which of the following risks are you most concerned about when it comes to using AI tools at your firm?

(Select your top three)



The data reveals that data privacy risks are the primary cause of apprehension, with 58% of firms citing concerns about the misuse or exposure of personal data as the top AI-related risk.

Information security risks (57%) follow closely behind, demonstrating that CCOs view AI's potential for misuse or loss of data, including sensitive customer data and critical firm data, as the top risks that need to be managed. Privacy risk was also identified as the top concern in our 2024 survey, with 60% of respondents citing it as their primary issue that year. However, information security has increased significantly since then, showing an 11-point increase in only a year.

Beyond data protection, firms are increasingly focused on hallucination risks (55%), referring to the potential for AI tools to generate incorrect or misleading outputs. These hallucinations can have serious implications for firms, especially when results inform strategic decisions or client-facing activities. Although hallucination risk remains the third highest concern, it has risen by six points since 2024.

Regulatory and compliance risks (46%) are also a concern for firms, though it is important to note that this concern has decreased significantly since 2024. Last year, regulatory risks associated with AI tools were the second highest risk identified by CCOs, with 59% of respondents selecting that risk. This 13-point drop speaks to firms gaining confidence in their ability to manage this risk and reflects a shift in regulatory focus under SEC Chair Paul Atkins.

Cybersecurity risk rounds out the top five risks at 41%, essentially unchanged from 2024 (42%) and, after this point, there is a steep drop off in the level of concern CCOs have about each risk. While the percentage of firms selecting third-party risk, conflicts of interest, and environmental risks has remained consistent year over year, intellectual property risk has dropped from 21% to 7%. This change likely reflects the growing prominence of other risks and the evolution of AI adoption, with many firms moving toward private AI tools rather than relying on less secure public model.

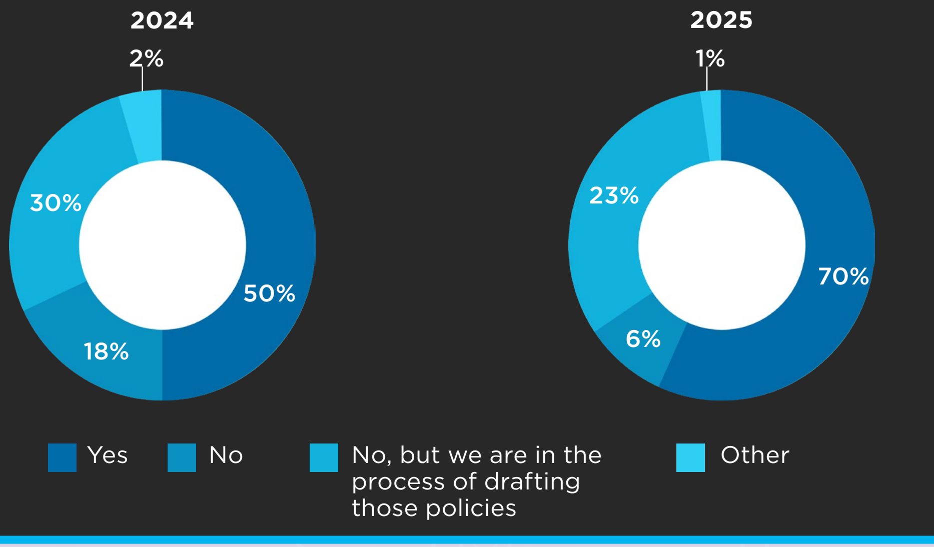
Top Risk Concerns When Using AI Tools

58%	Data privacy
57%	Information security risks
55%	Hallucination risks
46%	Regulatory and compliance risks
41%	Cybersecurity risks

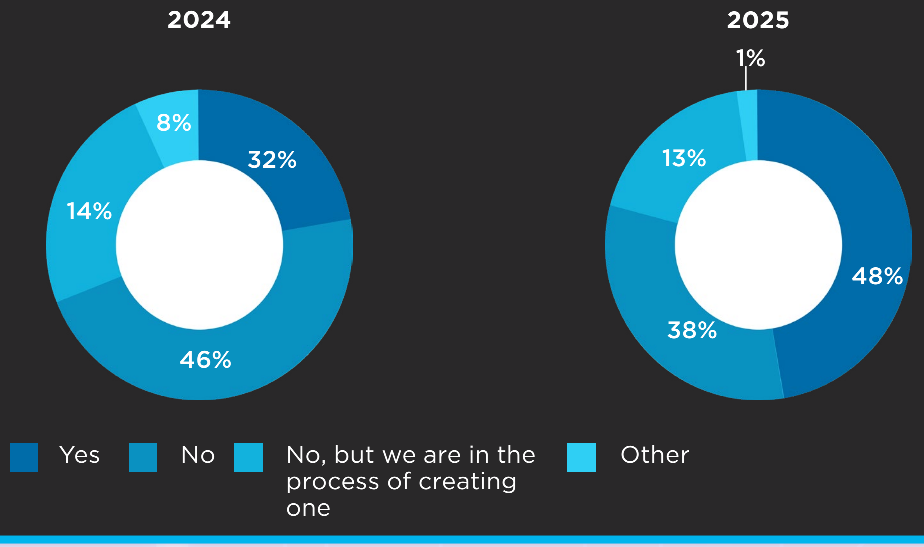
Progress on AI Risk Management

Over the past year, firms have taken steps to better manage AI risk across their organizations. This begins with establishing the appropriate policies, procedures, and governance structures for AI tools and technology—all of which have seen significant growth in just one year.

Has your firm established policies or protocols to govern AI use by employees?



Does your firm have an AI committee or similar AI governance group?



The percentage of firms with established policies and procedures governing employee use of AI tools has increased by 20 percentage points over the past year, reflecting growing operational maturity amid rapid adoption. This trend acknowledges that employees will use AI tools, formally or informally, and that, like any technology, firms must define when and how such use is acceptable. Even firms that choose to ban AI tools altogether (an uncommon approach in 2025) should document that decision in a formal policy and communicate it clearly to employees.

Firms are also strengthening governance over AI use, with the percentage of firms that have established a formal governance committee rising by 16 points. These governance committees can be essential in helping a firm establish consistent acceptable use cases for AI tools, define the firm's AI risk posture, and ensure that appropriate steps are taken to manage AI risk.

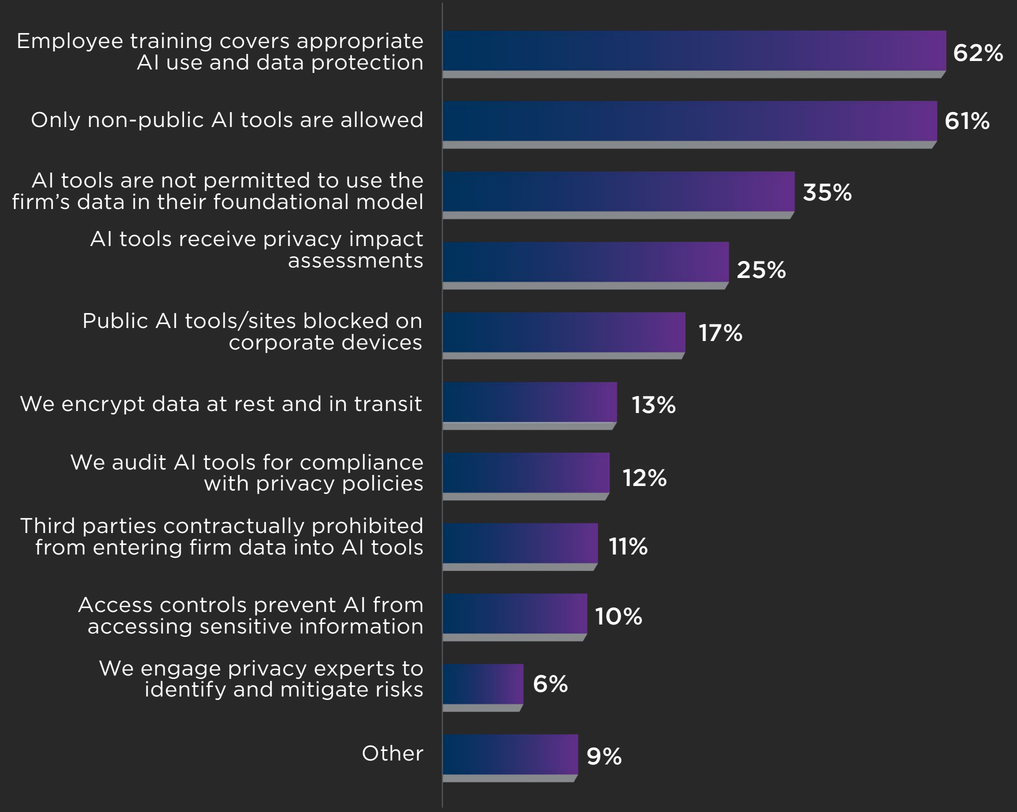
While firms can certainly establish these important elements of AI governance without a committee or working group, such committees help ensure consistency and accountability in AI decision-making.

Addressing the Top AI Concern: Privacy Risks

Privacy is one of the top concerns firms have about the adoption of AI tools and technologies, and establishing proper policies, procedures, and controls around AI tools is essential to effectively managing this risk.

What measures are in place to minimize the privacy risks associated with AI tools?

(Check all that apply)



Firms are working to raise awareness around the privacy risks of AI through their employee training, with an 11-point increase in the percentage of firms that cover AI topics in their privacy training since 2024. It is also a positive step to see more firms moving away from public AI tools, which can put the firm's sensitive data at greater risk for exposure and breaches. While these are important steps for firms to take, there are still opportunities for firms to better manage privacy risks.

Beyond training and preventing public tools from being used by employees, adoption of other controls and activities to manage privacy risk is limited. No single control is used by more than 35% of firms, indicating gaps in our approach to risk management. As firms continue to mature the management or privacy risks around AI tools, they are implementing access controls to limit their AI tool's access to sensitive data (10%), establishing contractual limitations on how service providers can use AI to work with customer data (11%), conducting privacy assessments (25%), and preventing the firm's data from being used to train AI models (35%).

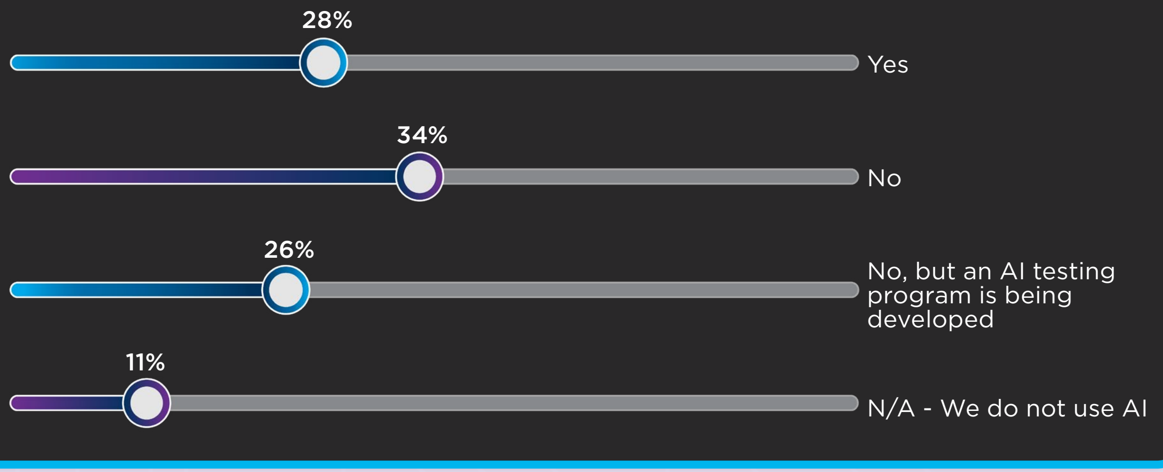
Managing AI Hallucinations Risks

One of the elements that make AI tools unique among other technologies is that these tools can and will produce non-deterministic results: asking an AI tool the same question twice can produce different outputs. Part of this is what makes AI tools so powerful. They will "learn" and evolve over time, which should cause their outputs to become more accurate over time. However, it also creates the risk that AI tools produce outputs that are misleading, based on fabricated information, or are simply incorrect. These inaccurate outputs are referred to as hallucinations, and they are one of the most cited AI-related risks (55%).

To address this, firms should establish formal processes or programs to validate the outputs of AI tools. However, these testing programs are uncommon, with only 28% of firms currently having them in place. It is worth noting that this does represent a 10-point increase from 2024, showing firms are making progress, even though this remains an opportunity for improvement.

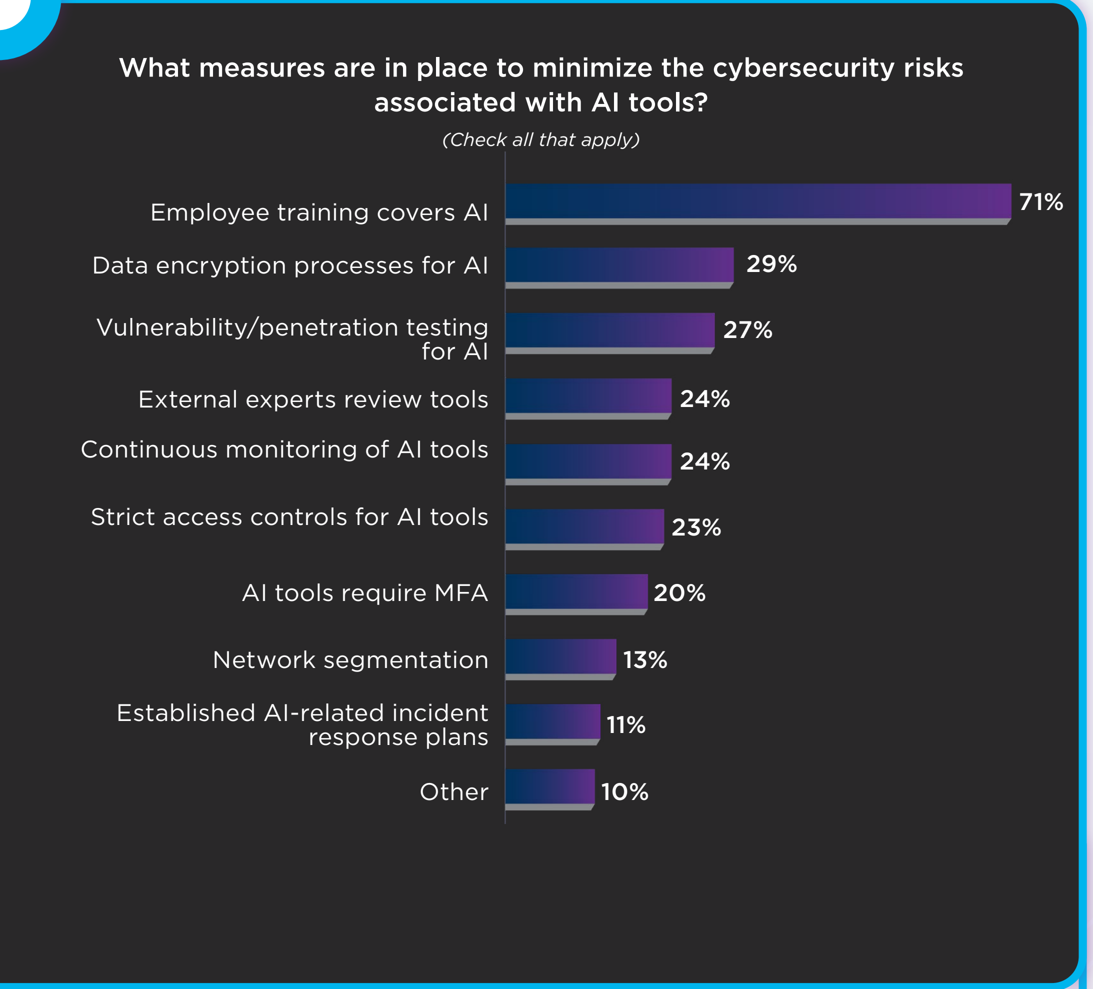
For firms that formally conduct validation and testing, having staff review a sample of AI outputs is the most common approach taken (55%). Other common testing techniques include ongoing monitoring of the performance of AI tools (40%), model reviews (35%), and model back-testing (11%), which involves comparing the outputs of an AI model to known historical data and outcomes. Implementing these steps or at least having a formal process for human oversight and review of the outputs of AI models, will help reduce the impact of potential AI hallucinations by catching incorrect outputs before they are used to make decisions or create client-facing materials.

If you are utilizing AI tools (internally or client-facing) have you established a program to test or validate the outputs of these tools?



Managing Cybersecurity Risks of AI Tools

While not as common a concern as privacy or hallucinations, cybersecurity remains an important AI-related risk for firms to manage.


What measures are in place to minimize the cybersecurity risks associated with AI tools?

(Check all that apply)

Similar to managing privacy risk, most firms (71%) have updated their employee training to include information on AI-related cyber risks, which is a significant increase from 2024 (50%). This is a critical step in managing cybersecurity risks, as employee behavior is a common root cause of cyber incidents. However, after employee training, no other control is used by more than 29% of firms, increasing the likelihood of a cybersecurity incident.

As businesses continue to integrate AI into their operations, these cybersecurity controls will become more essential to protecting the firm and investors from costly disruptions. This should include building or updating the firm's incident response plans to account for AI-related disruptions (11%), limiting what portions of the firms' network and infrastructure AI tools can interact with (13%), implementing strict access controls for AI tools (23%), and conducting vulnerability or penetration testing (27%). Firms should consider implementing these steps to better manage cybersecurity risks associated with AI tools and help protect against costly incidents.

Conclusion

AI presents tremendous opportunities for financial services firms, but it also introduces complex risks that require thoughtful management. While firms have made meaningful progress in addressing these risks, the increased use and integration of AI into how employees work will require firms to continue to evolve their approach to AI risk management. To protect themselves from the privacy, hallucination, and cyber risks that firms identify as top concerns, firms must prioritize the development of comprehensive AI governance frameworks, implement robust controls around these tools, and continue to communicate to their employees the risks that AI tools can present. With the right risk management approach, firms can turn AI risk into a strategic advantage, driving innovation while safeguarding their clients, data, and reputation.

Managing AI Across the Third-Party Network

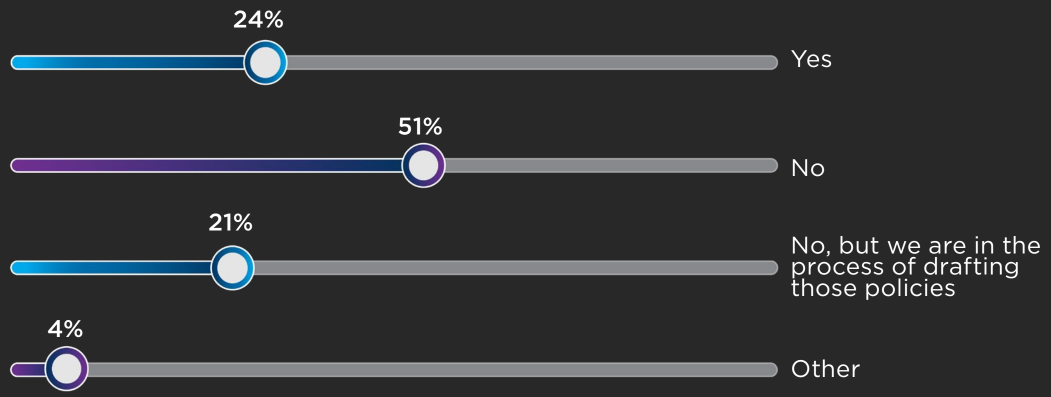
As financial services firms accelerate their adoption of AI technologies, the third parties they rely on for critical business operations do as well. From data analytics providers to outsourced customer service chatbots, vendors are increasingly integrating AI into their offerings, often without the visibility or oversight of the firms they serve. This growing reliance on AI-enabled third parties introduces a new dimension of risk that firms must address to mitigate privacy, cybersecurity, and operational disruptions.

Beyond internal risks, third-party exposure is a focal point for regulators. Recent developments, including the SEC's amendments to Regulation S-P and the EU's Digital Operational Resilience Act, underscore the growing importance of vendor oversight to regulators. These frameworks highlight the need for firms to understand and manage the risks posed by their external partners, particularly in areas involving sensitive data and operational resilience, where the use of AI tools can amplify vulnerabilities.

The Current State of Third-Party AI Risk Management

Based on the results of our survey, many firms are still in the early stages of addressing AI-related risks across their third-party networks.

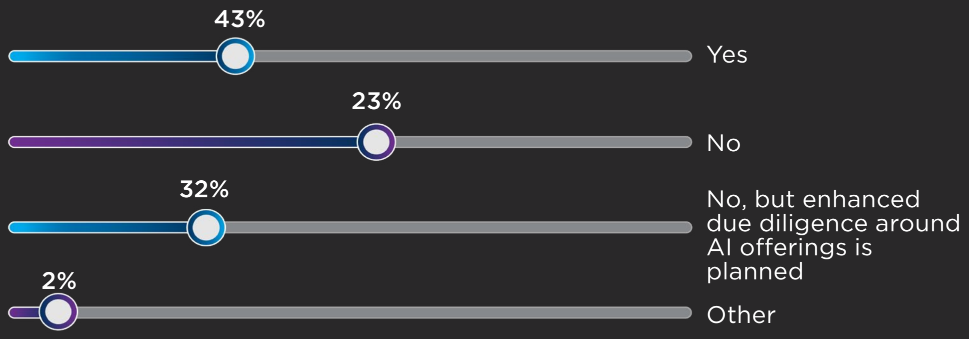
Has your firm established policies or protocols to govern AI use by third-parties or service providers?



Only 24% of firms have policies and procedures in place to govern third-party AI use, and over half of respondents have neither of these policies currently in place, nor plans to establish those policies in the near future. This gap isn't surprising, as the data shows firms have been primarily focused on establishing their own internal policies and procedures around AI. However, it is important that firms also begin to understand how their service providers are using AI and managing those risks.

Despite the lack of policies around third-party AI use, firms are beginning to enhance their due diligence and controls around third parties that are directly offering AI solutions.

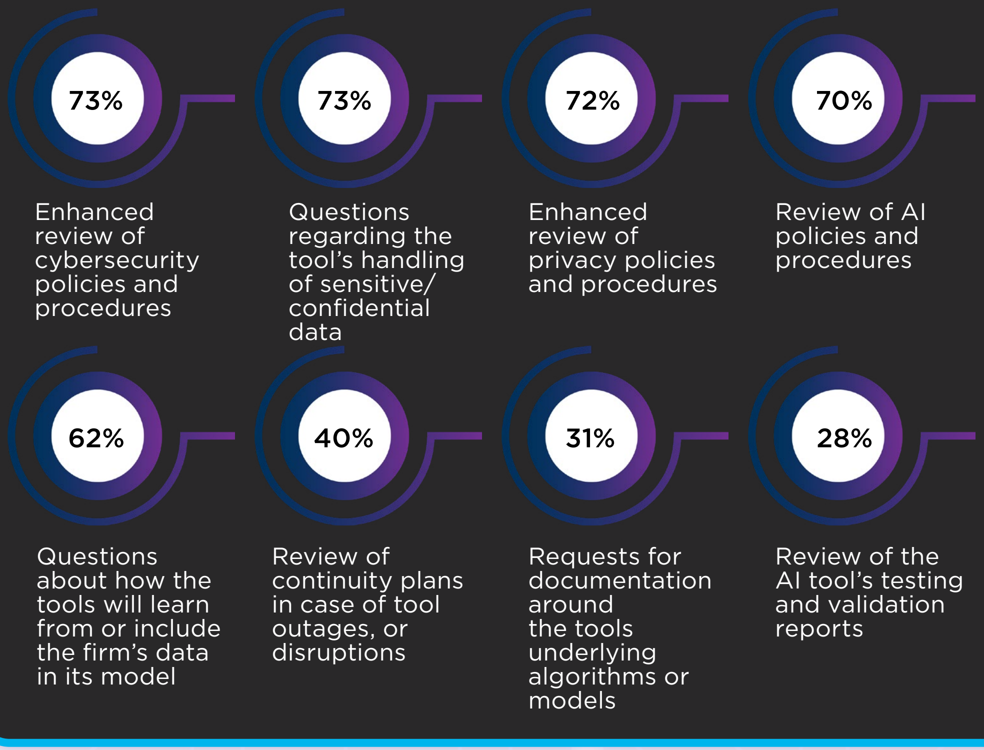
Have you enhanced your due diligence on vendors offering AI solutions?



For firms that are engaging in enhanced due diligence of AI vendors, there are a few common techniques used during this process.

Which of the following items are included in your enhanced due diligence of AI vendors?

(Check all that apply)



While it is a positive step that many firms are engaging in enhanced due diligence of AI vendors, firms still face challenges identifying which of their third parties are using AI, making it difficult to assess the associated risks and implement appropriate controls.

Closing Gaps in Third-Party Oversight of AI

Limited visibility into third-party AI adoption and weak governance over its use create meaningful risks for firms. With regulators emphasizing third-party oversight and AI tools becoming attractive targets for cyberattacks, firms have clear justification to actively monitor how their vendors deploy these technologies. Without clear oversight, firms may find themselves liable for incidents originating from their third-party AI systems.

To close these gaps and strengthen third-party AI risk management, firms should consider implementing the following steps:

Inventory AI use across vendors: As part of the firm's larger vendor inventory, firms should begin by identifying which third parties are currently using AI and for what purposes. This important first step can help the firm better understand how their third-party network's use of AI may be impacting their privacy, cyber, and regulatory risk.

Develop policies and procedures to manage third-party AI use: Firms should establish clear guidelines for acceptable AI use by third parties, including requirements for transparency, data handling, and model validation. These policies should be integrated into existing third-party risk management programs.

Enhance due diligence for third parties using AI: For third parties that handle sensitive customer or firm data, or who are classified as high risk, firms should be sure to use enhanced due diligence to evaluate the risks these firms present. This can include questionnaires with AI-specific considerations, such as the types of data used to train models, the presence of bias mitigation strategies, and the vendor's approach to monitoring and updating AI systems.

Monitor and audit third-party AI use: Firms should conduct monitoring of their AI use by their third parties to ensure they are adhering to the firm's expectations and requirements around AI use. As part of this process, firms should ask about the adoption of new AI technologies or evolving use cases for AI, since the rapid evolution of these tools can increase the risks a third party presents, and the steps needed to manage them.

Conclusion

AI is reshaping the financial services landscape, offering powerful tools for efficiency, insight, and innovation. However, as firms embrace these technologies, they must not overlook the risks introduced by their third-party partners. With regulators sharpening their focus and cyber threats on the rise, the time to act is now. By establishing clear policies, enhancing due diligence, and improving visibility into third-party AI use, firms can better protect themselves from the unintended consequences of unchecked innovation.

Progress and Next Steps in the AI Journey

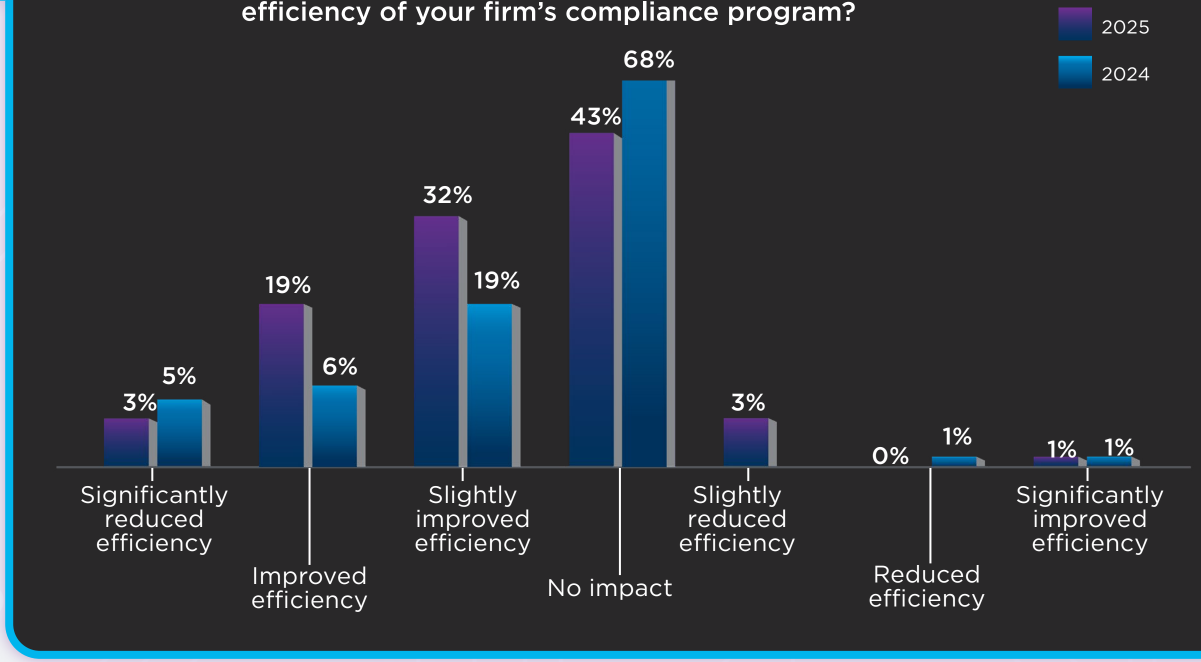
The financial services industry has entered a new phase in its relationship with AI; what was once a cautious exploration of emerging technologies has evolved into a more confident and strategic adoption of AI tools across research, compliance and risk management, and operations functions. While it is too soon to say if AI tools will live up to their promised efficiency gains, early indicators suggest encouraging outcomes for compliance leaders.

The Early Impact of AI Tools

For compliance leaders, the goal of AI adoption is primarily to improve the efficiency of their programs, with 70% of CCOs identifying this as their primary goal. For compliance programs that often feel like they are constantly being asked to do more with less, these tools and technologies can provide welcomed relief by reducing manual work and allowing the program to operate faster. So far, AI tools seem to be supporting these goals for compliance programs.

In 2024, 68% of CCOs reported that AI had “No impact” on their compliance programs. However, just one year later, that number has dropped to 43%, with most respondents (53%) now reporting that AI has had at least some positive impact on their compliance program.

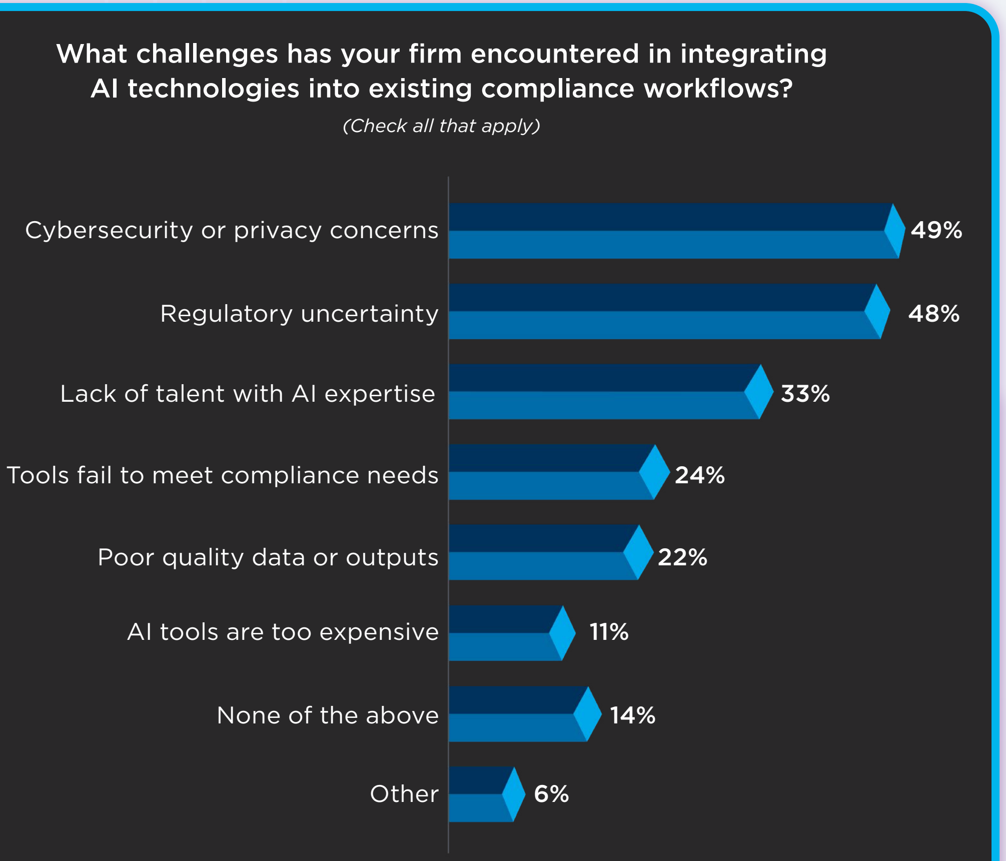
To what extent has the adoption of AI impacted the efficiency of your firm’s compliance program?



This rapid impact of AI is significant and reflects the growing comfort of compliance leaders with technology and their increasing willingness to integrate it into their operations. Compliance leaders are growing their skills and abilities to effectively use these tools.

Where Challenges in AI Adoption Remain

While these early results are promising, like the adoption or launch of any new technology, there have been challenges for compliance programs to integrate AI into their workflows.



The leading challenge for CCOs mirrors their primary concern with AI tools in general, that these technologies could create additional cybersecurity and privacy risks for the firm (49%). This is a risk firms will need to actively manage regardless of the use case. It is no surprise that compliance leaders are particularly concerned about how the tools used in their programs may increase this exposure.

Close behind cybersecurity and privacy concerns, compliance leaders are struggling to navigate uncertain regulatory expectations around AI tools (48%). There are meaningful questions that need to be resolved around how compliance leaders are expected to document AI outputs, especially when interacting with clients, and how AI risks should be managed. While it is very likely that regulators will begin providing guidance around AI use, for now, this remains a challenge for compliance leaders.

Next Steps in AI Adoption

Looking ahead, the next phase of AI adoption will likely focus on scaling successful use cases, enhancing governance structures to meet evolving regulatory expectations, and working with business leaders to ensure the responsible use of AI tools. As compliance leaders continue to explore and integrate AI into their programs, the shift from experimentation to meaningful impact is becoming increasingly clear. The early results are encouraging, with AI showing signs that it will be able to deliver on its promise of greater efficiency and operational support.

Our AI adoption journey is far from over; it will be a continual process of adapting to new cybersecurity and privacy challenges, responding to regulations, and working to ensure that AI tools are delivering their expected value to the firm. By staying informed and proactive, compliance teams can ensure that their use of AI not only enhances their programs but also aligns with broader firm priorities and evolving regulatory expectations.

How We Help

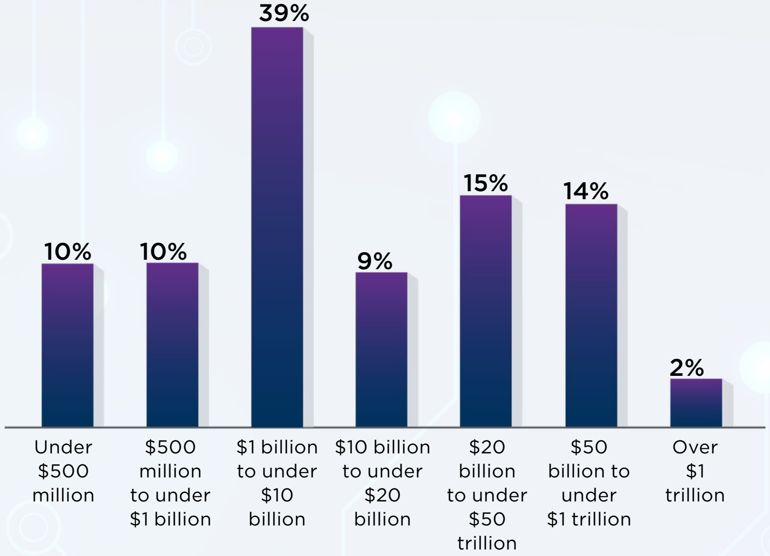
At ACA, our goal is to be your trusted partner as you navigate the opportunities and challenges of AI in compliance. That's why we developed **Encore AI**, a purpose-built solution designed to help compliance teams leverage AI responsibly and efficiently.

Encore AI combines advanced automation with ACA's deep regulatory expertise, enabling firms to streamline workflows, reduce risk, and stay ahead of evolving requirements.

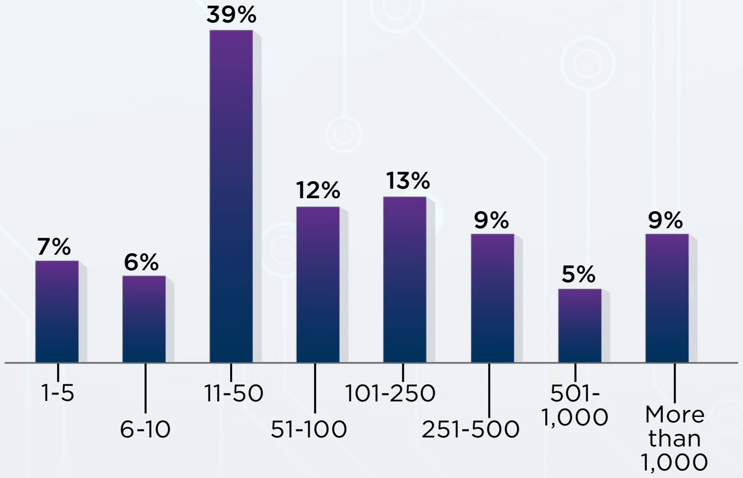
Connect with an expert to develop your AI strategy today.

Appendix: Participant Demographics

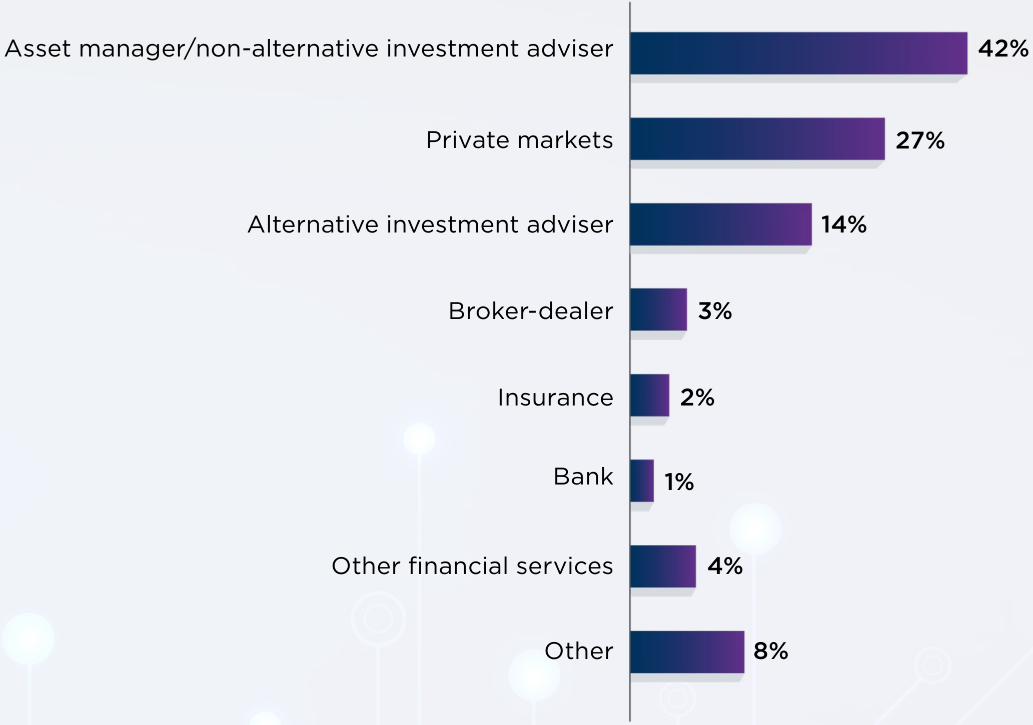
Which best describes your firm's total RAUM (Regulatory Assets Under Management)?



How many full and part-time employees does your firm employ?



What would you best classify your business as?


Asset manager/non-alternative investment adviser
Private markets
Alternative investment adviser
Broker-dealer
Insurance
Bank
Other financial services
Other