CircleSquare

WHITEPAPER

You have the AI policy. The question is whether you can produce the file underneath it.

For chief compliance officers at SEC-registered investment advisers

Signet, a division of Circle Square Consulting

August 2026

COVER LINE

This decides one thing: whether the firm builds its AI evidence file deliberately this year, or assembles it under a document request, a carrier questionnaire, or a diligence list.

Executive summary

Eighty-six percent of adviser firms have an AI acceptable use policy. Thirty-seven percent have an output testing policy, 30% a third-party AI policy, and 14% an incident response plan updated for AI disruption.[1] The policy layer of this industry is saturated. The evidence layer is empty.

That gap is not a drafting problem, which is why buying another policy does not close it. It is operations — running the inventory, keeping the register, capturing the incident record, running the test, configuring the retention, every month, in the Microsoft 365 tenant where it all lives.

The timing is not ours. Both Regulation S-P compliance dates have passed — December 3, 2025 at $1.5 billion or more in AUM, June 3, 2026 below it.[2] The FY2026 examination priorities say the staff will assess whether firms have implemented adequate policies to supervise their use of AI technologies.[3] Your cyber and E&O renewal asks for a version of the same list.[4] So does a buyer's diligence lead.[5]

The recommendation. Buy the three policies you do not have, not a fourth copy of the one you do. **AI Policies, $4,900 fixed** — third-party and vendor AI mapped to the Reg S-P service provider obligation; incident response that contemplates an AI failure; output testing that produces a record. Keep it current on the **GRC Platform, $495 a month, no term**. **Claude Setup — Connect, $3,900 fixed**, is the tenant work, priced separately so you can decline it.

What we refuse, before anything else. We build nothing that produces an investment recommendation, a suitability determination, a portfolio decision or a security selection. We write no marketing copy. We give no regulatory advice — we are not your compliance consultant, and when a question belongs to one we say so on the call, not after the invoice.

The situation

The 2026 Investment Management Compliance Testing Survey — the IAA with ACA Group and Yuter Compliance Consulting, 411 adviser firms — found 85% naming AI their number one compliance topic for the year, up 28 points and the most dominant single response in the survey's twenty-one-year history. Eighty percent have adopted AI tools; 86% have an acceptable use policy; 86% keep a tool inventory; 59% have a governance committee. Then: 48% human-in-the-loop, 37% output testing, 30% third-party AI, 14% incident response.[1] One caveat belongs on the page rather than in a footnote — those respondents skew larger and more institutional than a $250 million to $5 billion firm. Read them as an upper bound, not a median.

The regulatory calendar is behind us, not ahead. The SEC adopted the Reg S-P amendments on May 16, 2024. An adviser must now have a written incident response program; notification no later than 30 days after becoming aware of a breach of sensitive customer information, subject to a rebuttable determination that no substantial harm is reasonably likely; written policies establishing service provider oversight, including that a provider notify the adviser within 72 hours of unauthorized access; and five years of records covering all of it.[2] Ten trade associations asked for a six-month extension on November 19, 2025. It was not granted.

One point of precision, because it separates people who read the rule from people who read a summary: **the SEC declined to adopt the written-contract requirement it proposed.** The final rule requires written policies reasonably designed to establish oversight.[6] Most firms implement the 72-hour arrangement contractually anyway — but the obligation is the policy and the oversight, not a clause.

And it is worth knowing what did *not* happen. On June 12, 2025 the Commission withdrew fourteen proposed rules, including the 2022 adviser cybersecurity rule.[7] The obligation relocated into Reg S-P as amended, Reg S-ID and Rule 206(4)-7, enforced through examinations. That is harder to prepare for, not easier: a named rule tells you what the artifact should look like; an exam asks you to produce whatever you said you would.

What most firms miss

Here is the position, and a reasonable person could argue with it: **for a firm that already has an acceptable use policy, buying another policy is worse than doing nothing.**

The reason is Rule 206(4)-7. It requires an adviser to adopt **and implement** written policies, and to review annually both their adequacy and **the effectiveness of their implementation**.[8] Adequacy is a drafting question and the market has answered it — that is what 86% means. Effectiveness of implementation is a question about what actually happened inside your firm over twelve months, answered only with artifacts: a dated inventory, a completed test, an incident record, a determination, a review that left a trace.

Add a policy with no artifacts behind it and you have widened the distance between what the file says and what the firm does. A generic policy describing a firm that is not yours is worse than none: the moment anyone compares the policy to the practice, the comparison is the finding.

Two more places the instinct runs backwards.

Retaining everything is not the conservative choice. The retention decision for AI transcripts should be made in advance, at the category level; keeping everything gives examiners more material with no compliance benefit to you.[9] If a transcript is a required record, keep it and manage it. If not, keeping it buys nothing and costs surface area.

One artifact cannot be produced retroactively. Everything else here can be assembled by a competent person working hard for a fortnight. The risk assessment dated *before* the tool went live cannot — and it is the item carriers ask for by name.[4] The cost of waiting is not spread evenly. It lands entirely on the tools you deploy between now and the day you start.

One correction runs the other way, because credibility runs both directions: **Rule 206(4)-7 does not require a written report of the annual review.** That is industry practice driven by examination expectations and Rule 204-2, not rule text. In practice the staff treat an undocumented review as no review — a statement about evidence, not about the rule, and the same point.

What good looks like

Six artifacts. A standard, not a pitch — a firm that never hires anyone can build it.

1. The AI tool inventory. One row per tool: vendor, the underlying model where disclosed, what firm and client data it can reach, whether inputs train the model, where data is processed, retention, who approved it, the date of the risk assessment — which must precede go-live — and the date of last review. Save the vendor's terms as a dated PDF, because vendors change terms and "we checked once" is not a record. Keep a separate *discovered* list of what individuals bought on a card: adviser notetakers run $60 to $80 per adviser per month and up,[10] under every approval threshold you have.

2. The service provider register. Not the vendors finance pays — the vendors with access to customer information. That list is longer than people expect: an AI notetaker in a client meeting is a service provider with access to customer information, and so, frequently, is the model layer underneath it, a different company with different terms. Per provider: what data it touches, what you reviewed, when, what you kept, the monitoring cadence, and the 72-hour arrangement.

3. The incident and determination record. Every unauthorized-access incident in five years, and the determination of whether notification was required — **including the ones where you concluded it was not**. A determination is a decision. Made in a hallway and never written down, eighteen months later it is indistinguishable from a decision nobody made. Two paragraphs is enough: when you became aware, what you knew, how you established scope, who decided, on what basis.

4. One completed output test. Not a procedure describing a test — a test. It names the population, the sample, the standard compared against, what was found, what was done about exceptions, and when it gets re-run. A control with no test history is an assertion.

5. The written human review point. Where a person reviews before anything reaches a client, naming the person and the standard. "Outputs are reviewed" is not this. "The client service manager checks each meeting summary against the recording before filing, against the four-point checklist" is.

6. The retention decision. Category level, dated, made before the transcripts it governs. Meeting summaries supporting advice given; raw audio and verbatim transcripts; internal strategy discussions; prospect meetings that did not convert — plausibly different treatments. The configuration then has to match the decision in two places: your tenant, and the vendor's own retention setting, defaulted for the vendor's convenience. A policy saying ninety days against a vendor quietly holding four years is worse than no decision, because now your file contradicts you.

Rule 204-2 defines a record to include "transcribed information of any type, whether expressed in ordinary or machine language," and requires retention not less than five years from the end of the fiscal year of the last entry.[11] There is no SEC guidance expressly addressing AI-drafted communications under 204-2. We state the rule and stop there.

How we do it

ENGAGEMENT	DETAILS
AI Policies — $4,900 fixed.	Three policies scoped to the gaps rather than to the acceptable use layer you own: third-party and vendor AI, mapped to the Reg S-P service provider obligation; incident response that contemplates an AI failure; output testing that produces a record. Written against your actual environment, read line by line by our vCISO, who signs an attestation. Mapped to NIST CSF 2.0 and CIS Controls v8.1. A few weeks, and about two hours of your COO's time.
GRC Platform — $495 a month, no term.	Where the policies live and stay current: portal, annual review, regulatory monitoring, questionnaire support, with the review scheduled against your cyber and E&O renewal rather than a random anniversary. Month to month — if we are only keeping you through a contract term we have already lost.
Claude Setup — Connect — $3,900 fixed, optional.	The tenant work: what is connected to what, what data an agent may reach, retention and archiving configuration, access controls, and the logging that turns activity into a record. Priced separately so you can see it as its own line and decline it.

WHAT THIS DOES NOT INCLUDE.

Regulatory advice. An opinion on whether your compliance program is adequate. An assessment of your existing policies. Client-facing marketing copy. Any system producing a recommendation, a suitability determination, a portfolio decision or a security selection. A fixed fee against a custodian integration we have not tested — custodian touchpoints are assumed file-based or human-in-the-loop until proven otherwise. And we do not deploy into a tenant we cannot administer or see.

Engagement floor $4,900. Pass-throughs — platform, model, OCR — bill at cost. We do not mark up tokens. Month 1 is a kill switch; scope freezes after month 2.

Proof

What we can say, and the limits of it.

We are an MSP in Radnor, Pennsylvania. We deliver attested security policy programs to a law firm client, mapped to NIST CSF 2.0 and CIS Controls v8.1, in roughly 17.5 vCISO hours against about 30 for a traditional engagement. We run AI ticket triage on our own production queue, and an automated daily operating brief, end-of-day carry-over and weekly retrospective internally — we run the method on ourselves before selling it. We design, build and operate a commercial software product of our own. And we manage the environments of the clients we automate, which is the structural point: the inventory, the retention configuration, the access controls and the incident records are produced by whoever holds the credentials.

What we will not put on this page. No percentage time saving, no ROI multiple, no payback period, no client name. We have not measured them, and this is the audience for whom an unsourced number is disqualifying. The SEC charged two advisers in March 2024 for describing AI capabilities they did not have.[1][2] Overclaiming is the thing we sell against. If we did it here you would be right to stop reading.

Objections, answered before they are asked

OBJECTION	ANSWER
"Our compliance consultant handles this."	Keep them. We give no regulatory advice, and if we start you should fire us for it. They tell you what the rule requires of your firm. We produce and operate the artifacts the answer depends on. Ask them one question — once the framework is written, who here produces the inventory month to month and records that a test happened? At most firms the framework exists and the production does not. That is not a consulting failure. It is an operations vacancy.
"Why not our existing IT provider?"	Often the right answer, if they will do it. Ask them for three things: the register, a completed output test, and the retention configuration reconciled against the vendor's own setting. This work is unusual for an MSP not because it is hard but because it is a recurring documentary obligation rather than a ticket. Most have no process that produces a dated artifact every month. If yours does, use them.
"We just had a clean exam."	Then this is cheaper rather than unnecessary. The FY2026 priorities naming AI supervision were announced November 17, 2025; the Reg S-P dates were December 3, 2025 and June 3, 2026. If the exam predates those, the questions you passed are not the questions in front of you.
"$4,900 for policies we mostly have."	If it were a document, $4,900 would be too much. What it buys is three policies you do not have and a named vCISO who reads every line against your environment and signs. If you have all three and they are current, you do not need us, and we will say so in writing.

Footnotes

1 2026 Investment Management Compliance Testing Survey — Investment Adviser Association, ACA Group and Yuter Compliance Consulting. 411 adviser firms, fielded late April–May 2026, published July 29, 2026.

2 SEC Press Release 2024-58, May 16, 2024; FINRA compliance date reminder, November 14, 2025. The $1.5 billion smaller-entity threshold rests on law firm commentary — Holland & Knight, May 7, 2026, and Carlton Fields, 2026 — not the rule text. If your AUM is near the line, confirm against Table 3 of the adopting release.

3 SEC Division of Examinations FY2026 examination priorities, announced November 17, 2025 (Press Release 2025-132).

4 ACA Group, "How AI is changing the rules of cyber insurance," July 23, 2026. ACA sells AI governance services; this is directional evidence, not a carrier or broker survey. Check with your own broker.

5 DeVoe & Company RIA Deal Book, Q2 2026, reported July 27, 2026: 167 RIA transactions in H1 2026, up 13%; 46% of consolidators name $1B–$5B AUM firms as preferred targets; 82% expect valuations flat over six months, 18% expect declines, none expect increases.

6 Davis Polk client update on the Reg S-P adopting release.

7 SEC withdrawal of fourteen proposed rules, June 12, 2025, including S7-04-22 and S7-12-23. If the Commission pursues these areas again it has said it will issue a new proposed rule.

8 Rule 206(4)-7, 17 CFR 275.206(4)-7.

9 Cooley, TheFundLawyer, "AI notetakers and the books and records rule," April 24, 2026.

10 Kitces Research, Advisor Productivity study.

11 Rule 204-2(a)(7) and 204-2(e)(1), 17 CFR 275.204-2 — records kept the first two years in an appropriate office of the adviser. The SEC's July 7, 2026 rulemaking agenda lists amendments to the adviser recordkeeping rule at proposed-rule stage, targeting October 2026.

12 SEC Press Release 2024-36, March 18, 2024 — Delphia (USA) Inc., $225,000, and Global Predictions Inc., $175,000; both censured, both settled without admitting or denying. No verified SEC AI-washing action against a registered adviser after that date; the credible claim is examination risk, not enforcement.