SurgeONE.ai
AI-Powered. Practitioner-Led

Responsible AI in a Principle-Based Regulatory Era

What SEC and FINRA Expect in 2026 and Beyond

Introduction

Artificial intelligence is no longer a future consideration for registered investment advisors or broker-dealers. It is already embedded across research workflows, portfolio analytics, marketing content, client communications, cybersecurity defenses, and operational processes. Often, this adoption has happened incrementally and informally, without a corresponding evolution in governance, supervision, or documentation.

At the same time, regulators are signaling a shift toward principle-based oversight. Rather than issuing prescriptive rules for every new technology, regulators are increasingly emphasizing accountability, reasonableness, and evidence of supervision. This creates both opportunity and risk. Firms have more flexibility in how they design compliance programs, but regulators have far less tolerance for ambiguity when something goes wrong.

AI growth demands defensible governance and supervision

This ebook examines how SEC and FINRA expectations are evolving in an AI-heavy environment and what compliance leaders must do to prepare for 2026 examinations. The focus is not simply on tools or trends, but on regulatory reasoning, supervisory responsibility, and defensible execution.

www.surgeone.ai info@surgeone.ai +1 650-294-8889

SurgeONE.ai
AI-Powered. Practitioner-Led

Chapter 1

The Reality Behind Principle-Based Regulation

Principle-based regulation is often described as a move away from rigid checklists toward flexible, outcome-oriented supervision. In theory, this approach allows regulators to keep pace with innovation without rewriting rules every time technology changes.

In practice, exams have not become less exacting. Examiners still arrive with matrices, standard inquiries, and established expectations tied to existing rules. As one enforcement expert noted, principle-based regulation "sounds good," but examinations remain grounded in the rulebook and its application to observable behavior.

What has changed is not the presence of rules, but the discretion examiners exercise in interpreting them. When guidance is less prescriptive, enforcement becomes the mechanism through which regulators clarify expectations. This creates a higher burden on firms to demonstrate that their interpretations are reasonable, well-documented, and consistently applied.

For compliance leaders, the implication is clear. Flexibility does not reduce risk. It shifts risk from rule violations to judgment failures. Firms are no longer asked only whether they followed a rule, but whether their choices, controls, and oversight reflect a thoughtful and defensible compliance posture..

Principle-based regulation creates space for stronger judgment and smarter compliance.

SurgeONE.ai
AI-Powered. Practitioner-Led

Chapter 2

Regulation by Enforcement & the Documentation Imperative

When rulemaking slows, enforcement fills the gap. Regulators may apply existing rules more strictly or reinterpret how those rules apply to new technologies. In these situations, precedent is often set through enforcement actions rather than formal guidance.

This reality places documentation at the center of regulatory defense. The strongest safeguard in an exam or enforcement inquiry is not intent, but evidence. As one compliance veteran emphasized, “document everything you’re doing” because books and records become the firm’s primary line of defense.

Many firms still rely on fragmented approaches to documentation, including spreadsheets, emails, and informal file notes maintained by different teams. These methods create gaps, inconsistencies, and version control issues that are difficult to reconcile under regulatory scrutiny.

Examiners increasingly expect to see centralized, consistent records that demonstrate how decisions are made, reviewed, and supervised. Documentation must show not only that policies exist, but that they are actively implemented, monitored, and updated. Scrambling to assemble records after receiving an exam notice signals weakness rather than diligence.

Well-documented decisions demonstrate control, consistency, and accountability.

SurgeONE.ai
AI-Powered. Practitioner-Led

Chapter 3

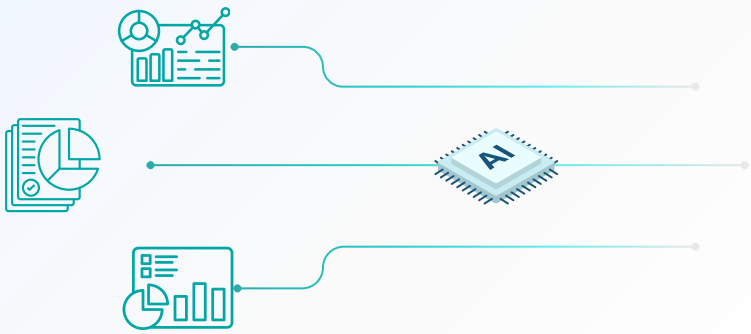
AI Use and the Expectation of Supervisory Control

AI presents a unique supervisory challenge because it is both powerful and accessible. Employees can adopt tools independently, often with minimal cost and little technical oversight. From a regulatory perspective, this informality poses a sizeable risk to a firm, and the ease of adoption without the firm's knowledge is not an excuse.

Regulators expect firms to know how and by whom AI is being used within their organizations. As one enforcement attorney stated plainly, firms "should have full visibility" into AI use, and if they do not, they are exposing themselves to potential civil litigation risk and significant regulatory risk.

This expectation mirrors prior enforcement trends around off-channel communications. Just as firms were held accountable for unauthorized messaging platforms, they are now responsible for unauthorized AI tools. The principle is the same. If a tool is used in the course of business, it falls under the firm's supervision and recordkeeping obligations.

A recurring theme in regulatory commentary is that responsibility cannot be delegated to technology. One SEC official has stated that firms cannot claim "it was AI's fault." The human supervisor remains accountable for outputs, decisions, and disclosures generated by AI systems.



Proactive AI supervision protects innovation while meeting regulatory expectations.

SurgeONE.ai
AI-Powered. Practitioner-Led

Chapter 4

Data Fragmentation, Cyber Risk, and Vendor Accountability

AI risk does not exist in isolation. It is deeply interconnected with cybersecurity, vendor management, and data governance. Fragmented systems and uncontrolled data flows magnify risk across all three areas.

Cyber threats are becoming more sophisticated as attackers leverage AI to automate phishing, malware development, and social engineering. Regulators increasingly view cybersecurity hygiene as a core compliance issue rather than a purely technical concern.

Vendor risk compounds this exposure. Firms are accountable not only for their own systems, but for the practices of third-party providers whom they choose to utilize. This includes understanding how vendors use AI, how they process client data, and whether those practices align with contractual obligations and privacy requirements.

Centralized governance turns regulatory expectations into operational confidence.

Many firms struggle simply to inventory their vendors, let alone assess AI usage across them. Regulators are now asking for vendor lists, due diligence records, cybersecurity policies, incident response plans, and technology governance procedures as standard exam requests.

Disconnected data systems further complicate compliance. When records are spread across tools, departments, and personal devices, firms lose the ability to produce consistent and reproducible evidence. Centralized data governance is becoming a regulatory expectation rather than an operational luxury.

SurgeONE.ai
AI-Powered. Practitioner-Led

Chapter 5

Preparing for 2026 Exams with Practical, Defensible Actions

Regulators are not expecting perfection. They are expecting preparation, awareness, and good-faith execution. Firms that acknowledge risk and take concrete steps to address it are in a far stronger position than those that delay action in pursuit of ideal solutions.

Based on recent examinations and enforcement experience, firms should prioritize the following actions:

- Review and update written supervisory procedures to explicitly address AI use, cybersecurity, vendor due diligence, and vendor oversight.
- Establish and document an AI acceptable use policy, including permitted tools, prohibited uses, and escalation procedures.
- Conduct discovery to identify shadow AI, note-taking tools, and unapproved applications used by their staff.
- Maintain centralized documentation of vendor due diligence, including AI disclosures and data handling practices.
- Firms should implement automated threat-intelligence monitoring—such as configuring Google Alerts—for each third-party vendor to detect indications of privacy incidents, data exposure events, or cybersecurity breaches.
- Test cybersecurity and incident response plans through tabletop exercises and retain evidence of those tests.
- Assign clear ownership for AI governance, whether through a designated officer or ca ross-functional committee.

When firms act early, exams become conversations, not confrontations.

As one advisor to firms noted, having an AI policy that is still maturing is preferable to having none at all. Regulators can work with a reasonable framework, but the absence of one leaves little to defend.

SurgeONE.ai
AI-Powered. Practitioner-Led

Conclusion

From Tool Adoption to Accountability

AI adoption is inevitable. Regulatory scrutiny is unavoidable. The defining question for compliance leaders is not whether AI will be used, but whether its use can be explained, documented, supervised, and defended.

The move toward principle-based regulation does not reduce regulatory risk. It increases the importance of judgment, documentation, and governance. Firms that treat AI as a compliance issue, rather than a purely operational one, will be best positioned to navigate the 2026 regulatory exam cycle and beyond.

Responsible AI adoption is not about innovation for its own sake. It is about aligning technology with fiduciary duty, regulatory expectations, and long-term trust. In a principle-based era, that alignment is what examiners are ultimately looking for.

If you would like to explore how your firm can responsibly adopt AI while meeting SEC and FINRA expectations, we invite you to learn more about how SurgeOne supports compliance teams in navigating this evolving regulatory landscape.

Learn more about SurgeOne's approach to responsible AI in compliance.

Book a Demo at **SurgeONE.ai** and future-proof your firm.

www.surgeone.ai
info@surgeone.ai
+1 650-294-8889