

FOR INDEPENDENT RIAS · SUPERVISION

Supervising AI That Acts.

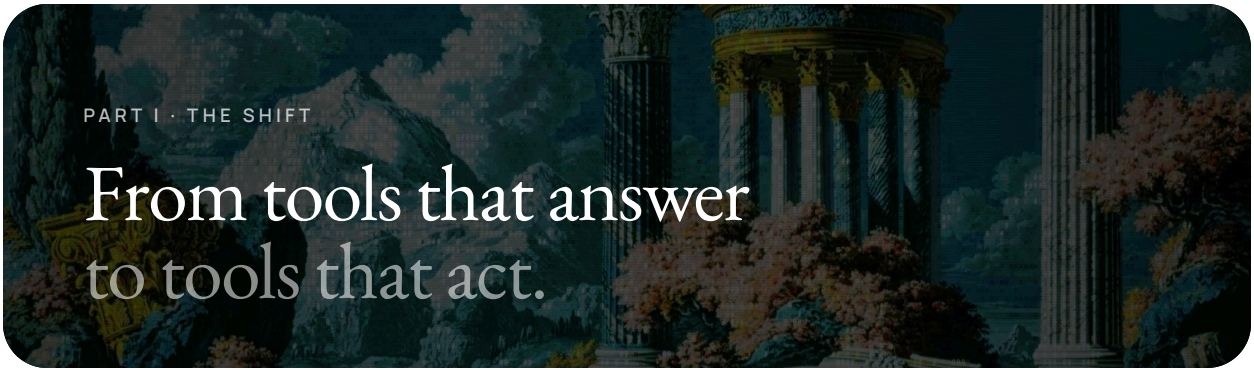
A compliance officer's guide to AI that signs in, prepares, and submits: four levels of authority, the rules that already apply, and a worksheet for approving each workflow.

Helmsted, Inc. · September 2026

helmsted.ai

INSIDE THIS GUIDE

01 Before it clicks Submit
02 Four levels of authority
03 No AI rule, and no gap
04 Custody: the access question
05 The record of an action
06 How FINRA describes agents
07 Six controls
08 The worksheet: approve one AI workflow
09 The Morgans, walked through
10 Models propose. Professionals decide. Helmsted executes.



PART I · THE SHIFT

From tools that answer to tools that act.

SECTION 01

Before it clicks Submit

An AI assistant retrieves a client's 401(k) fund menu, drafts a new allocation that fits the plan, and stages the change on the plan's website. Before anything is submitted, the firm needs three answers:

1. **Who authorized the action?**
2. **What, exactly, was approved?**
3. **What record will remain?**

No new rulebook is required to answer them. What is required is a way of supervising AI that follows what it is allowed to do, not what it is called. Products change names faster than policies can follow; authority, approval, and evidence do not.

No. 01 covered where client information goes. No. 02 covered the evidence that earns a system permission to act. No. 03 described the harness that makes delegation trustworthy. This installment is the chief compliance officer's working guide: how to classify AI by authority, what the existing rules ask, and a one-page worksheet for approving an AI workflow.

Supervise AI by what it can do, who approved it, and what it leaves behind.

SECTION 02

Four levels of authority

Classify each AI workflow by the authority it actually holds, meaning the permissions and access it has been given, not only what it is meant to do. A tool asked to retrieve a statement that signs in with access able to move money holds more authority than its task requires, and it belongs in the higher level until that access is narrowed. These four levels are Helmsted's framework, not a regulatory classification.

LEVEL	WHAT THE AI DOES	EXAMPLE	WHAT CAN GO WRONG	SUPERVISION
1. Answers	Explains or summarizes; nothing leaves the screen	Summarizing a meeting	A wrong fact an adviser repeats	Sources shown; adviser judgment
2. Drafts	Produces work product a person sends	A client letter or analysis	A wrong figure reaches a client	Review before release
3. Prepares	Gathers, assembles, and stages work in other systems, without changing anything outside the firm	Retrieving a fund menu; staging a form	Wrong account, wrong data, access broader than the task	Task authorization; scoped access; logged steps
4. Acts	Completes a step with an external effect	Submitting an allocation change	A mistaken or unauthorized change	Approval of the specific action; stop conditions; full record

Two kinds of permission run through the table, and it helps to keep them separate:

- **Task authorization** grants a bounded job in advance: retrieve this plan's fund menu, for this household, using this access, for this session. Levels 1 through 3 run on task authorization.
- **Action approval** approves one specific consequential step, with the exact change in front of the approver, immediately before it happens. In this framework, Level 4 requires it every time.

Most firms operate at Levels 1 and 2 today. Levels 3 and 4 are where the rules the firm already follows apply in new ways.



SECTION 03

No AI rule, and no gap

The SEC has not adopted an AI-specific rule for advisers; in June 2025 it withdrew its 2023 proposal on predictive data analytics. [1] AI remains governed by the rules already in place.

RULE	WHAT IT ASKS	WHERE AI THAT ACTS TOUCHES IT
Compliance rule, 206(4)-7	Written policies reasonably designed to prevent violations, reviewed at least annually	AI workflows belong in the policies and the annual review, by level of authority
Books and records, 204-2	Retention of required records, including certain written communications	Instructions, approvals, actions, and results may be records the firm must keep
Regulation S-P, as amended	An incident response program and oversight of service providers	AI vendors with access to customer information are service providers to oversee
Custody rule, 206(4)-2	Safeguards when an adviser can obtain client funds or securities	Access that could move client assets may raise custody questions
Marketing rule and antifraud, 206 and 206(4)-1	Accurate representations to clients and prospects	What the firm says about its AI must match what the AI does

The SEC's 2026 examination priorities point the same way: examiners will review firms' representations about their AI capabilities, their policies for monitoring and supervising AI, and compliance with amended Regulation S-P. [2][3] In March 2024, the SEC settled charges against two advisers for misleading statements about their use of AI, the first "AI washing" cases of their kind. [4]

SECTION 04

Custody: the access question

SEC staff guidance holds that an adviser with password access to a client account has custody if that access provides the ability to withdraw funds or securities, or to transfer them to an account not in the client's name. [5] The guidance predates AI agents and does not address them specifically. The same access question is relevant when software acts for the adviser.

Three practical questions frame the analysis:

- **Whose credentials, and whose session?** Does the firm, or a vendor acting for the firm, hold the client's login, or does the client sign in and control the session?
- **What can the session do?** Access that can only view is different from access that could move money, whether or not the tool intends to.

- **How long does access last?** A session that exists for one task differs from standing access that persists.

These questions inform the analysis; they do not settle it. Client approval and short-lived access do not, by themselves, resolve whether an arrangement implicates the custody rule. The facts of each arrangement matter, and firms should review them with counsel before a workflow goes live.

SECTION 05

The record of an action

An AI that answers leaves a transcript. An AI that acts leaves a trail. For any Level 3 or Level 4 workflow, the firm should be able to produce, in one place:

1. **The instruction.** Who asked for the work, and what they asked for.
2. **The authorization or approval.** Who granted it, when, and with what in front of them.
3. **The action.** What the system did, in which system, under whose authority.
4. **The result.** What changed, and how it was confirmed.
5. **The evidence.** The sources the work relied on.

Whether each element is a required record under Rule 204-2 depends on its content; written communications relating to advice or to the placing or execution of orders, for example, generally are. [6] Keeping the chain together is the starting point, not the finish line. Map each element to the firm's retention schedule, and test that the record can be retrieved, exported, and protected against alteration for the full retention period.

SECTION 06

How FINRA describes agents

FINRA regulates broker-dealers rather than advisers, but its 2026 oversight report describes AI agents and their risks in terms any CCO can use: autonomy without human validation, agents exceeding their intended scope, multi-step reasoning that is hard to audit, and unintended disclosure of sensitive data. Its effective practices include human-in-the-loop checkpoints, tracking of agent actions, and guardrails on behavior. [7]



PART III · THE PROGRAM

Approve one AI workflow.

SECTION 07

Six controls

The controls below are editorial recommendations, designed to sit inside an existing compliance program. The rules in Part II set the obligations; these are one way to meet them.

1. Inventory by actual authority. List every AI workflow, including features inside existing tools, and assign each a level based on the access it holds. Revisit the list at the annual review and whenever a vendor adds a capability.

2. Match permission to the level. Levels 1 and 2: adviser review before anything reaches a client. Level 3: task authorization, scoped to the task. Level 4: action approval of the specific step, by a named person, immediately before it happens. Where the step is in a client's own account, the client approves it.

3. Scope access to the task. Access should be granted for a task, limited to what the task needs, and end when the task ends. The firm should know, for every workflow, whether any session could move client assets.

4. Keep one record of the chain. Instruction, authorization or approval, action, result, and evidence, mapped to the retention schedule and tested for retrieval.

5. Plan for stopping and recovery. Decide in advance who can pause a workflow or revoke its access, and how quickly. Define what happens after a partial completion, and treat an uncertain result as unconfirmed: if a submission times out, verify whether it succeeded before retrying. Test each workflow before deployment and after material changes, then sample completed work on a set cadence; quarterly is a reasonable starting point for most firms.

6. Say what the AI actually does. Review Form ADV, the website, and client materials against the inventory, and describe each AI role and its limits as they stand today.

SECTION 08

The worksheet: approve one AI workflow

Complete one page per workflow before it goes live, and keep it with the compliance records.

FIELD	ENTRY
Workflow	*e.g., Retrieve and update 401(k) allocations for advisory clients*
Owner	*The person accountable for the workflow*
Maximum level of authority	*1 Answers · 2 Drafts · 3 Prepares · 4 Acts*
Systems and data it may use	*Which systems, which household data, which credentials or sessions, and whose*
Can any session move client assets?	*Yes / No. If yes, counsel review completed on (date)*
Task authorization	*Who grants it, and for what scope*
Action approval	*Who approves each Level 4 step: adviser, client, or both*
Prohibited actions	*e.g., no transfers or withdrawals; no changes to contact details*
Stop conditions	*Conflicting facts, changed amounts, uncertain recipients, errors, timeouts*
Pause and revoke	*Who can stop it, and how*
Evidence retained	*Instruction, approval, action, result, sources; where kept; retention period*
Testing	*Before deployment; after material changes; sampling cadence*
Disclosure check	*Form ADV and client materials reviewed on (date)*
Next review	*Date*

The worksheet also serves as a vendor conversation. A vendor that cannot supply the answers to fill it in has answered a different question. No. 02 covers the broader evidence to request, including independent assurance such as a SOC 2 report and, under amended Regulation S-P, oversight

procedures reasonably designed to ensure the vendor notifies the firm as soon as possible, and no later than 72 hours, after becoming aware of a breach resulting in unauthorized access to a customer information system it maintains. [3]

SECTION 09

The Morgans, walked through

The Morgans, the fictional couple three years from retirement who have appeared throughout this series, want to know whether Mr. Morgan's 401(k) investments still fit their plan.

Level 3, preparing. The fund menu exists only on the plan's website. Mr. Morgan signs in to his own account in a secure browser session; the firm never receives his password. The workflow limits this session to viewing and collecting information; it cannot submit changes, which is what keeps this step at Level 3. Under the task authorization, the system retrieves the fund menu and fees and files them in the household record with their source.

Level 2, drafting. The system drafts an allocation that fits the plan, citing each fund's details. The adviser changes one fund and approves the recommendation.

Level 4, acting. In a new session Mr. Morgan opens, the system enters the approved allocation on the plan's change screen and stops. Mr. Morgan sees the exact change, fund by fund, and approves it. The system submits it within his session and records the plan's confirmation.

The exception. Suppose the plan's screen shows a fund the adviser removed, or a percentage has shifted since approval. The system does not submit. It stops and shows the adviser the difference. If the allocation can no longer be entered as approved, the adviser revises the recommendation, and Mr. Morgan approves the final change. If the submission times out, the system checks the account for the change before it tries again.

The record. A year later, the CCO pulls one entry: the question, the sources, the adviser's recommendation, Mr. Morgan's approval of the specific change, the submission, and the confirmation.



The adviser recommends. The client approves the specific change. The record keeps both.

This scenario is illustrative. Whether a particular arrangement for acting in client accounts implicates the custody rule depends on its facts.



SECTION 10

Models propose. Professionals decide. Helmsted executes.

Helmsted is an AI-native operating system for independent RIAs, built on the structure this installment describes: AI drafts and prepares the work, advisers make the decisions, clients approve what is done in their own accounts, and Helmsted is rolling out the ability to carry out approved steps and record them. The table separates what is available today from what is rolling out, so a CCO can test each item.

WHAT A CCO CAN INSPECT	STATUS
Sources. Facts in the household record show their sources	Available
Adviser review. Work reaches a client only when the adviser publishes it	Available
Client questions. In the portal, advice questions go to the adviser with a summary	Available
Access and isolation. Passkey sign-in; firms isolated at the database level; permissions enforced by the application, not the AI model	Available
Activity records. Per-user audit logs	Available
Data terms. No training on client data, in the contract; public subprocessor list	Available
Independent assurance. Clean SOC 2 Type I report from Sensiba LLP, under NDA	Available
Browser control. Works in the web screens a firm uses, with approval at consequential steps	Rolling out
Client-controlled sessions. Clients sign in themselves and approve specific actions	Rolling out

Over time, Helmsted is being built to carry out the work a firm performs on a screen, with direct connections replacing the browser as they mature. Each capability arrives inside the same structure: a level of authority, an approval, and a record a CCO can inspect.

IN CLOSING

Supervise the authority, not the product.

Professionals decide

Authorize the task

Approve the action

Resolve exceptions

Helmsted executes

Within set permissions

Stops when facts change

Records each step

AI tools will keep changing names, vendors, and features. The questions a compliance officer asks will not: what the system can do, who approved it, and what it left behind. A program built on those questions holds up as AI moves from answering to acting, and it gives the firm the confidence to let AI do more of the work.

Know what your AI is allowed to do. Be able to prove what it did.

See what a CCO can inspect in Helmsted.

Thirty minutes with the team, and every security question answered.

Book a demo · helmsted.ai/demo

Sources and further reading

Research checked September 27, 2026. Bracketed numbers in the text refer to the sources below.

1. **SEC, withdrawal of proposed rules, including "Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers" (withdrawn June 2025; proposed July 2023).** Read the notice.
2. **SEC, "SEC Division of Examinations Announces 2026 Priorities" (November 17, 2025).** Read the release.
3. **SEC, Regulation S-P amendments, Release 34-100155 (2024).** Service-provider oversight and notification timing; compliance dates December 3, 2025 for larger entities and June 3, 2026 for smaller entities. Read the release. For the 2026 examination focus on AI and Regulation S-P, see also Goodwin, "2026 SEC Exam Priorities for Registered Investment Advisers" (December 2025), read the alert.
4. **SEC, "SEC Charges Two Investment Advisers with Making False and Misleading Statements About Their Use of Artificial Intelligence" (March 18, 2024).** Delphia (USA) Inc. and Global Predictions Inc.; $400,000 in combined penalties. Read the release.
5. **SEC Division of Investment Management, Staff Responses to Questions About the Custody Rule, Question II.6 (May 20, 2010).** Password access to client accounts. Staff guidance, not a rule. Read the FAQ.
6. **Investment Advisers Act Rule 204-2, books and records,** including paragraph (a)(7) on written communications. Read the rule.
7. **FINRA, 2026 Annual Regulatory Oversight Report, "GenAI: Continuing and Emerging Trends" (December 2025).** Applies to broker-dealers. Read the section.

Also in The RIA's Chartbook. No. 01, *Client Data and the Law*: what Reg S-P expects as AI enters the workflow. No. 02, *Every Vendor Is Part of Your Safeguards*: evaluating the technology that holds client information. No. 03, *Faster Check-ins, or Better Health?*: the harness behind proactive, AI-enabled advice. No. 06, *The Stack Tax*: what a firm really pays for its technology.

Educational information, not legal or compliance advice. Firms should consult their own counsel about their specific arrangements. The four levels, controls, and worksheet are editorial recommendations, not regulatory classifications or requirements. Helmsted capabilities are described as of September 2026; items described as rolling out, in development, planned, or on the roadmap are not yet generally available. The Morgans are fictional.

Helmsted

One secure, AI-native platform for the independent RIA. Learn more at helmsted.ai, or write to hello@helmsted.ai.