AI Due Diligence Checklist

Four points for regulated financial firms, from Larry Shumbres at NSCP 2026

1 Build an AI inventory

- [ ] Is every AI tool in use at the firm on the inventory, including tools individual advisors use?[1]
- [ ] Does each tool have an owner and a written approved use?[1]
- [ ] Are approved uses in the supervisory procedures, and do advisors know which tools are approved?[1, 6]
- [ ] Is there a formal review and approval step before a new AI tool goes live?[1]
- [ ] For larger firms, does an AI control plane or MCP gateway centrally govern which AI tools are used and what data they can access?[7]

2 Review each vendor's AI and privacy policies

- [ ] Do the policies state whether firm or client data is used to train models?[1]
- [ ] Do they state where data is stored and whether third-party AI models are involved?[1, 2]
- [ ] Is it documented which firm data the vendor's AI can reach and which systems it connects to?[2]
- [ ] Are security attestations current, with ongoing reviews scheduled?[2, 3]

3 Add Data Processing Agreements (DPAs) to service agreements

- [ ] Is a DPA part of the service agreement?[7]
- [ ] Does the contract prohibit firm or client sensitive information from being ingested into the vendor's open-source GenAI tools?[2]
- [ ] Does the contract require the vendor to notify the firm as soon as possible, and no later than 72 hours, after becoming aware of a security breach resulting in unauthorized access to a customer information system the vendor maintains?[3]

4 Confirm the vendor provides audit logs of AI activity

- [ ] Does the vendor provide audit logs of AI activity, such as prompt and output logs, and does the firm know how to get them?[1]
- [ ] Are AI-assisted client communications and chatbot interactions supervised and retained like other communications?[4, 6]
- [ ] Has the firm decided which AI meeting notes and summaries it keeps as records, and can it produce them for a given client and date?[5]
- [ ] Is evidence of supervisory review of AI use retained?[6]

Sources for each question are listed on page 2.

Sources

Each question on the checklist is numbered to the source below. Regulatory references are current as of November 2026. This checklist is a starting point for a firm's own review and is not legal advice.

1. **FINRA, 2026 Annual Regulatory Oversight Report (December 2025), Generative AI section.** Effective practices include "formal review and approval processes" for GenAI, assessing risks of "third-party vendors' use of GenAI," and "storing prompt and output logs for accountability."
   finra.org/sites/default/files/2025-12/2026-annual-regulatory-oversight-report.pdf

2. **FINRA, 2026 Annual Regulatory Oversight Report, Third-Party Risk Landscape section.** Effective practices include Effective practices include contract language thatldquo;initial and ongoing due diligenceEffective practices include contract language thatrdquo; on vendors, contract language that "prohibits firm or customer sensitive information from being ingested into a third-party vendor's open-source GenAI tool" and an "inventory of firm data types accessed or stored by the firm's vendors."
   finra.org/sites/default/files/2025-12/2026-annual-regulatory-oversight-report.pdf

3. **SEC, Regulation S-P amendments, Small Entity Compliance Guide (2024).** Covered institutions must have written policies and procedures for oversight of service providers, including notice "as soon as possible, but no later than 72 hours after becoming aware" of a breach resulting in unauthorized access to a customer information system the provider maintains. Compliance dates: December 3, 2025 for larger entities and June 3, 2026 for smaller entities.
   sec.gov/files/rules/final/2024/regulation-s-p-small-entity-compliance-guide.pdf

4. **FINRA, 2026 Annual Regulatory Oversight Report, Communications with the Public section.** When GenAI assists with chatbot communications to investors, firms should ensure "the appropriate supervision and retention of those communications, and retention of those chat sessions."
   finra.org/sites/default/files/2025-12/2026-annual-regulatory-oversight-report.pdf

5. **FINRA, Regulatory Notice 25-07 (April 14, 2025).** FINRA asks how recordkeeping challenges vary by type of AI-generated communication, including "AI-generated transcripts or summaries of meetings." How these records are treated remains an open question, so firms set their own approach.
   finra.org/sites/default/files/2025-04/Regulation-Notice-25-07.pdf

6. **FINRA, Regulatory Notice 24-09 (June 2024).** FINRA rules apply to Gen AI the same as any other technology. Under Rule 3110, a firm must have "a reasonably designed supervisory system tailored to its business."
   finra.org/rules-guidance/notices/24-09

7. **Larry Shumbres, NSCP 2026 National Conference panel, "AI & GenAI in Compliance: From Productivity Booster to Regulatory Risk."** The four points, Data Processing Agreements, and the AI control plane or MCP gateway for larger firms are Larry's recommendations as good practice, beyond what the rules require.