Comply

AI Governance

The Gap Regulators Won't Overlook

It is impossible to get through the work week without having a conversation around AI. AI is a force multiplier moving at a lightning speed across financial services firms. Tech savvy firms deploying AI across departments and functions are seeing massive spikes in productivity and less time spent on labor-intensive (but critical) tasks like content development, data analysis, and document summarization – to name a few.

Technology innovation comes with risk, and AI is no exception.

Which begs the question: When was the last time your firm updated your policies and procedures around AI? And do you have a formal AI governance structure in place?

Comply's recent 2026 CCO & Compliance Leader Insights Report shows that **69%** of firms are already using AI in their compliance programs, yet only **49%** have formal governance policies in place to manage it. That makes sense: AI is moving faster than compliance teams can keep up with, but that doesn't' mean you're off the hook.

Regulators are going to start asking tough questions like: Where is AI being used in the decision-making process? Let's use a marketing review as an example. It's one of the most common uses of AI we're seeing in the market today.

If you're leveraging an AI tool to review your marketing materials – is it operating as a black box? Meaning, you can see the inputs and the outputs, but you don't truly understand how the system came to the conclusion. Regulators still need cold, hard proof of your decision-making process – regardless of what technology you use.

This guide explores AI and governance trends and what chief compliance officers (CCOs) can do now to build regulatory ready defensible oversight.
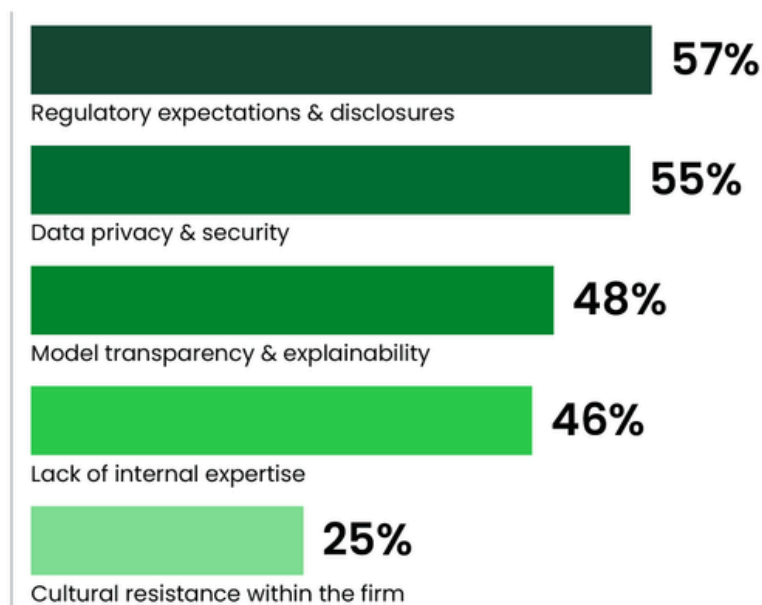
Let's dig in.

The Governance Gap

AI has augmented the way employees work and is moving at a pace that is difficult for compliance and IT teams to keep up with. Governance structures around the approved, ethical and responsible use of AI across departments, and geographies remain inconsistent. Many firms have deployed AI tools before defining ownership, testing requirements, or documentation standards. That lack of structure is emerging as a key area of regulatory concern and heightened risk to the business

Compliance leaders are clear about the risks. In the *2026 CCO & Compliance Leader Insights Report*, the top areas of anxiety include:

Top Concerns with Adoption of AI

Concern	Percentage
Regulatory expectations & disclosures	57%
Data privacy & security	55%
Model transparency & explainability	48%
Lack of internal expertise	46%
Cultural resistance within the firm	25%

These figures point to a simple truth: **awareness of risk is not the same as control.** Without defined governance, firms struggle to explain how AI systems reach conclusions, how outputs are validated, or who is accountable for errors.

That uncertainty can quickly become a compliance issue. Examiners expect firms to demonstrate that AI-driven decision-making, and activities are conducted with the same rigor applied to any other

compliance process. Establishing Policies and Procedures now will help firms stay prepared as expectations evolve.

Regulatory Expectations Are Outpacing Firm Readiness

Regulators have not issued AI-specific rules, but expectations are already taking shape through existing frameworks. The SEC continues to emphasize documentation, supervision, and accountability as essential under Rule 204-2 and Rule 206(4)-7. When technology influences compliance decisions, those same principles apply.

Our data shows that most compliance leaders recognize this shift. Respondents cited regulatory expectations (57%), data privacy (55%), and model transparency and explainability (48%) as top areas of concern.

Recent enforcement trends show how quickly technology risks can become exam priorities. Requirements for monitoring and archiving off-channel communications, for example, are rooted in long-standing regulatory obligations, not in new, standalone rules, though recent enforcement and interpretive guidance have clarified how these obligations apply to modern communication tools. Advancements in technology – like email and social media way back in the day – led to a new interpretation of the long-standing Books & Records requirements for firms. AI is following a similar trajectory: regulators are applying long-standing requirements to emerging technologies that shape firm decisions.

Firms must start documenting AI oversight and developing policies and procedures around the approved use cases for AI within the firm — including ownership, validation, and recordkeeping.

Building a Defensible AI Governance Framework

Regulators expect to see how it is AI is governed, and it's your job to show them. A defensible framework brings clarity to ownership, documentation, and accountability Across the industry, compliance leaders are calling for consistency: defined responsibilities, formal approval processes, and clear documentation for every system that informs compliance decisions.

A strong AI governance framework should include five core elements:

1. Ownership and Accountability

Assign a clear owner for every AI tool used within compliance. Outline responsibilities for approval, monitoring, and escalation. Oversight should sit with compliance leadership, not only IT, ensuring systems are validated and their purpose documented.

2. Policy and Procedures

Integrate AI into existing policies. Document approved use cases, data sources, and decision parameters. The clearer your use cases are, the easier it will be for your employees to follow the rules. Policies should specify when human review is required and how model changes are authorized.

3. Documentation and Recordkeeping

Maintain detailed records of model versions, inputs, and outputs in line with **Rule 204-2**. Retain AI-generated materials such as summaries, alerts, and scores to create an audit trail an examiner can follow.

4. Testing and Validation

Schedule periodic reviews to confirm accuracy, fairness, and consistency of our AI outputs. Capture testing results and any remediation steps. This demonstrates that models operate within controlled, documented parameters.

5. Training and Certifications

What happens when you create a new policy? You need to certify employees understand it and will follow it. Partner with HR and IT to educate employees on the purpose and limits of approved AI tools. Continuous training builds understanding and accountability across teams.

Key Takeaway: Implementing these elements signals readiness. It shows that AI is managed through established compliance processes, with transparency and control built in from the start.

Culture Is the Missing Control

Even the strongest frameworks depend on how people use them. Culture remains the most reliable indicator of program effectiveness, and one of the hardest to maintain as technology evolves.

The *2026 CCO & Compliance Leader Insights Report* found that while most firms rate their culture as generally strong, **41% of compliance leaders still see education gaps around AI use and governance. Many report uneven understanding of how automated systems fit into compliance responsibilities.**

Embedding AI oversight into culture starts with leadership. Executives and CCOs set the tone when they treat governance as an ongoing process, not a policy on paper. Training should move beyond annual refreshers to reinforce accountability throughout the year. Linking adherence to performance goals or supervisory metrics helps turn awareness into behavior.

Communication is equally important. Employees should understand when to rely on AI tools and when to escalate to human review. Creating open channels for feedback, especially around errors or model inconsistencies, builds trust and transparency.

A strong compliance culture ensures that governance doesn't live in isolation. It connects policy, technology, and people into one system of accountability. When culture supports control, AI becomes less a source of risk and more of a demonstration of operational maturity.

Where Compliance Goes Next

Firms that document ownership, validate outputs, and align AI oversight with existing policies will be better prepared for exams and better protected against risk. Those that delay will find that "waiting for guidance" is no defense when expectations are already in motion.

Key takeaways for compliance leaders:

- Integrate AI oversight into your core compliance framework.
- Define ownership and accountability across teams.
- Test, document, and retain records for all AI-driven activities.
- Reinforce culture through ongoing training and communication.

Comply provides technology and consulting designed to help firms operationalize AI governance. Our solutions connect policy, documentation, and oversight – giving compliance leaders a single, defensible system to manage emerging risks with confidence.

AI is here. Firms that implement sound governance frameworks are more likely to meet emerging regulatory expectations

Stay ahead of the AI curve

Let's Talk.