GiGCXOs

AI Compliance Outsourcing Checklist

Broker-dealer and investment adviser use case review guide

Use this checklist before adopting AI for surveillance, communications review, marketing review, trade monitoring, books and records support, risk management, or related compliance workflows.

Prepared for	GiGCXOs clients and prospects
Intended users	Chief Compliance Officer, CEO, Operations, IT, Legal, and vendor management
Date	March 10, 2026

This checklist is a practical compliance tool, not legal advice. Each firm should tailor its review to its business model, disclosures, recordkeeping obligations, supervisory system, and vendor stack.

Purpose and How to Use This Checklist

This document helps a broker-dealer or SEC-registered investment adviser evaluate whether an AI solution can be used in a manner consistent with existing regulatory obligations. It is designed for both outsourced compliance engagements and internal diligence before deployment.

Core regulatory themes that apply to AI use

Even without a standalone AI rule in effect, existing SEC and FINRA requirements still apply when a firm uses AI in its business or supervisory system.

- Supervision: Firms must maintain a reasonably designed supervisory system, written supervisory procedures, and documented review processes.
- Books and records: AI-generated or AI-assisted communications, alerts, evidence, approvals, and exception handling may create retention obligations.
- Data protection and Reg S-P: Customer information, including nonpublic personal information and sensitive customer information, must be safeguarded with written controls and incident response planning.
- Vendor management: Outsourcing does not outsource regulatory responsibility. Firms must diligence, contract with, monitor, and test vendors supporting compliance functions.
- Accuracy, explainability, and escalation: Human reviewers remain accountable for final compliance judgments, especially when the model produces false positives, false negatives, or unsupported output.

Readiness snapshot

Check	Readiness item	Owner	Status
□	Business use case is clearly defined and limited to approved compliance tasks.		
□	Compliance, IT, legal, operations, and senior management have reviewed the use case.		
□	The firm has identified what data the tool will access, store, and transmit.		
□	The firm has determined how human review and escalation will work.		

Check	Readiness item	Owner	Status
□	WSPs, vendor contracts, testing, and books and records controls are addressed before launch.		

1. Assess the firm's compliance needs

- Identify the exact compliance activity the tool will support, such as advertising review, electronic communications review, exception triage, trade surveillance, code of ethics monitoring, or branch supervision.
- Define the business problem being solved, the manual process being replaced or supplemented, and the measurable compliance objective.
- Document whether the AI output is advisory only, workflow support, or a control that can affect an approval, escalation, or surveillance outcome.
- Identify applicable rules, books and records requirements, and escalation obligations before configuration begins.

2. Research and diligence AI solutions

- Confirm whether the product uses rules-based logic, machine learning, large language models, or a combination of methods.
- Determine whether the vendor uses your firm data to train public or shared models.
- Review accuracy claims, model limitations, false positive and false negative rates, and any explainability tools available to reviewers.
- Confirm where data is stored, how long it is retained, and whether subcontractors or fourth parties are involved.

3. Engage key stakeholders

- Involve compliance, IT security, legal, operations, records management, and business owners in the evaluation.
- Assign a business owner, control owner, technology owner, and escalation owner for the tool.
- Determine whether board, senior management, or committee reporting is needed based on the tool's risk profile.

4. Pilot the tool in a controlled setting

- Run the AI solution in a limited pilot using a defined data set, date range, or business line.
- Compare AI results to the firm's current manual review process and document the differences.
- Measure speed, hit rate, exception quality, reviewer burden, and missed issue rates before broad deployment.

5. Customize to firm requirements

- Tune prompts, lexicons, thresholds, rule sets, exception categories, and workflows to the firm's actual products, communications, and risk profile.

- Block prohibited inputs such as customer NPI, account credentials, or source code unless specifically approved and secured.
- Establish documented confidence thresholds and escalation rules for ambiguous or high-risk outputs.

6. Integrate with existing systems

- Map system connections to email, chat, CRM, archiving, marketing review, OMS/EMS, trade surveillance, document repositories, and case management tools.
- Validate that integrations do not break retention, indexing, time stamping, approval logs, or supervisory evidence.
- Ensure secure file transfer and access controls are in place for any customer or firm-sensitive data exchanged with the tool.

7. Establish ongoing monitoring and oversight

- Assign periodic review of output quality, exception handling, prompt changes, model updates, and vendor releases.
- Create a process to detect model drift, recurring hallucinations, or changing error patterns.
- Require human review for material determinations, novel fact patterns, and exceptions that could affect client treatment or regulatory reporting.

8. Train personnel

- Train staff on permitted and prohibited uses, approved prompts, data handling restrictions, escalation triggers, and books and records expectations.
- Require acknowledgement of the tool's limitations, including that users may not treat AI output as automatically correct.
- Refresh training whenever functionality, vendor terms, or regulatory expectations materially change.

9. Document the program

- Document use cases, data flows, approvals, testing results, configuration decisions, reviewer responsibilities, and change management.
- Retain evidence of pilot results, exception reviews, overrides, vendor diligence, and periodic testing.
- Maintain an inventory of AI tools, embedded AI features, and business owners.

10. Stay current on regulatory and firm changes

- Track new FINRA and SEC guidance, enforcement trends, cybersecurity developments, and Reg S-P implementation changes.
- Review whether the tool remains appropriate when the firm adds products, channels, third-party vendors, or new communication platforms.

11. Audit and test regularly

- Schedule periodic testing under the firm's supervisory control system and annual review framework.

- Test sampling methods, exception closure quality, books and records capture, and access controls.
- Document remediation steps, owners, and target dates for any gaps.

12. Evaluate whether to scale

- Scale only after the pilot demonstrates that the tool improves the process without weakening supervision, retention, privacy, or evidence quality.
- Expand in phases by use case, business line, or data type, with re-approval at each stage.

Questions a broker-dealer or investment adviser should ask before using AI

Area	Questions to ask before launch	Why it matters
Governance	Who approved this use case, who owns it, and who can change prompts, thresholds, or model settings?	Prevents unmanaged changes to a control environment.
Use case scope	Is the tool merely assisting a reviewer, or can it influence approvals, exceptions, disclosures, client communications, or surveillance outcomes?	Determines risk rating and control design.
Supervision	How will the firm supervise the tool's output, sampling, overrides, and exception handling under WSPs?	AI use must fit within the firm's supervisory system.
Books and records	What records must be retained, where are they stored, and will prompts, outputs, approvals, and escalation notes be captured?	Evidence may be needed for exams, audits, or investigations.
Accuracy	What is the known error rate, when does the model hallucinate, and how will the firm test reliability before and after deployment?	Weak output can create missed issues or bad decisions.
Data access	What firm, customer, employee, issuer, or market data will the tool ingest, and is any of it NPI or sensitive customer information?	Supports privacy and data minimization.
Privacy and Reg S-P	Could the tool expose customer information, credentials, account data, or authentication data, and how would the firm detect, respond to, and recover from an incident?	Reg S-P requires written safeguards and incident response planning.
Vendor risk	Does the vendor train on firm data, use subprocessors, allow opt-	Outsourcing does not

Area	Questions to ask before launch	Why it matters
	out, and contractually restrict use or disclosure of firm and customer information?	shift compliance responsibility.
Cybersecurity	Are encryption, access controls, logging, secure file transfer, incident notification, and data deletion standards contractually defined?	Controls reduce breach and leakage risk.
Communications	Could the tool draft or alter client-facing content, marketing content, or registered representative communications?	Triggers communications content standards and review obligations.
Escalation	Which outputs require principal review, legal review, manual escalation, or suspension of the tool?	Ensures people intervene on high-risk matters.
Conflicts and fiduciary issues	Could the tool optimize for firm revenue, steer recommendations, shape disclosures, or otherwise affect investor treatment?	Advisers and broker-dealers must avoid or manage harmful conflicts.
Testing	How often will the firm retest prompts, workflows, and model performance after vendor updates or business changes?	Controls can degrade over time.
Business continuity	What happens if the tool goes down, produces degraded output, or the vendor suffers a cyber event?	Critical compliance functions need fallback procedures.
Termination	How will the firm retrieve, delete, or transition data and evidence when the contract ends?	Required for vendor offboarding and records integrity.

Vendor diligence questions

Use these questions with any AI vendor, including vendors that embed AI into an existing archive, surveillance, CRM, email, chatbot, or marketing review platform.

- What data is used to train, fine-tune, or improve the model, and can the firm opt out completely?
- Does the vendor prohibit firm or customer sensitive information from being ingested into open-source or public models?

- What subprocessors, hosting providers, model providers, or fourth parties support the service?
- How are access rights managed, logged, reviewed, and revoked?
- What retention, deletion, export, and legal hold capabilities exist?
- What service levels, incident notification timelines, audit rights, and cybersecurity representations are in the contract?
- How does the vendor validate output quality, bias, drift, or degraded model performance?
- Can the vendor provide evidence of penetration testing, vulnerability management, secure development, and business continuity planning?
- Can the firm independently review prompts, thresholds, confidence scores, and workflow rules that affect compliance outcomes?

Recommended implementation sequence

Phase	What to do	Evidence to keep	Complete
1	Define use case and risk rating	Use case memo, stakeholders, rule map	□
2	Complete vendor diligence and contract review	Questionnaire, security docs, contract redlines	□
3	Pilot with limited data and human review	Pilot plan, test results, gap log	□
4	Update WSPs, controls, and books and records procedures	WSP changes, retention map, training plan	□
5	Launch with monitoring, metrics, and escalation	Launch approval, KPI dashboard, review logs	□
6	Retest periodically and reapprove material changes	Annual review, exception summaries, remediation tracker	□

Selected regulatory references

- FINRA Regulatory Notice 24-09, Regulatory Obligations When Using Gen AI Tools (June 27, 2024).
- FINRA 2026 Annual Regulatory Oversight Report, GenAI: Continuing and Emerging Trends.
- FINRA 2026 Annual Regulatory Oversight Report, Third-Party Risk Landscape.
- FINRA Rule 3110 and FINRA Rule 3120 supervisory framework materials.
- FINRA Books and Records topic page.
- SEC Regulation S-P final amendments and small entity compliance guide (May 2024).

- SEC enforcement actions concerning electronic communications and recordkeeping failures, including January 13, 2025 settlement announcement.

Practical reminder: Do not place customer NPI or sensitive information into unapproved email, chat, or public AI tools. Use approved secure file transfer methods and firm-approved systems only.