Survey Findings

2026 Investment Management Compliance Testing Report

Key Trends in Compliance Risk and Program Management

ACA® IAA INVESTMENT ADVISER ASSOCIATION YUTER COMPLIANCE CONSULTING

Contents

Key Findings

Five key findings from the 2026 IMCT Survey reveal where compliance leaders are focusing, the progress being made, and the challenges that remain.

1 AI Takes the Lead

85%

of respondents cited AI as the hottest compliance topic for 2026

↑ 28 percentage-point increase from 2025

Firms are making strong progress in managing AI risks, but opportunities remain to strengthen oversight, testing, and incident response preparedness.

2 BCP Focuses on Cyber

88%

of firms review and update their business continuity plans at least annually

Cyber incidents and vendor outages are the most commonly tested scenarios, reflecting the industry's focus on operational resilience.

3 Regulation S-P Progress

83%

of firms had updated policies and procedures to align with Regulation S-P

Despite this progress, many firms still faced challenges meeting the new third-party oversight and incident notification requirements.

4 TPRM Under the Spotlight

39%

of respondents have made significant changes to their third-party risk management programs

An additional 22% plan to do so, driven by increased regulatory scrutiny. Key changes include updating policies and procedures (69%), refining vendor risk-tiering (58%), and expanding due diligence requirements (54%).

5 Compliance Program Structure

60%

of CCOs serve in multiple executive roles

Overall program structure, staffing, and budgets remained consistent with 2025, suggesting compliance teams continue to do more with less.

What This Means

Compliance teams continue to navigate a rapidly evolving risk landscape.

AI has surged to the top of the agenda, making strong governance and testing critical.

Regulatory expectations around third parties and data privacy are driving program enhancements.

Despite steady resources, compliance leaders are finding new ways to do more with less.

About the Investment Management Compliance Testing Survey

The 2026 Investment Management Compliance Testing Survey (IMCT), co-sponsored by ACA Group, the Investment Adviser Association, and Yuter Compliance Consulting, marks the survey's 21st year. Since the survey's first launch in 2006, it has provided compliance leaders at SEC-registered investment advisers with benchmarking data on key compliance activities, priorities, resource allocation, and an evolving range of important topics. The 2026 survey continues this effort by providing the industry with key insights and opportunities for improvement in emerging topics. It explores emerging topics such as AI and the amendments to Regulation S-P, alongside perennial priorities including compliance program testing and SEC examination trends.

The 2026 IMCT includes data from 411 firms in the investment management space (For a full breakdown of respondent demographics, please see Appendix A). Data was gathered via an online survey during April and May 2026 that was deployed to clients of ACA Group, Yuter Compliance Consulting, and IAA members.

Survey at a Glance

411
Respondents

April-May 2026
Data Collection Period

21 Years
of Benchmarking Insights

3 Sponsors
ACA Group, IAA and Yuter Compliance Consulting

Diverse Firm Profiles
By AUM, Strategy, and Geography

Compliance Priorities for 2026

AI Reigns as the "Hottest" Topic

85% **of respondents identified AI as the hottest compliance topic for 2026.**

↑ *Up 28 percentage points from 2025*

Since generative AI tools became widely available, AI has been one of the most talked-about topics across the investment management industry. Since 2024, the IMCT survey has been tracking how firms use AI, the importance of the topic, and how compliance programs are working to govern and manage AI risks. During that time, focus on AI has steadily increased, and the 2026 survey results continue that trend (see **Table 1**).

85% of respondents identified AI as their "hottest" topic for 2026, a 28 percentage point increase from the previous year's survey, and almost almost 50 percentage points higher than the second most selected topic, cybersecurity. This focus on AI is also seen in how firms are adopting AI tools and technologies, and the steps firms are taking to manage the risks associated with AI.

AI tools are now being used by 80% of respondents for internal or external use cases (see **Graph 1**). Most respondents (70%) limit AI use to internal applications, while only 10% allow employees to use AI for client-facing or external use cases. Another 18% of firms are still exploring AI, and only 2% have banned AI tools.

Table 1

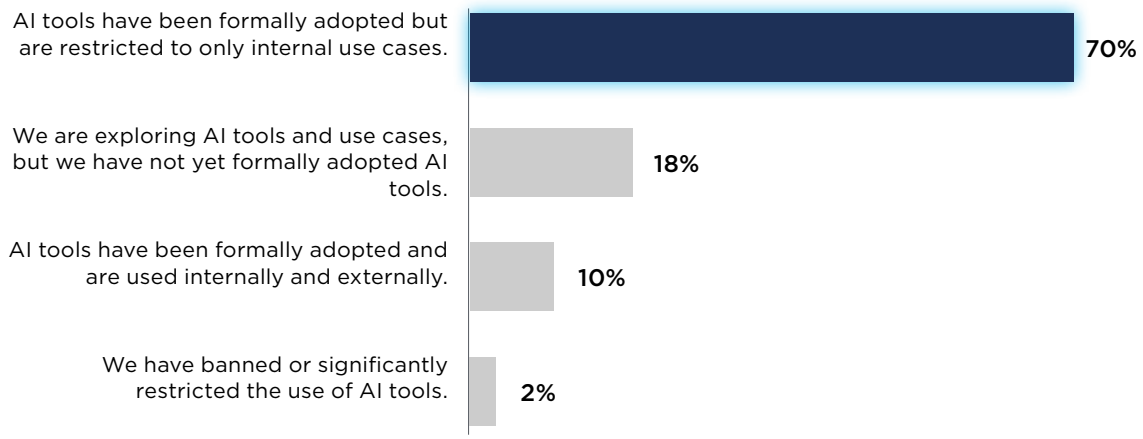
Top Compliance Topics Identified by Survey Respondents

(Top 10 Responses Displayed)

1.	Artificial intelligence	85%
2.	Cybersecurity	37%
3.	Privacy/Regulation S-P	35%
4.	Advertising/Marketing	19%
5.	Prediction markets	14%
6.	Vendor due diligence	10%
7.	Digital assets	9%
8.	Conflicts of interest	9%
9.	Alternative investment for retail investors	8%
10.	Valuation	7%

Graph 1

Which of the Following Best Describes Your Firm's Current Use of AI Systems and Tools?



Along with this AI integration, firms have also made significant progress implementing policies and procedures to manage AI risk.

86% have established policies and procedures governing employee use of AI, and another 10% are developing them.

59% have established AI governance committees, while another 10% are developing them.

86% maintain an inventory of approved AI tools, while another 8% are creating AI inventories.

72% have updated their training to cover AI risks and appropriate use, while another 19% are updating their training.

72% have increased compliance testing for AI.

Key Takeaways

- AI remains the leading priority.
- Most firms have established strong governance.
- Opportunities remain around third-party oversight.

These data points highlight the importance firms place on managing the risks of AI adoption. U.S. regulators continue to focus on how firms govern AI use to interact with clients and provide investment advice. The firms that have taken steps to appropriately govern AI use and manage its unique risks are better positioned to meet future regulatory scrutiny around AI tools.

However, given the relative immaturity of these tools, many firms still have opportunities to improve AI risk management practices.

These opportunities include:

- Enhancing incident response plans to address AI-related disruptions and incidents
- Developing policies and procedures governing AI use by third parties
- Formalizing the testing and validation of AI outputs

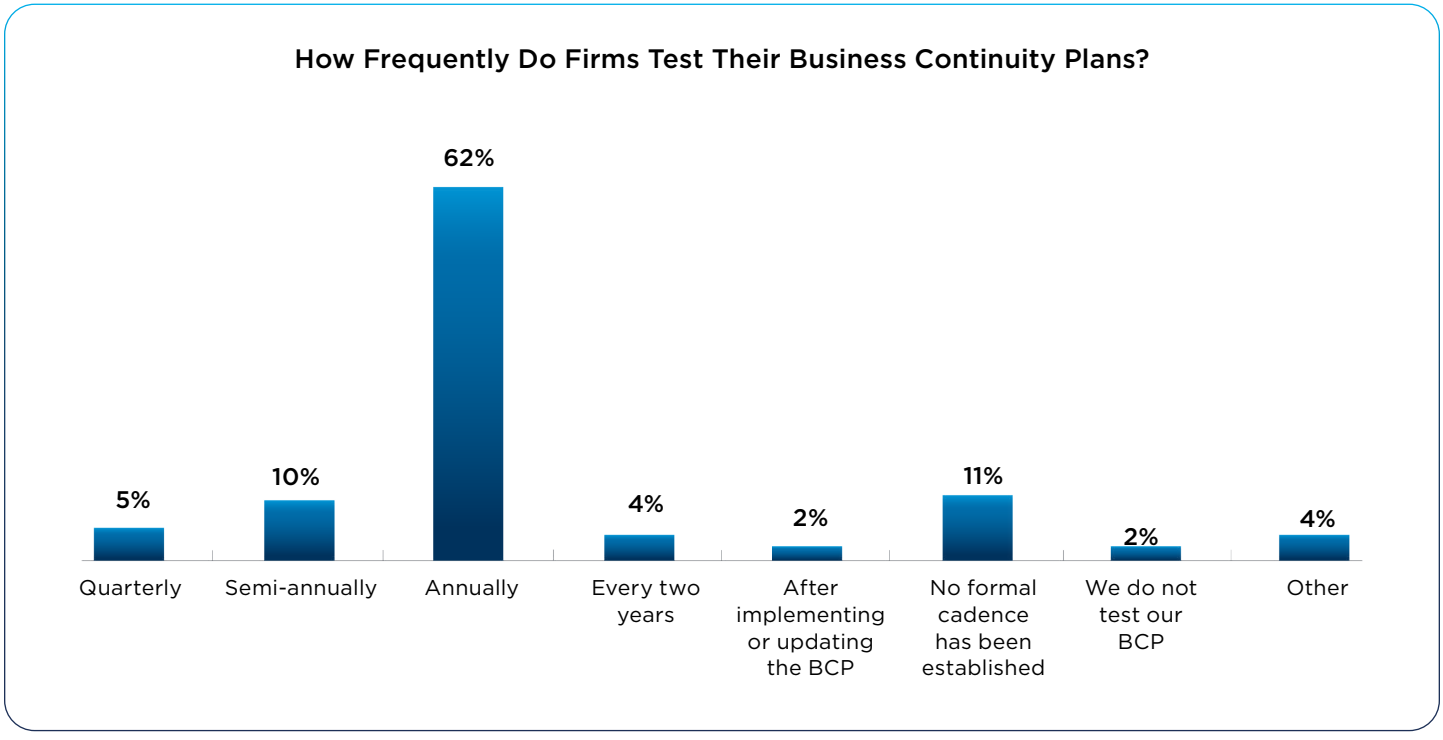
As firms continue to expand their use of AI, closing these gaps can help them manage evolving associated risks and better respond to potential AI-related incidents and disruptions.

Preparing for Cyber and Information Security Incidents and Disruptions

88% **of respondents review and update their BCP at least annually.**

Cybersecurity maintained its place as one of the hottest compliance topics in 2026 (see **Table 1**). Driven by regulatory pressures around a firm's ability to detect and recover from information security incidents (e.g., the amendments to Reg S-P and the Digital Operational Resilience Act (DORA) in the EU) and the rising cost and visibility of cyber threats, firms are paying increasing attention to their incident response and business continuity planning. This reflects the fact that not even the best compliance, cybersecurity, or information security program can prevent every disruption. Firms must prepare for these disruptions and test their preparations to ensure they are effective.

While nearly all firms update and review their incident response plans and business continuity plans at least annually (81% and 88%, respectively), testing occurs less frequently. Only 77% of firms test their BCPs at least annually.



While annual BCP testing may be a reasonable cadence in many instances, the 13% of firms that either have no formal cadence for testing or do not test their BCPs have an improvement opportunity. Testing a continuity plan can help the firm identify portions of the plan that may seem appropriate in theory but fail in practice, allowing the firm to make practical improvements to its BCP. This testing also reinforces key roles and responsibilities outlined in the BCP, helping staff respond during an incident.

Table 3

Which Scenarios Have Been Tested in the Last 12 Months?

(check all that apply)

62%	Cybersecurity incident (e.g., ransomware/data breach)
48%	Critical vendor or service outage
46%	Facility inaccessibility
31%	Unauthorized access/use of customer data
19%	Key-person unavailability

As part of this BCP testing, most firms are focusing on cybersecurity incidents (62%), operational disruptions related to third parties (48%), and disruptions related to facility closures (46%). Firms are also increasingly testing their response to incidents involving unauthorized access or use of customer information, likely in response to the recent amendments to Regulation S-P.

Key Takeaways

- Most firms review and update their BCPs annually, but testing frequency varies.
- Cybersecurity incidents, vendor outages, and facility disruptions are the most commonly tested scenarios.
- Firms without a formal testing cadence may have opportunities to strengthen operational resilience.

Meeting the Requirements of the Amended Regulation S-P

Regulation S-P and privacy risk were the third "hottest" topic for compliance leaders in 2026 (see **Table 1**), and for good reason. The SEC's 2026 Examination Priorities make it clear that compliance with the amendments to Regulation S-P will be a focus for the Division of Examinations. And because the compliance dates (December 3, 2025, and June 3, 2026) coincided with the survey period, meeting the safeguarding, disposal, and incident response requirements was a key priority for compliance leaders.

To prepare for the amendments, firms are updating their information security policies and procedures (83%), formalizing their incident response plans (53%), and updating their data retention policies and procedures (35%)[1]. While the data showed firms making progress in preparing for the amendments to Regulation S-P, firms have opportunities to better protect customer information. These include creating a data map of customer information, conducting due diligence on service provider incident response plans, and training staff on information security and Reg S-P-related topics.

What steps has your firm taken to address the amended Regulation S-P?

(check all that apply)

83%
Updated our privacy policies and procedures

53%
Formalized our IRP

35%
Updated our data retention/books and records policy

34%
Created a data map of our non-public personal data, including where it is stored and who has access

33%
Required certain vendors to affirmatively consent to incident notification

29%
Documented compliance with vendor notification requirements and risk assessment of vendors

28%
Conducted due diligence on vendor's security breach notification policies and plans

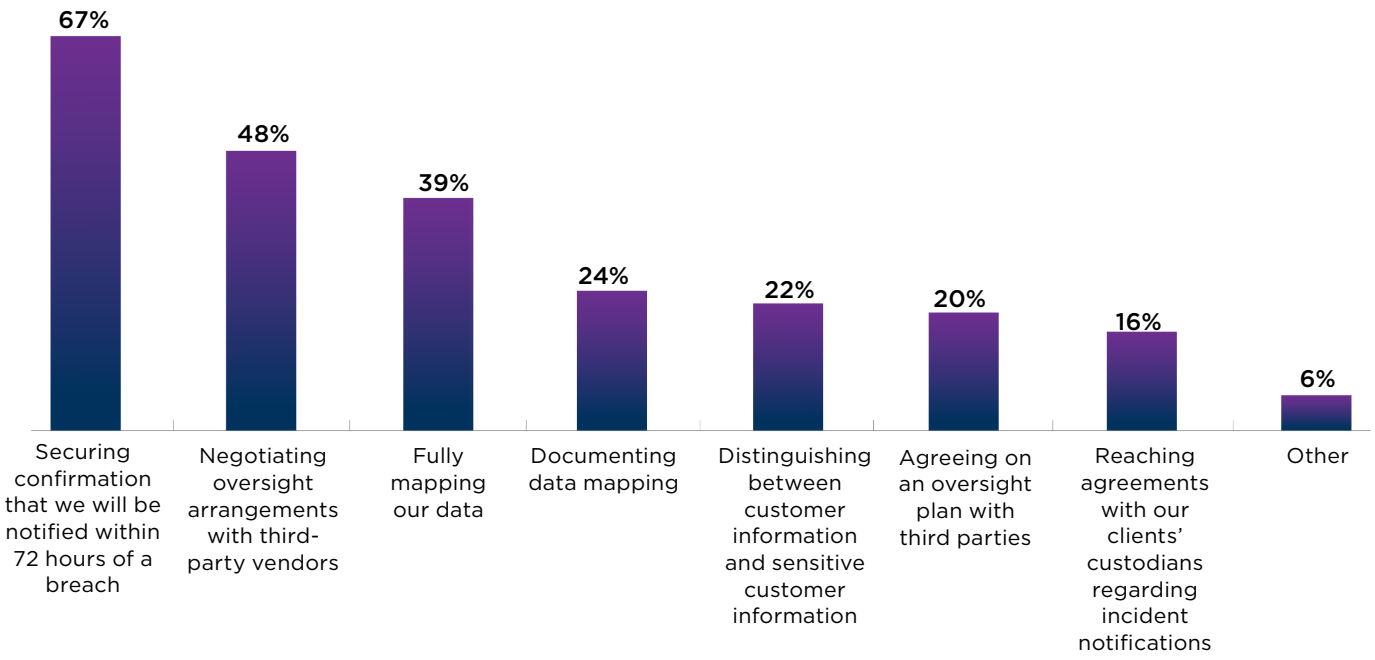
27%
Conducted training

[1]It is important to remember the survey's data was collected in April and May of 2026. That means that many smaller firms that completed the survey were still in the process of preparing for the regulation's June 3 compliance deadline, which at least partially explains why there may appear to be gaps between the regulation's requirements and common industry practice.

These improvement areas align with the expectations of the amended regulation. Common challenges include securing confirmation from service providers that they will notify the firm within the required 72-hour window (67%), negotiating oversight of service providers (48%), and mapping the firm's data (39%).

What Challenges Have You Faced in Implementing the Amended Regulation S-P?

(Check all that apply)



Addressing these areas will be critical not only for meeting regulatory expectations but also for building a resilient information security framework that can adapt to evolving risks. Firms that proactively strengthen governance, incident response, and third-party oversight will be best positioned to navigate regulatory scrutiny and protect customer information.

Key Takeaways

- Most firms have updated policies and procedures to address the amended Regulation S-P requirements.
- Third-party oversight and incident notification were the most significant implementation challenges.
- Data mapping, vendor due diligence, and employee training continue to be common areas for improvement.

Managing Third-Party Risk

Driven by regulatory pressures (e.g., the amendments to Reg S-P) as well as an expanding reliance on service providers, respondents to the survey identified vendor due diligence as one of the hottest compliance topics of 2026 (see **Table 1**). While this topic is much more of a perennial concern for compliance leaders, as noted in the previous section, the issue continues to evolve and create unique challenges for compliance leaders that need to be addressed. In fact, the majority of firms (60%) have made or are making significant changes to their third-party risk management programs, and 48% have increased their compliance testing around vendor due diligence.

The most common change firms are making centers on broad updates to the firm's third-party risk management policies and procedures (69%), which for many firms is likely in response to increased regulatory scrutiny of vendor risks. After this update to policies and procedures, firms are focusing on elements of their third-party governance by revising risk tiering of vendors (58%), expanding due diligence requirements for key service providers (54%), and establishing clearer owners and accountability for third-party relationships (49%). Firms are also working to ensure their third parties meet the 72-hour incident notification requirements of Regulation S-P, with 22% obtaining contractual commitments that third parties will comply with the 72-hour notification requirement, and 14% obtaining negative consent around the notification requirements.

Which of the Following Changes Have You Made to Your Third-Party Risk Management Program in the Past 12 Months?

(check all that apply

69% Updated third-party risk management policies and procedures

58% Introduced or revised vendor risk-tiering criteria (e.g., critical vs. non-critical vendors)

54% Expanded due diligence requirements for Key Service Providers

49% Established clearer internal ownership or accountability for vendor oversight

34% Updated standard vendor contract language (e.g., audit rights, incident notification, data protection)

32% Reviewed or renegotiated contracts with Key Service Providers

31% Improved internal tracking (e.g., standardized templates, dashboards, or workflows)

27% Implemented or enhanced continuous or periodic vendor risk reviews

Key Takeaways

- Firms continue to expand third-party risk management programs in response to evolving regulatory expectations.
- Policy updates, vendor risk tiering, and enhanced due diligence are the most common program enhancements.
- Many firms are also strengthening contractual oversight related to incident notification requirements.

Other Hot Topics

Prediction Markets, Social Media, and Advertising

For more than 20 years, the IMCT has played a critical role in equipping SEC-registered investment advisers with meaningful insight into industry best practices. The insight it provides enables compliance professionals to evaluate how their compliance programs compare to peers and support the regulatory expectation that advisers understand prevailing industry practices. SEC examination staff have consistently emphasized the importance of considering industry common practice when designing and enhancing compliance programs, and the survey's benchmarking helps firms recognize emerging best practices and prepare for regulatory examinations.

Along with the cosponsors' commitment to addressing key focus areas, this year we introduced a new "Lightning Round" feature designed to capture trending information across a range of topical areas. This approach was intentionally designed to offer quick insights rather than an in-depth review, helping to reduce survey fatigue while still providing meaningful, actionable takeaways for compliance professionals.

This year's Lightning Round covered the following topics:

- Marketing Rule net of fee FAQ relief
- Fiduciary duty policy trends
- Gift and entertainment policy trends
- New client solicitation trends
- Prediction market policy trends
- Performance usage trends
- Social media policy trends

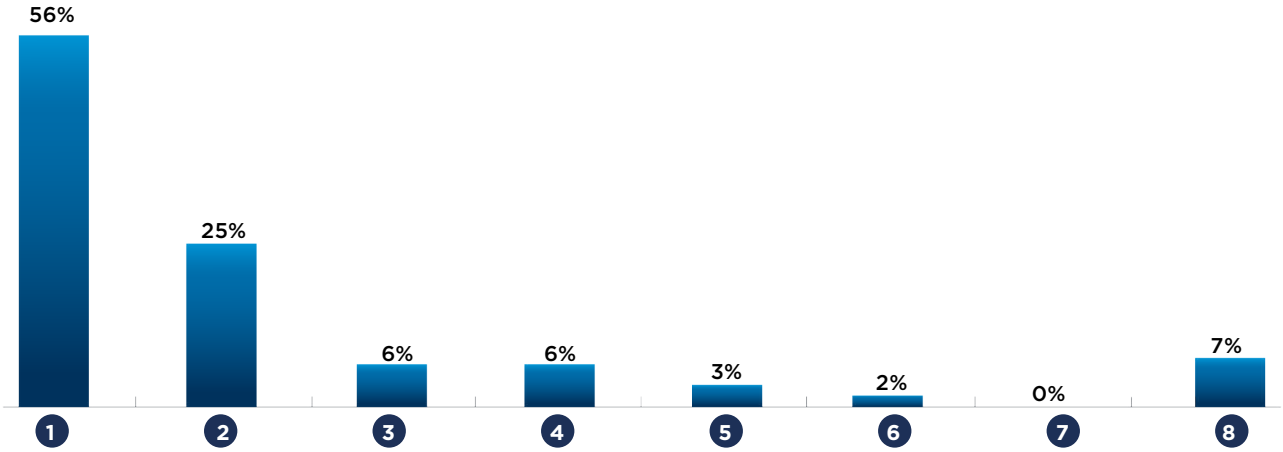
Prediction markets and social media emerged as the most noteworthy topics from this year's Lightning Round.

Prediction Markets

Like cryptocurrencies and digital assets a few years ago, prediction markets, such as Kalshi and Polymarket, have emerged as an area of interest for compliance leaders as employees and clients ask questions about the risks and opportunities of these platforms. Prediction markets allow individuals to place bets on a wide range of outcomes, including stock price movements, inflation rates, and election results, which could create greater risks for firms around insider trading and money laundering. But despite this risk, most firms have yet to change their code of ethics and/or insider trading policies to account for prediction markets.

How Has Your Firm Updated Its Code of Ethics and/or Policies To Prevent Insider Trading To Address How Supervised Persons Use Prediction Market Platforms (e.g., Kalshi, Polymarket)?

(check all that apply)



1. No updates or changes made, and none are planned at this time.
2. No updates or changes made, but we plan to make updates in the near future.
3. Our Code/Insider Trading Policy allows for trading on prediction markets, but bans trading on certain high-risk events.
4. Our Code/Insider Trading Policy treats prediction markets like personal trading of securities, subject to the firm's existing restrictions.
5. Our Code/Insider Trading Policy bans all use of prediction market platforms.
6. Our Code/Insider Trading Policy allows for trading on prediction markets, without restrictions.
7. Our Code/Insider Trading Policy restricts trading on prediction markets based on an employee's role or level.
8. Other

While some firms are planning to update their policies or have already addressed prediction markets, most firms (56%) seem to be waiting for greater regulatory clarity around the topic, or to better understand the potential risks and opportunities of these platforms.

Key Takeaways

- Prediction markets have emerged as an area of growing interest for compliance leaders.
- Most firms have not yet updated insider trading or Code of Ethics policies to specifically address prediction markets.
- Many firms appear to be waiting for greater regulatory clarity before changing policies or relying on existing restrictions.

Social Media Implications

Across firms, social media remains an area of concern, as it presents both reputational and regulatory risks. In response, firms have implemented and maintained a wide array of controls on employee usage of social media.

What Controls Have You Implemented With Respect to Social Media Use?

(check all that apply)

Training remains the most common social media control (53%). Firms also require preclearance for posts about advisory services (47%), while 39% prohibit these posts altogether, reflecting a cautious approach to communications that could be interpreted as advertising or investment advice.

Firms are also strengthening monitoring and recordkeeping. Thirty-seven percent periodically sample employee activity, 22% review all activity, and 30% retain social media posts to meet compliance obligations. These practices reflect continued regulatory focus on surveillance and documentation.

- **11%** pre-review comments about advisory services
- **13%** include abbreviated disclosures in social content
- **14%** require business email addresses for LinkedIn
- **22%** prohibit LinkedIn InMail

Key Takeaways

Training remains the foundation of social media compliance programs.

Controls increasingly limit advertising and communications risk.

Monitoring and recordkeeping continue to support regulatory compliance.

Compliance Program Resourcing Trends

From managing the risks of emerging technologies like AI and prediction markets, to perennial challenges like managing third-party risk and preparing for regulatory examinations, compliance leaders have seen their responsibilities expand in recent years. This is in addition to the fact that many CCOs report having additional C-suite-level responsibilities (**Table 4**)– a trend that has been common in the industry for years.

Despite the expanding role of the CCO and the growing complexity of regulatory expectations, compliance programs continue to operate with limited staffing and budgets.

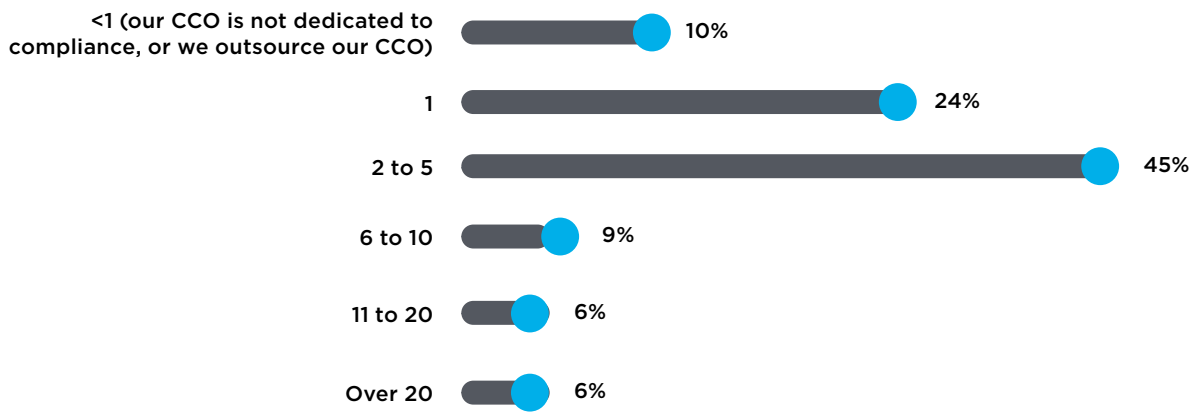
Table 4

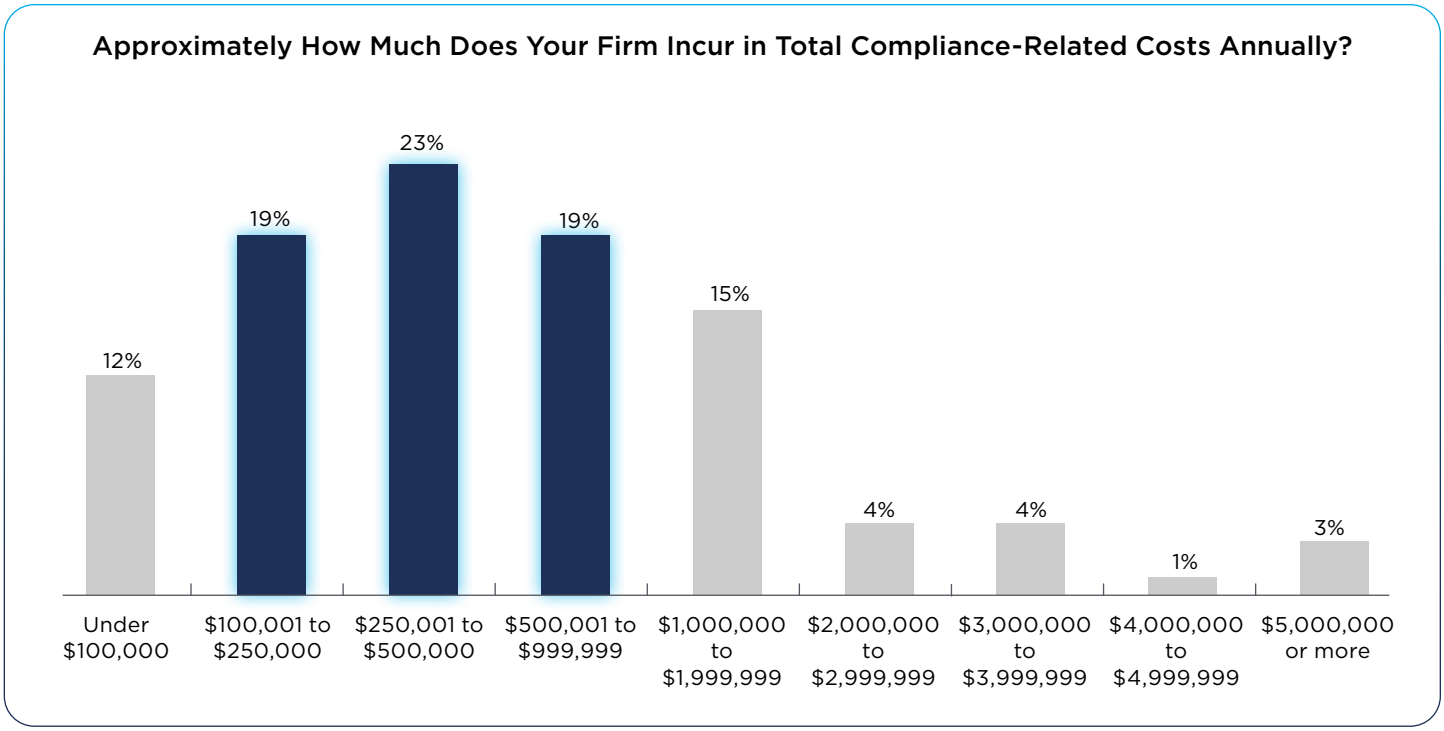
Does Your Firm's CCO Perform Non-CCO Functions?

(check all that apply)

40%	19%	17%	12%	7%	16%	2%
Our CCO is solely a CCO	Our CCO is also our COO	Our CCO is also our GC	Our CCO is also our CFO	Our CCO is also our CIO	Our CCO also performs another function	Our CCO is outsourced

How Many Employees Are Currently Employed in Your Firm's Compliance Department (Including the Firm's CCO)?





61% of firms spend between $100,001 and $999,999 annually on compliance.

This imbalance between expanding expectations and static resources is forcing compliance leaders to rethink how they prioritize efforts and allocate time. Rather than waiting for additional resources, CCOs are increasingly focusing on risk-based approaches, leveraging technology to automate routine tasks, and embedding compliance more deeply into business processes.

Key Takeaways

- Compliance responsibilities continue to expand while staffing and budgets remain relatively stable.
- Many CCOs continue to perform multiple executive functions.
- Firms are increasingly relying on risk-based approaches and technology to support compliance operations.

Conclusion

The findings from the 2026 IMCT survey highlight a compliance function undergoing significant change. As firms navigate the growing complexity of AI, heightened regulatory scrutiny around data protection, and increasing reliance on third-party providers, the role of compliance continues to expand in both scope and strategic importance.

Across these areas, a consistent theme emerges: firms are making meaningful progress, but enhancement opportunities remain. While most organizations have taken initial steps to address emerging risks—such as implementing AI governance frameworks or updating policies for Regulation S-P—fewer have fully operationalized these controls through rigorous testing, monitoring, and cross-functional integration.

At the same time, compliance leaders face a structural challenge. Expectations are rising faster than resources, with many CCOs continuing to balance multiple roles while managing increasingly complex programs. This dynamic makes prioritization, efficiency, and effective use of technology more critical than ever.

Looking ahead, firms that take a proactive and integrated approach to compliance will be best positioned for success. This includes:

- Embedding **governance frameworks** that evolve alongside emerging technologies, such as AI
- Strengthening **third-party oversight** and data protection practices
- Enhancing the testing and validation of **business continuity** and incident response plans
- Leveraging **benchmarking data** to align with industry practices and regulatory expectations

What This Means

AI has surged to the top of the agenda, making strong governance and testing critical.

Regulatory expectations around third parties and data privacy are driving program enhancements.

Despite steady resources, compliance leaders are finding new ways to do more with less.

Continue the Conversation

For more information or to discuss how these insights may impact your firm, **contact** an ACA expert today.

ACA® IAA INVESTMENT ADVISER ASSOCIATION YUTER COMPLIANCE CONSULTING

About the Investment Adviser Association

The Investment Adviser Association (IAA) is the leading organization dedicated to advancing the interests of fiduciary investment advisers. For nearly 90 years, the IAA has been advocating for advisers before Congress and U.S. and global regulators, promoting best practices and providing education and resources to empower advisers to effectively serve their clients, the capital markets, and the U.S. economy.

Our members range from global asset managers to the medium- and small-sized firms that make up the majority of our industry. Together, the IAA's member firms manage more than $57 trillion in assets for a wide variety of institutional and individual investors, including pension plans, trusts, mutual funds, private funds, endowments, foundations, and corporations. The IAA also provides extensive practical and educational resources to its membership. For more information, visit **www.investmentadviser.org** or follow us on **LinkedIn** and **YouTube**.

About ACA Group

ACA is the leading governance, risk, and compliance (GRC) partner in financial services. For over 20 years, ACA has empowered clients to launch, grow, and protect their businesses. Its global team of 1,700 professionals includes former regulators and industry practitioners. CNBC recognized ACA as one of the World's Top Fintech Companies in 2026. ACA's innovative approach integrates advisory, managed services, distribution solutions, and analytics with its ComplianceAlpha® technology platform. For more information, visit **www.acaglobal.com**.

About Yuter Compliance Consulting

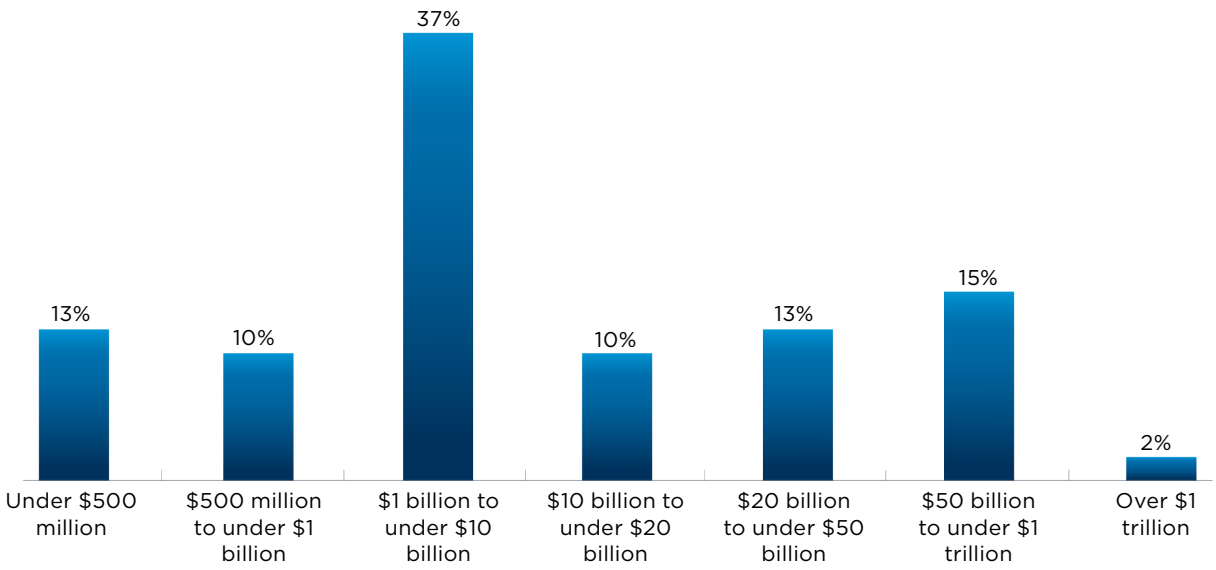
Yuter Compliance Consulting (YCC) is a leading, boutique compliance consulting firm, specializing in tailored consultation and support services for registered investment advisers, including asset managers, private equity firms, and hedge funds. Amy Yuter, Managing Principal of Yuter Compliance Consulting, has over three decades of industry experience, including as a regulator in the Division of Examinations at the U.S. Securities and Exchange Commission. As a thought leader in the compliance industry, Amy has made significant contributions. Amy is the founder of The Philadelphia Compliance Roundtable and the Investment Management Compliance Testing Survey. YCC partners with clients to provide personalized consultation and support to enhance compliance resources and improve compliance programs.

Our deep industry knowledge and regulatory expertise helps us in guiding clients to navigate the complex landscape of financial regulations. For more information, visit **www.yutercompliance.com**.

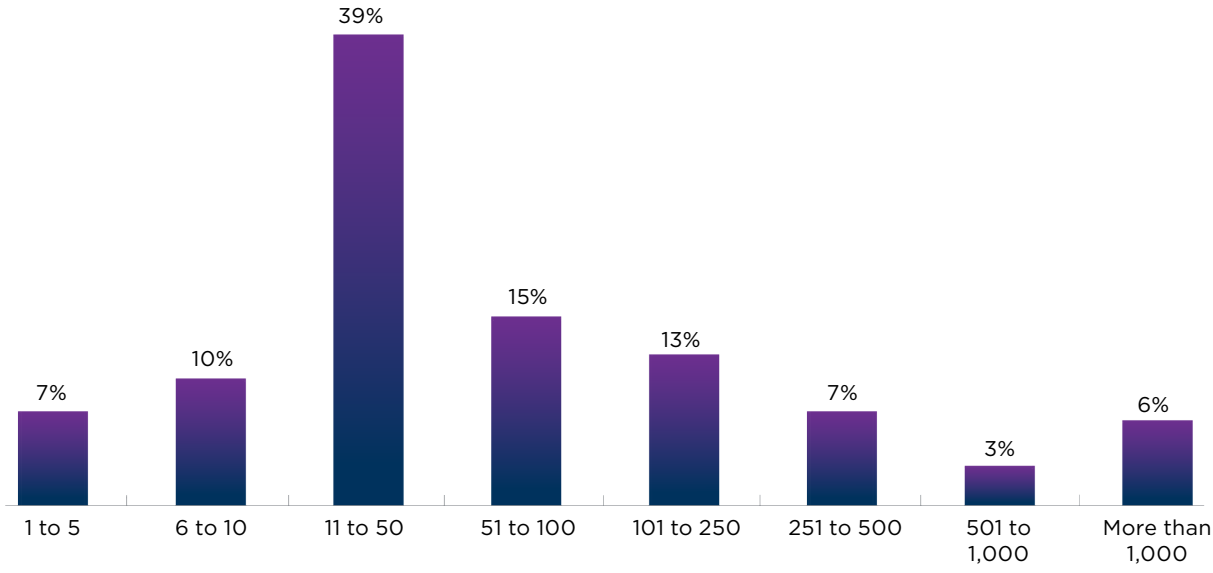
Note: Due to rounding, the sum of results may not equal 100%.

Appendix A: Demographics

What Is Your Firm's Total Regulatory Assets Under Management?

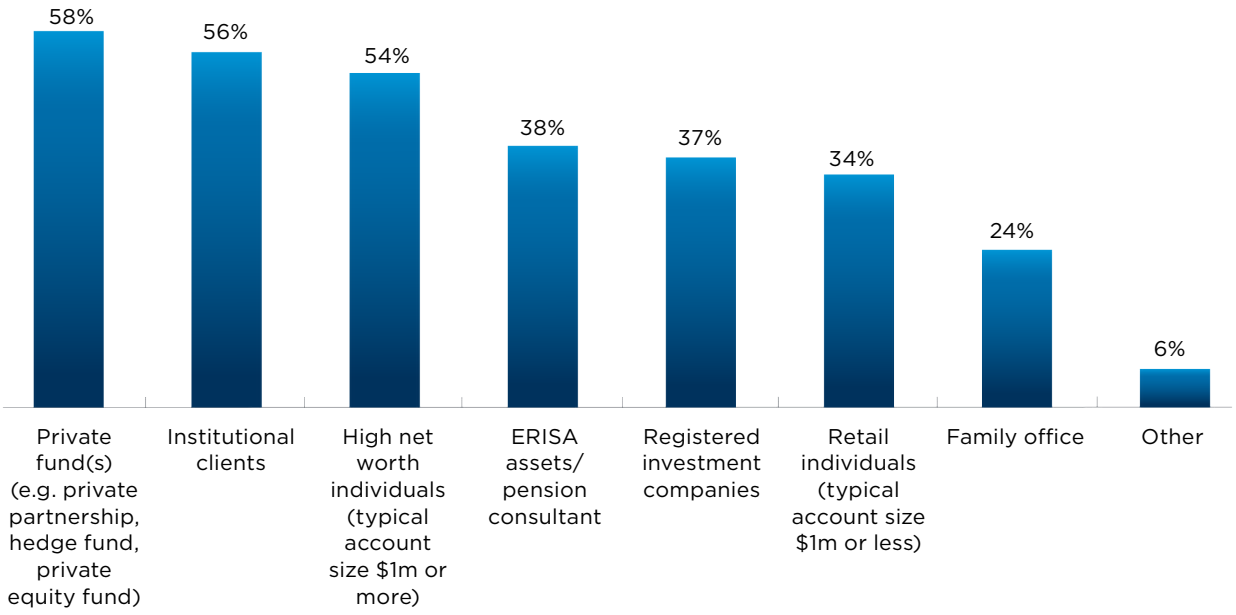


How Many Full and Part-Time Employees Does Your Firm Employ?



Your Firm Is an Investment Adviser To:

(check all that apply)



You Indicated That You Have at Least One Client That Is a Private Fund. Please Specify What Type of Private Fund Client(s) You Have.