2026 SEC EXAMINATION INSIGHTS

20 AI Questions the SEC Is Asking RIAs in 2026 Exams

Real AI-related document requests from SEC examinations of RIAs, and the best practices that help you answer them.

Introduction

SEC examiners are no longer asking advisers *whether* they use artificial intelligence. They are asking firms to prove how they use it, what data feeds it, who supervises it, and whether client disclosures match reality.

AI adoption across the advisory industry has moved quickly. Advisers now use AI for investment research, marketing, client communications, data extraction, and meeting notes. Newer tools raise the stakes further: AI connectors that link chat platforms to CRMs and email, AI features quietly added to the software that firms already licensed, agentic AI that takes action before a human sees the result, and AI notetakers that record client conversations.

Regulators have noticed. Since the SEC's first "AI-washing" enforcement actions, firms that market their AI capabilities have faced pointed substantiation questions. Firms that use AI for core functions, such as managing portfolios, now face requests that look a lot like a full model-risk and vendor-oversight review.

Below is a compilation of AI-related document requests drawn from actual SEC examinations of registered investment advisers in 2026. We have grouped the requests by theme and noted what examiners appear to be testing in each area. We close with practical best practices CCOs can put in place now, so that if this list lands on your desk, you are ready to answer it.

> One point stands out across every request: **where there is AI, there is SEC interest.** Even firms with modest AI use should expect questions about inventory, disclosures, data security, supervision, and training.

The 2026 SEC AI Exam Request List

The 20 requests below fall into four themes. Request language is reproduced as examiners issued it, lightly edited for readability.

1. How you describe AI to clients and prospects

> *What examiners are testing:* whether your marketing and disclosures accurately reflect how AI is actually being used and the risks of that AI use.

- **AI Disclosures and Marketing.** All disclosure and marketing documents to clients where the use of AI by the Adviser is stated or referred to, specifically in the disclosure. Include all audio and video marketing in which the Adviser's use of AI is mentioned.
- **AI Use.** (i) Categorize and describe all AI used for: (a) portfolio management; (b) risk; (c) prospecting; (d) marketing; (e) customer experience; (f) performance; and (g) fraud prevention. (ii) Provide disclosures relating to the utilization of AI, including disclosures concerning risks associated with such use.
- **AI-Robo Investing.** Describe all artificial intelligence, predictive analytics capabilities, or robo-advisor technology.

2. Models, signals, and performance

> *What examiners are testing:* whether you understand, document, test, and validate the AI that touches investment decisions and client suitability.

- **Description of AI Models and Techniques.** A written description of all distinct AI-based models and techniques developed and implemented by the Registrant to manage client portfolios or make investment decisions and transactions since inception. This would include any formal model document and/or memos/PowerPoints that discuss how the model is specified, tested, and performed.
- **AI-Robo Investing:** Please describe all artificial intelligence, predictive analytics capabilities, or robo-advisor technology.
- **List of Algorithmic Trading Signals and Associated Models.** List and description of all algorithmic trading signals generated by AI models during the Examination Period. For each signal, list input data sources along with their vendor or, if generated in-house, method of acquisition, as well as primary data inputs.
- **Client Profile Documents.** Sample client profile documents used by the AI system to understand each client's risk tolerance and investment objectives.
- **Performance Evaluation Reports.** Reports on the AI models' performance over time and under various market conditions.
- **Model Validation Reports.** Samples of any reports detailing the validation process and performance of artificial intelligence algorithms.

3. Data: sources, providers, errors, and security

> *What examiners are testing:* where AI inputs come from, how they are obtained and maintained, what happens when data goes wrong, and how sensitive information is protected.

- **Data Sources.** List of all data sources utilized by artificial intelligence systems, including: (a) item name; (b) description; (c) source; (d) manner of acquisition; and (e) related trading or other strategy.
- **Data Source Providers.** List of contracted data source providers utilized by Registrant during the examination period, list of the "in-house" alternative data sources, and description of how each is obtained and maintained (e.g., web scraping).
- **Data Acquisition Errors and Adjustments.** List and description of all data acquisition errors and/or adjustments to algorithmic modifications due to data acquisition errors (i.e., web scraping problems) during the examination period, including the date and reason for adjustment.
- **Data Security.** Documentation on data security measures when using AI.

4. Governance, policies, and people

> *What examiners are testing:* whether a real supervisory structure surrounds AI, with written policies, accountable people, training, and a plan for when things fail.

- **Compliance Policies and Procedures.** All written compliance and operational policies and procedures concerning the supervision of all AI systems utilized by the Registrant. If any material amendment was made to these policies and procedures during the Examination Period, describe the amendment and when it became effective.
- **AI Governance, Controls, and Accountability.** Please provide Registrant's procedures to govern, supervise, test, and defend disclosures surrounding AI.
- **Contingency Plans.** Documents detailing contingency plans in case of AI system failures or inaccuracies.
- **Incident Reports.** Reports on any incidents where AI use raised any regulatory, ethical, or legal issues.
- **Supervised Persons.** A list of the Adviser's Supervised Persons employed by, or active with, the Adviser during the Examination Period who develop, implement, operate, manage, or supervise AI software systems, including for each: (a) title/position with the Adviser; (b) areas of responsibility, including committees involving the supervision, monitoring, development, or operation of AI software programs; (c) position held with affiliated entities (if applicable); (d) office location (if multiple) and DBA name (if applicable); and (e) hire date (year only is acceptable if prior to the Examination Period).
- **Compliance Training.** Written guidance the Adviser provided to its employees regarding the compliance program, and documents evidencing employee compliance training during the Examination Period specifically addressing AI.
- **Committees.** A list of all Board, management, or staff committees with specific AI-related responsibilities. Include a description of each committee's responsibilities, meeting frequency, and members, and indicate whether the committees keep written minutes and receive written materials to review as part of their meetings.

> One request worth highlighting: the contingency-plan question. Although AI use is relatively new, RIAs are using it at an increasing rate and tasking AI with core functions, so examiners are treating AI much like a key service provider. If AI performs a core function or a task tied to your fiduciary duty, expect close scrutiny of the controls and supervision around it. Firms have also recently been asked how they use AI to write code that implements analytical methods. Examiners want to understand the process and its oversight, not the code itself.

Best Practices for CCOs and RIAs

The firms best positioned for these requests treat AI like any other high-risk vendor or system: inventoried, approved, configured, supervised, and documented. The practices below map directly to what examiners are asking for.

1. Start with an AI inventory and risk assessment

You cannot supervise, disclose, or defend AI you don't know about. Begin with an audit that identifies every AI tool in use, what it does, what data it touches, and who uses it. Categorize uses the way examiners do: portfolio management, risk, prospecting, marketing, customer experience, performance, and fraud prevention. Then assess each for vulnerabilities, gaps, and exposure.

2. Conduct vendor due diligence on every AI product, including add-ins

- Run all AI products through vendor due diligence, especially if the platform is a service provider under amended Regulation S-P.
- Ask about AI usage in *all* vendor due diligence. Many vendors do not heavily advertise new AI features.
- Do not assume an approved application's new AI features are approved too. Review updated contracts, terms of service, and data processing agreements before use.
- Confirm whether firm or client data may be used to train the vendor's models. Embedded or "free" AI features often do.
- Disable AI add-ins in existing platforms unless they have been formally reviewed and approved.

3. Put it in writing: AI policy and software development lifecycle policy

- Adopt an AI acceptable use policy that names permitted and prohibited tools, platforms, and use cases. Update it before rolling out any expanded use.
- Add a software development lifecycle policy if staff build AI tools, prompts, or code. A simple model works: a builder creates the tool, a reviewer confirms it works as intended, an approver weighs business value, and a small beta group tests it before firm-wide release.
- Document shared tools and consider storing them in a code repository with review before release.
- Track material amendments and effective dates. Examiners ask for both.

4. Configure AI platforms for compliance

Use the highest enterprise or business tier available. Higher tiers are typically more secure and allow firms to customize security settings. Using an enterprise AI platform such as Claude Enterprise as an example, key configuration steps include:

- Set data retention to match your books and records policy, rather than accepting the default.
- Enable the platform's compliance or audit API so chats and files can feed your archive and supervision process.
- Approve connectors centrally, and set any tool that writes, sends, or deletes data to require human approval.
- Make a deliberate decision on agentic features, which may be on by default. If enabled, start with a small group of experienced users.
- Limit browsing and code execution to approved sites.
- Enforce single sign-on, use automated provisioning so access ends when employees leave, and use roles to restrict advanced or agentic tools to technical users.

5. Keep a human in the loop and defend against prompt injection

Generative AI leaves a human as the decision maker; agentic AI acts before a human sees the result. Either way, regulatory obligations do not transfer to the AI vendor. Prompt injection, where malicious instructions hidden in emails, documents, web pages, or CRM notes hijack an AI tool, makes oversight essential. To reduce risk:

- Require human approval for higher-risk actions such as sending emails, executing code, sharing sensitive data, or finalizing client documents.
- Verify output accuracy and require AI to cite sources.
- Follow the principle of least privilege for both users and AI tools.
- Keep AI tools and integrations patched, and monitor activity with endpoint detection, SIEM, and intrusion detection tools.

6. Handle AI notetakers deliberately

AI notetakers are among the most widely adopted tools, and they raise distinct issues. Address consent (several states require all-party consent to record), recordkeeping (transcripts or summaries sent to clients, or used to document instructions or decisions, must be retained), privacy of personal information and MNPI, discovery exposure, and the risk of waiving attorney-client privilege by sharing communications with a third-party vendor. Be transparent with clients when these tools are in use.

7. Train employees and monitor usage

- Provide routine, AI-specific training covering permitted tools, prohibited uses, prompt injection, and data handling. Keep evidence of completion.
- Monitor for both approved and unapproved use. Shadow AI, such as an employee using a free consumer tool on a company device, is a real risk.

- Use platform logs, custom usage reports, device-level software that monitors popular language models, or third-party monitoring tools. Trust, but verify.
- Conduct periodic access reviews and audit AI agents to confirm they still work as intended.

8. Validate outputs and plan for failure

For AI that supports critical business functions, benchmark actual results against intended results, especially after material changes. Log data errors and the adjustments made in response. Document a contingency plan that answers a simple question: what happens if this AI system fails or produces inaccurate output?

9. Substantiate every AI claim

If you market AI, make sure your actual use matches what your marketing says, including audio and video. Maintain a file that supports each AI-related statement in your Form ADV, website, pitch materials, and client communications, and review it whenever your AI use changes.

What Does This Mean for Me?

The message from these exam requests is clear: AI is now squarely within the scope of an SEC examination, and examiners expect advisers to govern it with the same rigor they apply to portfolio management, vendor oversight, and cybersecurity, even in the absence of a formal rule.

The good news is that the expectations are knowable. Read the list above as a readiness checklist. If you could not produce a response to a request today, we suggest starting there. For most firms, the starting point is the same: know what AI you use, put clear policies around it, configure tools securely, train your people, monitor what actually happens, and make sure every claim you make about AI can be backed up.

AI can make things go really well, or really badly, really fast. A thoughtful compliance framework lets your firm capture the efficiencies AI offers while staying prepared for the questions examiners are already asking.

Need help getting exam-ready? Fairview helps RIAs conduct AI audits and risk assessments, draft AI and software development lifecycle policies, deliver AI-specific employee training, and set up AI usage monitoring. Visit fairviewinvest.com to learn more.

This article is provided for informational purposes only and does not constitute legal advice. Firms should consult their compliance and legal advisers regarding their specific circumstances.