

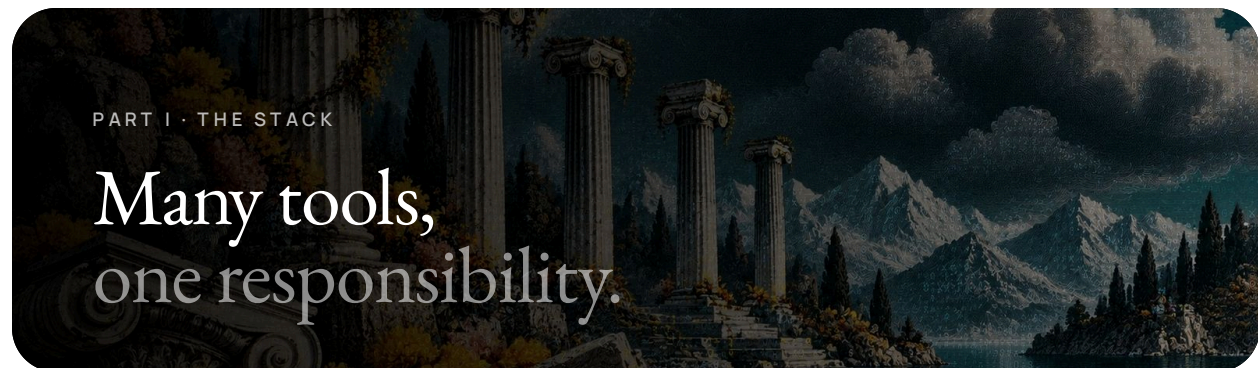
FOR INDEPENDENT RIAs · VENDOR OVERSIGHT

Every Vendor Is Part of Your Safeguards.

How independent RIAs can evaluate the technology that holds client information, from no-training promises to SOC 2 reports and the auditors who sign them.

INSIDE THIS GUIDE

- 01 The technology stack is part of the client file
- 02 A no-training promise answers one question
- 03 Evidence for a system that acts
- 04 What a SOC 2 report does and does not show
- 05 Start with your vendor inventory
- 06 Consolidation simplifies oversight and concentrates dependency



SECTION 01

The technology stack is part of the client file

Most independent RIAs did not choose their technology all at once. A CRM, a planning tool, a portal, an aggregator, a document system, a note-taker, an e-signature service, and now several AI tools each arrived to solve one problem. Many of them hold client information. Each is a vendor the firm is expected to oversee.

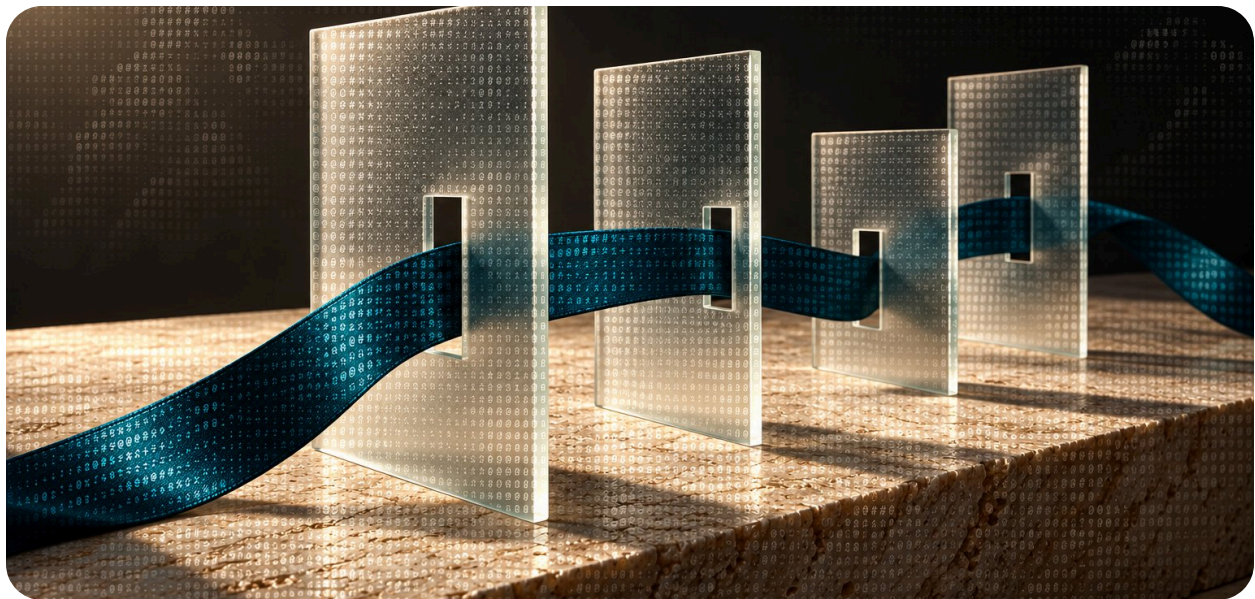
AI tends to add to that list quickly: one more point tool, one more data copy, one more contract, one more place an incident could begin.

Under the final amendments, service-provider oversight means due diligence and monitoring. The rule does not impose the proposed universal written-contract requirement. Contracts can support an oversight program; signing one does not finish the program. [1, section II.A.4] Examiners have said where they will look: the SEC Division of Examinations' fiscal 2026 priorities state that Reg S-P examinations "will focus on firms' policies and procedures, internal controls, oversight of third-party vendors, and governance practices." [2]

So the inventory matters. List every vendor that receives customer information, what it receives, why, and what evidence the firm holds about its safeguards. Then ask a strategic question alongside the compliance one: does each additional tool improve outcomes for clients enough to justify another place their information lives?

Every tool that holds client information is a vendor the firm is expected to oversee.

As AI moves from holding information to carrying out work, vendor diligence must examine both **access to data and authority to act**. That makes the central question of this installment: *what evidence earns a system permission to act?*



Useful execution depends on clear boundaries.

A no-training promise answers one question

Ask whether client information is used to train or improve models. Then continue the conversation.

A statement about training does not, by itself, tell the firm whether information is stored, how long it remains accessible, whether people can review it, or which other services receive it. Those are separate questions about the application and the arrangement being purchased.

Useful diligence connects a specific claim to supporting evidence:

QUESTION	EVIDENCE TO REQUEST OR INSPECT
What information enters each part of this workflow?	A data-flow description for the intended features and configuration.
What is used for training, evaluation, or product improvement?	Applicable terms, exceptions, and settings for each relevant service.
What remains after the task ends?	Retention and deletion details for files, outputs, indexes, logs, and backups.
Who else can receive or access the information?	Provider and subprocessor information, support-access practices, and integration permissions.
How is access separated between firms, households, and users?	An explanation of authorization controls and evidence appropriate to the intended use.
What happens if something goes wrong?	Incident contacts, reporting arrangements, and procedures for cooperation and evidence preservation.

These are suggested review questions. Their relevance and the evidence needed depend on the intended use; they are not a list of clauses that Reg S-P universally requires.

A vendor conversation becomes more useful when it starts with a real task. “We intend to analyze a household’s uploaded tax return and create internal follow-up tasks” is a clearer basis for review than “We want to use AI.” It gives both parties a concrete boundary to examine.

Evidence earns permission to act.

SECTION 03

Evidence for a system that acts

A system that only stores information is evaluated on what it keeps and who can see it. A system that acts, updating a record, sending a document request, or preparing a transfer for approval, also has to show what it is allowed to do, how it is stopped, and how the firm knows the work was finished. Consider a request to collect the Morgans' missing beneficiary forms:

EXECUTION EVIDENCE	WHAT TO ASK THE VENDOR	EXAMPLE: THE MORGANS
Permitted action	Which actions can the system take, and on which records?	Request forms from the Morgans only; no changes to accounts.
Authorization	Who granted that authority, when, and where is it recorded?	The lead adviser approved the task, logged with a date.
Boundary test	What happens when it is asked to exceed that authority?	A request to email another household is blocked and escalated.
Completion record	How is the result verified and recorded?	Forms received, matched to the file, and the task closed with evidence.
Revocation method	How is authority paused or withdrawn, and how fast?	One control pauses the workflow and revokes the connector.

Ask vendors to demonstrate, not describe: show an unauthorized action being blocked, and show a completed task with its verification record. A slide about controls is a claim; a live test is evidence.

What a SOC 2 report does and does not show

Continuous monitoring is the vendor watching itself. Compliance-automation platforms collect evidence from cloud accounts, code, identity systems, and devices, and flag controls that drift. It is a good sign of daily discipline, but it is still the vendor’s own view.

An independent examination is a licensed CPA firm checking. A SOC 2 report is an attestation, not a certification: an auditor’s opinion on the vendor’s controls against the AICPA’s trust services criteria. A Type 1 addresses design at a point in time; a Type 2 addresses operation over a period. Reports are restricted in use, which is why vendors share them under NDA. [3] A SOC 2 report speaks to security controls. It does not establish that an AI system’s outputs or actions are accurate; that evidence comes from the execution tests above.

WHAT TO CHECK	WHY IT MATTERS
Opinion, type, and period	A clean opinion is the baseline. Check that the period is recent and covers the service you use.
Scope	Which system and criteria are covered. A report on one product does not cover another.
Subservice organizations	Carved-out cloud and model providers need their own evidence.
Complementary user entity controls	Controls the firm must perform become its own responsibilities.
The auditor	A licensed CPA firm with peer review results and real SOC experience. [4]

Start with your vendor inventory

List every vendor that receives customer information. For each one, record what it receives, why, who approved it, and when it was last reviewed.

Collect the evidence: the data-flow description, the training and retention terms, the subprocessor list, and the most recent SOC 2 report. Read each report the way the table above suggests, and note the auditor, the period, and the complementary user entity controls the firm must perform itself.

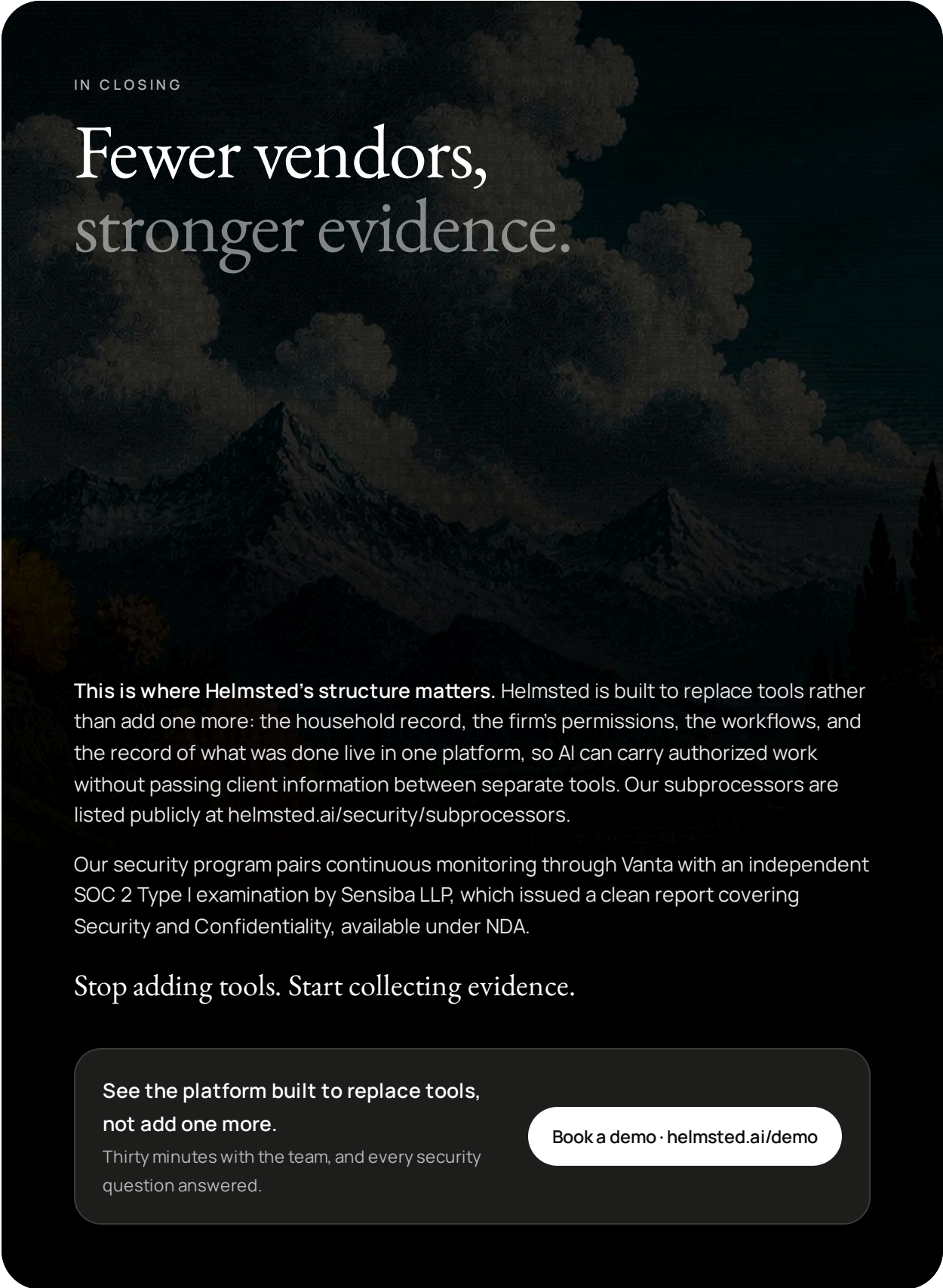
Mark the gaps plainly: reports that are out of date, carve-outs without their own evidence, and vendors that hold client information but no longer earn their place. Then decide what to renew, what to replace, and what to remove. NIST’s supply-chain risk guidance is a useful broader framework here: it treats technology suppliers as an ongoing risk to be managed across the relationship, not a set of reports to collect. [5] Repeat the review at least annually, and whenever a vendor adds a feature, a subprocessor, or a new use of client information.

KEEP IN EACH VENDOR’S FILE	WHY
What it receives, why, and who approved it	The basis for the use, and accountability for the decision.
Data flow, training, and retention terms	What happens to client information inside the service.
Subprocessor list	Who else receives the information.
Latest SOC 2 report, period, and auditor	Independent evidence, and how current it is.
Controls the firm must perform, and next review date	The firm’s side of the arrangement, kept current.

SECTION 06

Consolidation simplifies oversight and concentrates dependency

Fewer vendors can mean fewer data copies, fewer contracts, and a clearer record. It also means more depends on one provider, and one platform does not remove the provider chain beneath it: cloud hosting, model providers, and other subprocessors remain. Keep asking the same questions of a consolidated platform: Who are its subprocessors? What happens during an outage? Can the firm export its data in a usable form? What are the exit arrangements if the relationship ends?



IN CLOSING

Fewer vendors, stronger evidence.

This is where Helmsted's structure matters. Helmsted is built to replace tools rather than add one more: the household record, the firm's permissions, the workflows, and the record of what was done live in one platform, so AI can carry authorized work without passing client information between separate tools. Our subprocessors are listed publicly at helmsted.ai/security/subprocessors.

Our security program pairs continuous monitoring through Vanta with an independent SOC 2 Type I examination by Sensiba LLP, which issued a clean report covering Security and Confidentiality, available under NDA.

Stop adding tools. Start collecting evidence.

**See the platform built to replace tools,
not add one more.**

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

Book a demo · helmsted.ai/demo

Sources and further reading

Research checked September 24, 2026. Bracketed numbers in the text refer to the sources below.

1. **SEC, Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, Release Nos. 34-100155, IA-6604, IC-35193 (May 16, 2024), conformed to the Federal Register version.** Relevant sections: II.A.3, customer notices; II.A.4, provider oversight, reporting, and removal of the proposed written-contract requirement; II.B, scope; II.C, records; II.F, compliance period. Adopted rule text: 17 CFR 248.30 (a) (3) – (5). [Read the adopting release and rule.](#)
2. **SEC Division of Examinations, Fiscal Year 2026 Examination Priorities (November 17, 2025).** Sections on Regulation S-P and S-ID, cybersecurity, and emerging financial technology, including AI. Staff priorities, not rules. [Read the priorities.](#)
3. **AICPA, SOC 2 Logo for Use by Service Organizations: Terms, Conditions and Guidelines (April 2026).** Descriptions of SOC 2 Type 1 and Type 2 reports and their restricted use. [View on AICPA & CIMA.](#)
4. **AICPA, Questions and Answers About the AICPA Peer Review Program (February 2024).** Which firms enroll, review frequency, and ratings. Firms that authorize disclosure appear in the AICPA Peer Review Public File. [Read the Q&A.](#)
5. **NIST, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, SP 800-161 Rev. 1 (May 2022, updated November 1, 2024).** A framework for identifying, assessing, and responding to technology supply-chain risk across the life of a relationship. Voluntary guidance. [Read the publication.](#)

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.

Educational information, not legal advice. Applicability and incident decisions depend on the firm's circumstances and other relevant requirements. Workflow examples describe an operating vision, not a representation that all features are currently available in Helmsted. Images are AI-generated editorial illustrations; people and settings are fictional.

Helmsted

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