ACTIONABLE AI

presents

Vendor AI & Data Governance

Audit Playbook

for Small Law Firms

No theory. No hype. Just the file a firm needs when someone asks, "What did you do before giving this vendor access to client data?"

actionableai.net · Prepared by Greg Yates - Updated September 28, 2026

Important Notice

This playbook is educational and informational. It is not legal advice, ethics counsel, or a substitute for consultation with The Florida Bar or qualified counsel on any specific matter or on your firm's own professional-responsibility obligations.

Nothing here creates an attorney-client relationship. Actionable AI is a consulting firm, not a law firm.

Vendor contracts, AI terms, privacy policies, and data-handling practices change constantly. Every standard, deadline, and reference cited in this playbook is current as of the September 2026 edition date and must be independently verified before you rely on it. A vendor's terms from last year may not be their terms today.

All sample policies, disclosures, questionnaires, decision memos, and prompts are starting points. Have a Florida-licensed attorney review them before adoption or use. Adapt every template to your firm's jurisdiction, clients, vendor contracts, and applicable privacy and security obligations.

Vendors are named in these pages because small firms already own or evaluate them, not as endorsements. Actionable AI takes no fees from any vendor and recommends no product.

A note on numbers. Every figure here falls into one of three buckets, and you can tell which from the sentence around it. Statutory amounts, deadlines, and case outcomes carry their own citation and can be checked at the source. Third-party statistics name the body that produced them. Anything else is an Actionable AI working assumption, offered to be stress-tested against your firm's own rates, volumes, and matter values rather than repeated as fact.

Contents

Important Notice 1

The Problem With Generic Vendor Governance Advice 6

- What This Playbook Does Differently 6
- The Actionable AI Philosophy 6

Why Vendor Governance Is Different for Law Firms 8

- The Confidentiality Obligation Is Not Optional 8
- AI Is Already in Tools You Have Been Using for Years 8
- A Security Breach Is Not Just a Business Problem 9
- Small Firms Have None of the Enterprise Leverage 9
- The Website Is Not Proof 9

The Florida Ethics Reality 11

- The Rules That Matter Most 11
- Other Rules That Touch This Work 13
- The Courts Are Writing Their Own Rules: Right Now 13

The Emerging Issue Most Small Firms Are Missing: Shadow AI 15

- The Scale of the Problem 15
- Why This Creates a Governance Problem Right Now 15
- What the Audit Finds 16

Ethics Risks and Governance Framework 17

- High-Risk Failure Modes 17
- Data Classification Framework 18
- Vendor Minimum Standards 19
- Approval Levels 19
- Practical Vendor Rules for Law Firm Staff 20

The Audit Process: Stage by Stage 21

- Stage 1: Build the Vendor Inventory 21
- Stage 2: Classify Vendors by Risk Tier 22
- Stage 3: Identify AI Features 23
- Stage 4: Assign Risk Tiers and Define Minimum Standards 23
- Stage 5: Build the Evidence File 23
- Stage 6: Send the Vendor Request Email and Questionnaire 24

Stage 7: Review the Responses....25
Stage 8: Send Follow-Up Questions....25
Stage 9: Approve, Limit, or Reject Each Vendor....25
Stage 10: Configure Settings and Document Them....27
Stage 11: Train Staff....27
Stage 12: Set the Re-Review Schedule....28
Prompts Library....29
Appendix A: Sample AI Governance Policy....37
Purpose....37
General Principles....37
Definitions....37
Permitted Uses....37
Prohibited Uses....38
Confidentiality and Data Handling....38
Court and Tribunal Filings....38
Incident Response....38
Acknowledgment....39
Appendix B: Client AI Disclosure Statement....40
Implementation Notes....40
Appendix C: Vendor AI, Data Retention, Confidentiality, and Security Questionnaire....41
Section A: Vendor Identity....41
Section B: Data Handled....41
Section C: AI Use....42
Section D: Confidentiality....43
Section E: Data Retention and Deletion....43
Section F: Security Controls....44
Section G: Subprocessors and Third Parties....45
Section H: Legal Process and Government Requests....45
Section I: Contract and Policy Changes....46
Section J: Vendor Certification....46
Appendix D: Copy-Ready Vendor Emails and Decision Memo Template....47
Initial Vendor Request Email....47

Follow-Up Email for Incomplete or Vague Responses....47
Decision Memo Template....48
Appendix E: 90-Day Vendor Governance Rollout Plan....50
Week 1: Build the Inventory and Triage....50
Week 2: Send Vendor Requests....50
Week 3: Review Responses....50
Week 4: Decide, Configure, and Train....50
Weeks 5–8: Expand to Remaining Tier 3 and Tier 4 Vendors....50
Weeks 9–13: Close the Remaining Decisions....51
Ongoing: Sustain the Program....51
About Actionable AI....52
What We Do....52
Who This Playbook Is For....52
Sources and Ethics Anchors....53

The Problem With Generic Vendor Governance Advice

Here is what the AI influencers will not tell you: the vendor checklist circulating on LinkedIn was written for nobody. The same template gets handed to a dental practice, a software startup, and a plaintiff's family law firm. It does not know the difference, because it was never built for law.

It does not know that your obligation to protect client data is not a preference or a best practice. It is a mandatory professional duty under Rule 4-1.6 of the Florida Rules of Professional Conduct. It does not know that when Microsoft, Google, Zoom, or Clio add AI features to their platforms, those features may already be processing your clients' privileged documents, matter notes, and billing records without a single notice beyond a paragraph buried in an updated terms-of-service email you did not open. It does not know that "we take security seriously" is not a contractual obligation and will not protect you if a client's confidential records end up in a training dataset.

Generic advice produces generic results. In a law firm, generic results mean a confidentiality breach involving a client's most sensitive documents, a disciplinary complaint to The Florida Bar, a malpractice exposure that no vendor will share, and a client who trusted you with information they shared with no one else. The cost of wrong is not a failed vendor audit. It is a Bar grievance and a career that ends because a sales rep said "our platform is secure" and you believed it.

What This Playbook Does Differently

This playbook was built for the small Florida firm that needs a defensible vendor-governance record, solos and firms with fewer than 25 lawyers handling any practice area. AI is now embedded in almost every tool a small law firm uses. This playbook gives you the process, the questionnaire, the decision framework, and the documentation templates to govern it.

It answers three questions that matter:

1. What are the real ethics and governance risks of using AI-enabled vendors, and how do you build a documented record that protects you?
2. Which vendors deserve the deepest scrutiny, and what specifically do you need from them in writing?
3. How do you implement a vendor governance program that actually runs in a firm where the managing partner is also the trial lawyer?

No enterprise consulting overhead. No 90-page risk program that sits in a drawer. Just the specific, Florida-grounded process a small firm can run, document, and defend.

The Actionable AI Philosophy

Tools serve lawyers. Not the other way around.

The small firm that survives AI adoption is not the one that installed the most software. It is the one that asked the right questions first, got the answers in writing, and made a documented decision. Vendor governance is not about being anti-AI. It is about knowing exactly what your vendors are doing with the most sensitive professional information in your community, and being able to prove you asked.

THE ACTIONABLE AI TEST

Before any vendor touches client data, answer four questions:

1. Does the vendor have a contractual confidentiality obligation, not just a public privacy policy?
2. Is client or firm data used to train AI models, and can you opt out in writing?
3. Can you verify what the vendor retains, and can you require deletion on demand?
4. Would you be comfortable explaining this vendor relationship to The Florida Bar?

If you cannot answer all four confidently, the vendor review is not complete.

Why Vendor Governance Is Different for Law Firms

Enterprise companies run vendor-risk programs because it is good business and, in some industries, a regulatory requirement. Law firms run vendor-governance programs because their professional obligations under the Florida Rules of Professional Conduct make systematic vendor review the most defensible way to demonstrate compliance, and because the stakes of a breach are not just financial. They are professional.

The Confidentiality Obligation Is Not Optional

Rule 4-1.6 of the Florida Rules of Professional Conduct requires a lawyer to make reasonable efforts to prevent the unauthorized disclosure of client information. The rule was written before cloud software existed. It applies anyway. When you hand a vendor access to your email, your document management system, your practice management platform, or your transcription tool, you are extending your confidentiality obligation through them. The vendor's terms-of-service page does not satisfy that obligation. A signed contractual commitment to protect confidential information does.

Rule 4-5.3 adds the supervision layer. When you use a vendor as a nonlawyer assistant, and AI-enabled vendors increasingly function exactly that way, you must make reasonable efforts to ensure the vendor's conduct is compatible with your professional obligations. That requires knowing what they do with your data, who can access it, and what happens when something goes wrong.

> **KEY FINDING**
>
> Florida Bar Ethics Opinion 24-1 (January 19, 2024) told Florida lawyers they must evaluate an AI tool's confidentiality terms before running client information through it. ABA Formal Opinion 512 (July 29, 2024) reached the same conclusion nationally six months later under Model Rule 1.6. The duty applies every time a lawyer's use of a vendor implicates client information, not just with dedicated AI tools. What a lawyer must address in each such relationship: confidentiality, competence, supervision, accuracy, and billing.

AI Is Already in Tools You Have Been Using for Years

This is the point most vendor-governance conversations miss. When firms hear "AI vendor governance," they think of ChatGPT and Claude. The actual exposure is broader. AI is now embedded in the ordinary business and legal tools small firms have relied on for years:

— Microsoft 365 / Copilot: AI drafting, summarization, and meeting notes, processing email, documents, and Teams calls

— Google Workspace / Gemini: AI generation and search across Gmail, Drive, and Docs

— Clio / Clio Duo: AI-powered document drafting, case summaries, and client communication

— Zoom AI Companion: Meeting summaries and transcription processing call content

— Adobe Acrobat AI Assistant: Document summarization and Q&A across uploaded PDFs

— QuickBooks: AI-powered insights processing financial and billing data

— Legal research platforms (Westlaw, Lexis, vLex, CoCounsel): AI summarization and drafting features embedded in research tools

— Intake and CRM tools: AI classification, chatbots, and lead scoring

— Transcription and answering services: AI processing of client call recordings

Each of these vendors has its own AI data-handling policy. Each has its own terms for whether your inputs are used for model training. Each has its own retention schedule for prompts, outputs, and interaction logs. And most of them updated those terms in the last 12 months without sending you a plain-English summary of what changed.

> **IMPORTANT**
>
> You do not have to add a new AI tool to have a vendor AI governance problem. You already have one. The audit this playbook describes is the process for finding out exactly where you stand.

A Security Breach Is Not Just a Business Problem

For most businesses, a data breach is an operational and financial event. For a law firm, it is also a potential ethics violation. If client confidential information is exposed because a vendor did not have adequate security controls, and you did not do the due diligence to discover that before handing them access, the question is whether you made the "reasonable efforts" Rule 4-1.6 requires.

The answer to that question is your audit file. Not your memory of a sales call. Not the vendor's website. The written questionnaire, the written responses, the decision memo, and the documentation that you reviewed, decided, and set a re-review date. That file is what reasonable efforts looks like in 2026.

Small Firms Have None of the Enterprise Leverage

When a 500-lawyer firm tells Microsoft or Clio to negotiate their data terms, someone takes the call. When a three-lawyer firm asks the same question, the answer is usually "our standard terms govern." That reality shapes what vendor governance looks like for small firms. You cannot always get a fully negotiated enterprise agreement. What you can do is know exactly what the standard terms say, document that you reviewed them, configure every available setting in your favor, and limit the data categories that touch the highest-risk vendors.

The goal of this playbook is not perfection. It is a defensible, documented record showing that the firm asked the right questions, reviewed the answers, made a considered decision, and scheduled follow-up review. That is the difference between a firm that can defend itself and a firm that relied on vibes.

The Website Is Not Proof

Every vendor in this space has a trust page, a security whitepaper, and a "we take your privacy seriously" header. None of it, standing alone, is a contract. A trust page or public privacy policy is not a binding contractual commitment unless it is expressly incorporated into the governing agreement. None of it satisfies your professional obligations under Rule 4-1.6 or Rule 4-5.3.

What counts is the signed contract, the data processing addendum, and the written questionnaire responses from someone with authority, not a sales representative guessing from a script. The audit process in this playbook is designed to get you to those written commitments, in a file that can be opened and reviewed when it matters.

NOTE

The operating standard: Ask in writing. Get written answers. Save the documents. Make a written decision. Set limits. Review again.

That is the difference between ‘we were careful’ and ‘we were vibes-based.’

The Florida Ethics Reality

Florida's core ethics duties predate generative AI, cloud software, and every vendor data-handling policy in existence. They apply anyway, and since October 28, 2024 they say so out loud: the Florida Supreme Court amended the Comments to Rules 4-1.1, 4-1.6, 4-5.1, and 4-5.3 to address generative artificial intelligence by name. In re Amendments to Rules Regulating The Florida Bar – Chapter 4, 393 So. 3d 137 (Fla. 2024). The Florida Rules of Professional Conduct do not distinguish between old-technology confidentiality breaches and new-technology ones. They require reasonable efforts. Whether those efforts were reasonable is determined after the fact, in light of the risks a competent lawyer should have known to manage.

Florida Bar Ethics Opinion 24-1 (issued January 19, 2024) addressed the use of generative AI tools by Florida lawyers directly. While it does not prohibit AI use, it makes clear that lawyers must evaluate AI tools for confidentiality compliance before use, supervise AI-generated work product, and exercise independent professional judgment on AI outputs. The opinion is available at floridabar.org/etopinions/opinion-24-1/.

ABA Formal Opinion 512 (issued July 29, 2024) adds national ethics guidance under the ABA Model Rules that Florida practitioners should read alongside Op 24-1. It addresses the use of generative AI under the Model Rules, with direct application to confidentiality, supervision, fees, and candor obligations. Both opinions apply to vendor governance, not just the dedicated AI tools a lawyer chooses. They apply to every vendor that processes client information using AI.

The Rules That Matter Most

RULE 4-1.1: COMPETENCE AND TECHNOLOGICAL COMPETENCE

Rule 4-1.1 requires competent representation, including the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation. The comment to Rule 4-1.1, under the heading Maintaining competence, extends this to technological competence: a lawyer should keep abreast of changes in the law and its practice and engage in continuing study, "including an understanding of the benefits and risks associated with the use of technology, including generative artificial intelligence."

In the context of vendor governance, competence means understanding what the tools you use actually do with client data, not just whether they perform the task you bought them for. A managing partner who installs Microsoft Copilot, enables it across the firm, and never reviews the AI data-handling terms is not exercising the technological competence Rule 4-1.1 requires. The audit process is how a competent lawyer discharges that obligation.

> **KEY FINDING**
>
> Technological competence does not require technical expertise. It requires a reasonable understanding of the technology's benefits and risks. Asking a vendor the right questions in writing, and reviewing the answers, is what reasonable technological competence looks like for small firm AI governance.

RULE 4-1.6: CONFIDENTIALITY

Rule 4-1.6 prohibits revealing information relating to representation without client consent. It also requires reasonable efforts to prevent unauthorized access to or disclosure of client information. The rule covers all

information relating to representation, not just the documents in a matter file. Email, billing records, calendar entries, meeting notes, and intake data are all covered.

The vendor governance implication: when a vendor processes any of this information, the firm's confidentiality obligation travels with it. The vendor's own terms govern what they do with that information. If those terms permit the vendor to use client inputs for AI model training, aggregate client data for analytics, or allow vendor employees to review firm data for support purposes without restriction, the firm's confidentiality obligation is at risk. The audit process is how you find out what the terms actually say, before you sign, not after.

> **IMPORTANT**
>
> One confidentiality risk is a vendor using client inputs to improve a shared AI model. Even when the inputs remain in the vendor's environment, their use for training matters. Read the AI training and data-retention terms for every vendor that processes client data (Florida Bar Ethics Op. 24-1, pp. 2–4).

RULE 4-5.3: SUPERVISION OF NONLAWYER ASSISTANCE

Rule 4-5.3 requires that a lawyer with supervisory authority over nonlawyer assistance make reasonable efforts to ensure that the conduct is compatible with the lawyer's professional obligations. The rule is not limited to employees. Its comment carries a section headed Nonlawyers Outside the Firm, and since October 28, 2024 that section lists "using generative artificial intelligence" and "using an Internet-based service to store client information" among the examples. A vendor holding your client files is the case the comment describes.

For vendor governance, Rule 4-5.3 means that when a vendor's AI processes client information, drafting documents, summarizing calls, classifying data, generating responses, the lawyer is responsible for the output. The vendor is not. You cannot outsource ethics compliance to a vendor terms-of-service page. You must configure the tool within your professional obligations, train the people using it, and review outputs before they reach a client or a court.

RULE 4-3.3: CANDOR TOWARD THE TRIBUNAL

Rule 4-3.3 prohibits making false statements of fact or law to a tribunal and requires disclosure of directly adverse controlling authority. In the context of vendor governance, candor applies when AI-generated work product is used in court filings. If a vendor's AI tool produces a citation, a case summary, or a legal argument that is inaccurate, and a lawyer files it without independent verification, Rule 4-3.3 is implicated.

The vendor does not carry this risk. The lawyer does. The audit process includes configuring vendor AI tools so that outputs are clearly labeled as AI-generated drafts requiring attorney review, and training staff that no AI output goes into a filing without independent verification.

RULE 4-1.5: FEES

Rule 4-1.5 requires that fees be reasonable. For law firms using AI to improve efficiency, this has practical billing implications. When AI reduces a task that once took four hours to forty minutes, billing the original four-hour rate for AI-assisted work raises a reasonableness question. The answer is not to avoid AI. It is to document how AI is used and adjust billing practices accordingly.

For vendor governance specifically, fee implications arise in the cost of the audit itself. The time spent reviewing vendor contracts, completing questionnaires, and building the evidence file is a legitimate administrative investment in the firm's governance. Some of that time is billable to matters if the review is matter-specific. The rest is firm overhead, the cost of running a professional practice in 2026.

RULE 4-5.1: RESPONSIBILITIES OF PARTNERS, MANAGERS, AND SUPERVISORY LAWYERS

Rule 4-5.1 requires a lawyer with managerial authority in a firm to make reasonable efforts to establish internal policies and procedures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct. Since October 28, 2024, the comment states that such policies include those designed to "consider safeguards for the firm's use of technologies such as generative artificial intelligence."

Rule 4-5.1 calls for reasonable firm measures, including consideration of safeguards for generative AI. It does not prescribe a separate written vendor policy for every firm. This playbook recommends one, with a vendor decision record, so the firm can apply its standards consistently and show what it did. Lawyers with managerial authority own those reasonable efforts (Rule 4-5.1 cmt.; SC2024-0032, PDF p. 11).

Other Rules That Touch This Work

— **Rule 4-1.4, Communication:** If a client specifically asks whether AI tools are used in their matter, Rule 4-1.4 requires a truthful response. Firms should decide proactively what they will disclose and build that language into engagement letters rather than improvising when clients ask.

— **Rule 4-1.18, Prospective Clients:** Information shared during intake, even before representation begins, is protected. AI-enabled intake tools that process prospective-client information are subject to the same vendor governance standards as tools used in active matters.

— **Rule 4-6.1, Pro Bono:** Firms using AI efficiency gains to reduce costs and expand access to justice are applying Rule 4-6.1's aspirational standard in the most direct way possible. Vendor governance is not a barrier to that goal. It is what makes the efficiency sustainable.

The Courts Are Writing Their Own Rules: Right Now

Florida state courts and federal courts in Florida have been addressing AI disclosure in filings through administrative orders and standing orders that change frequently. Before any filing, verify the current requirement for your specific court and judge.

FLORIDA STATE COURTS: NEW STATEWIDE RULE

Florida Supreme Court Opinion SC2026-0673 (May 28, 2026, effective June 15, 2026) amended Rule of General Practice and Judicial Administration 2.515(d)(2). The signing attorney must represent that cited authorities 'exist and are accurately cited.'

Scope: Florida state courts only. This rule does NOT govern federal courts, including federal bankruptcy courts or any of Florida's three federal district courts: the Northern District of Florida, the Middle District of Florida, or the Southern District of Florida.

Authorized sanctions: reprimand, contempt, stricken document, dismissal, costs, fees, or other sanctions.

Practical implication: every AI-generated citation must be independently verified before any state court filing. The amendment took effect on schedule, but the Court accepted comments through

August 11, 2026, so confirm the current text of the rule before relying on this summary.

BEFORE EVERY FILING: CHECKLIST

1. For AI citation certification in Florida state courts, comply with Rule 2.515(d)(2) under SC2026-0673. Under AOSC26-12, Florida state courts may not impose the covered circuit-level AI disclosure or certification requirements through local orders, policies, or judicial practices. Check circuit administrative orders for other local requirements (AOSC26-12, pp. 2–3).

2. Check the standing order for your assigned judge in the Northern, Middle, or Southern District of Florida for federal matters.

3. Independently verify every AI-generated case citation against Westlaw, Lexis, or the court's own docket.

4. On filing, the signer represents under Rule 2.515(d)(2)(D) that the legal authorities identified exist and are accurately cited. Separately verify the propositions and holdings before relying on them. Voluntary disclosure of AI use remains an option and is generally safer than non-disclosure where AI involvement was significant. (SC2026-0673, appendix, PDF p. 5)

The Emerging Issue Most Small Firms Are Missing: Shadow AI

Most small law firm vendor governance conversations focus on the tools a firm deliberately chose: the AI legal research platform they subscribed to, the document drafting tool they piloted. That is the visible surface. The deeper problem is the tools they did not choose, the AI features that arrived inside software the firm was already using, on a product update the firm did not review.

Call it shadow AI: the AI already running inside your firm's existing vendor stack, often enabled by default, often processing client data, and almost never reviewed as an AI adoption decision.

The Scale of the Problem

The 2025 and 2026 platform updates from the major vendors were not minor feature additions. They were AI integrations that fundamentally changed what these platforms do with the data stored on them:

— Microsoft 365 Copilot and Copilot Chat (eligible commercial customers; availability depends on license tier and configuration, rollout 2024–2025): Integrated across Word, Outlook, Teams, SharePoint, and OneDrive. Verify tenant settings, user licensing, and data-retention configuration before use with client data.

— Google Workspace Gemini (available across many Workspace Business and Enterprise editions; feature availability, admin controls, and data-use terms vary by plan): Integrated across Gmail, Drive, Docs, Meet. Verify your firm's specific plan and admin settings before use with client data.

— Clio Manage AI, formerly Clio Duo (released October 2024, renamed since): AI features embedded in Clio, a widely used law practice management platform. Document drafting, matter summaries, and client communication features process matter data. Clio completed its announced $1 billion acquisition of vLex in November 2025, so a firm running Clio for practice management and vLex for research now has one corporate parent, not two independent vendors.

— Zoom AI Companion (available with eligible paid Zoom accounts; availability and default settings depend on account, admin, and feature configuration): Meeting summaries, transcription, and chat AI process call content, including client intake calls, deposition prep sessions, and settlement discussions.

— Adobe Acrobat AI Assistant (included in select plans, 2024): Summarization and Q&A features process uploaded PDFs, including pleadings, contracts, and client records.

— QuickBooks AI features (2024–2025): Automated categorization and financial insights process billing and trust account data.

Each of these updates landed in the form of a product release or a terms-of-service update. Most small firms did not treat them as AI adoption decisions. They were already paying for the platform. They kept paying. The AI came along.

Why This Creates a Governance Problem Right Now

The governance problem is specific. These features may be:

— **Enabled by default:** meaning the firm is using AI without having reviewed whether it meets the firm's confidentiality standards.

— **Processing client data:** meaning confidential matter information, client communications, and privileged documents may be processed by AI features. Note: data processing (generating a summary

or output) is not the same as data training (using inputs to improve a model). Verify both separately for each vendor.

— **Subject to training opt-outs the firm never exercised:** meaning the firm may have a right to opt out of AI training but never used it because they did not know it was an option.

— **Operating under updated terms the firm never reviewed:** meaning the contract the firm signed last year may no longer govern what the vendor does with AI.

The vendor governance audit in this playbook is specifically designed to surface these situations. The vendor inventory process asks not just which AI tools the firm uses, but which AI features exist within the tools the firm already uses. For many small firms, the audit produces a map of AI exposure that surprises them, not because they took risks, but because the risks arrived without being flagged.

PRACTICE DEVELOPMENT OPPORTUNITY

The shadow AI problem is also a client-service opportunity. Firms that complete this audit and document their results can add a vendor governance disclosure to their engagement letters, offer their own review process as a differentiator, and, for firms serving business clients, position themselves to advise those clients on the same governance issues.

Add to new client intake: 'Has your business reviewed the AI data-handling terms for the software platforms you use? Would a brief review be useful?'

What the Audit Finds

Illustrative planning scenario, not survey results: in a small firm's first vendor audit, test for findings like these (see Important Notice):

— One to three Tier 4 (Critical) vendors already processing client data, with AI terms that have never been reviewed

— Two to four Tier 3 (High) vendors with AI features enabled by default, where the opt-out was available but never exercised

— A gap between the firm's general vendor contract (signed at subscription) and the vendor's current AI terms (added later in an update)

— A vendor with a training opt-out that requires an affirmative action by an account administrator, and no one in the firm knew it existed

The audit should produce specific findings. A documented list of exactly where the firm stands, exactly what needs to be fixed, and exactly what to configure before the next client file lands in a vendor platform. That is what reasonable efforts looks like.

Ethics Risks and Governance Framework

The vendor governance program is built on four governance principles that apply to every vendor decision, regardless of the tool or the practice area:

— **Ask in writing:** The firm sends a written questionnaire and requires written responses from someone with authority. Verbal assurances from sales representatives are not part of the governance record.

— **Get written commitments:** The critical protections, no training on client data, deletion on demand, breach notification, confidentiality obligations, must be contractual. A privacy policy on a website is not a contract.

— **Document the decision:** Every Tier 3 or Tier 4 vendor gets a written decision memo. The memo states what was reviewed, what the risks are, what limits apply, and who approved.

— **Schedule re-review:** Vendor terms change. AI features expand. New subprocessors appear. A review that was current 18 months ago may not be current today. The governance calendar is part of the governance program.

High-Risk Failure Modes

FAILURE MODE 1: THE UNCHECKED AI FEATURE

A Tier 4 vendor, the firm's practice management platform, document management system, or legal research tool, ships an AI feature. It is enabled by default. No one in the firm notices. Client documents, emails, and billing data are now feeding the feature. Three months later, the vendor updates its terms to allow use of interaction data to improve the model. The firm never gets a plain-English alert. The exposure exists.

The fix: the vendor audit inventory asks, specifically, whether AI features are enabled and whether they are enabled by default. The re-review calendar catches the update. The configured opt-out prevents the training use.

FAILURE MODE 2: THE CONFIDENTIALITY BREACH VIA FREE TOOL

A paralegal uses a free AI tool, a web-based summarizer, a transcription tool, a general-purpose chatbot, to process a client's deposition transcript, medical records, or financial documents. The tool's terms may permit use of inputs for model improvement. The records leave the firm's control in a way that cannot be recalled. The client never consented. Rule 4-1.6 is implicated.

The fix is not banning AI tools across the firm. It is a written policy that specifies which tools may touch client data and which may not, and training that ensures staff know the difference. The Practical Vendor Rules for Law Firm Staff table gives the staff rules. The policy language is in Appendix A.

FAILURE MODE 3: THE HALLUCINATED VENDOR CLAIM

A lawyer reviews a vendor questionnaire response that says "our platform does not train on customer data." The lawyer approves the vendor for Tier 3 use. Later, the vendor's actual contract language permits training on "aggregated and anonymized" data that includes processed versions of customer inputs. The questionnaire response was not false, but it was incomplete. The contract said something different.

The fix: the audit process requires reviewing the actual contract, DPA, AI addendum, and privacy policy, not just the questionnaire response. The decision memo records which documents were reviewed. The red-flag review process in Stage 7 of the audit specifically checks for gaps between questionnaire responses and contract language.

FAILURE MODE 4: THE STALE REVIEW

A Tier 4 vendor was fully reviewed 18 months ago. The firm's evidence file is complete, the decision memo is signed, and the settings are configured. Then the vendor makes a material change to its AI terms, adds a new AI model provider as a subprocessor, and updates its training opt-out policy. The firm never reviews. The approved status is still in the file. The current exposure is not.

The fix: a re-review calendar that treats vendor governance as an ongoing process rather than a one-time event. The re-review schedule in Stage 12 sets the cadence. Tier 4 vendors are reviewed every 6–12 months. Any vendor with a material AI, privacy, or security change triggers an immediate review.

Data Classification Framework

Not every piece of firm data carries the same risk, and not every vendor deserves the same scrutiny. The classification framework below is the same four-tier system used in the vendor risk tiers in Stage 2. Use it to match data categories to vendor access decisions.

Tier	Data Category	Examples	Approved Tool Standard
Tier 1 Public	No client or confidential data	Office supplies vendors, generic scheduling pages with no matter details	Basic vendor file only
Tier 2 Firm Business	Firm administrative or limited client contact data only	Newsletter platform, general CRM, appointment scheduler (no matter details)	Short questionnaire; no DPA required if no client confidential data
Tier 3 Client Matter	Client files, matter data, email, pleadings, billing, contracts, discovery	Practice management, cloud storage, email platform, document management, e-signature, transcription	Full audit; DPA or written data addendum required (firm minimum standard); annual review
Tier 4 Highly Sensitive	Privileged/ confidential plus AI processing, OR financial/trust data, health data, criminal/family/immigration matter data, large-scale document review	Legal AI tools, M365 Copilot or Gemini on client files, e-discovery AI, intake bots, medical-records processing tools	Full audit; DPA or written data addendum required (firm minimum standard); partner approval; contract review; review every 6–12 months

Vendor Minimum Standards

Before sending questionnaires, the firm should adopt written minimum standards. Without them, every vendor response becomes a negotiation rather than a comparison.

Area	Required Standard
Confidentiality	Vendor agrees to protect confidential information and restrict use to providing the service.
AI training	Client and firm data are not used to train public or shared AI models unless the firm gives written consent.
Data retention	Vendor states how long data, prompts, outputs, metadata, logs, and backups are retained.
Data deletion	Vendor explains how the firm can delete and export data, and what happens on termination.
Human review	Vendor discloses whether humans may review firm data, prompts, outputs, support tickets, or model interactions.
Subprocessors	Vendor identifies subprocessors and gives notice of material changes.
Security	Encryption in transit and at rest; MFA/SSO options; access controls; audit logs where appropriate.
Breach notice	Vendor provides notice of security incidents affecting firm or client data.
Legal process	Vendor explains whether it will notify the firm of subpoenas or legal demands unless prohibited.
Data location	Vendor discloses where data may be stored or processed.
Contract priority	Vendor confirms which document controls if website terms conflict with the contract.
Change notice	Vendor provides notice before material privacy, AI, data retention, or security changes.

Approval Levels

Risk Tier	Approval Required
Tier 1	Office manager or admin.
Tier 2	Office manager and responsible lawyer.
Tier 3	Managing partner or designated technology partner.
Tier 4	Managing partner, written risk memo, and contract review.

Practical Vendor Rules for Law Firm Staff

Post these where staff can access them. Include them in new-hire onboarding.

Situation	Rule
Public or free AI tool	Do not enter client names, facts, documents, transcripts, pleadings, financials, medical records, or privileged communications.
Approved enterprise AI tool	Use only within the approved workspace or account.
Vendor not yet reviewed	Do not upload client confidential information until the vendor review is complete.
AI summarization of client documents	A lawyer must review the output before use.
AI legal research	A lawyer must verify all authorities in a primary legal database before filing or relying on.
Intake chatbot or AI intake tool	Must clearly disclose that it is AI and not a lawyer or firm employee; limit intake to factual and administrative information; do not provide legal advice; route legal questions to a lawyer.
Transcription tools	Use only approved tools with retention and confidentiality settings reviewed.
New vendor	No client data until vendor review is completed.
New AI feature appears in an existing tool	Treat as unapproved until reviewed.

The Audit Process: Stage by Stage

The audit runs in twelve stages. Run them in order for a new firm doing its first review. For an ongoing program, Stages 1–4 are annual refreshes; Stages 5–12 apply to any new vendor or material change. The full workflow produces the evidence file that answers the question: “What did you do before giving this vendor access to client data?”

Stage	Action	Output
1	Build vendor inventory	Complete vendor list
2	Map data touched and make initial tier assessment	Data map and provisional tier
3	Identify AI features in each vendor platform	AI inventory
4	Finalize risk tier and minimum standards	Risk rating and standards
5	Open evidence file and save current materials	Initial evidence file
6	Send vendor request email and questionnaire	Written request
7	Collect responses and assess against standards	Response record and risk notes
8	Send follow-up questions where needed	Clarified record
9	Approve, limit, or reject each vendor	Decision memo
10	Configure settings and document them	Screenshots on file
11	Train users on approved-use rules	Staff guidance record
12	Set re-review calendar	Ongoing diligence schedule

Stage 1: Build the Vendor Inventory

Start with every vendor, not just dedicated AI vendors. AI is now embedded in many ordinary legal and business tools. The inventory should include: Microsoft 365, Google Workspace, practice management platforms (Clio, MyCase, Practice Panther, Filevine, etc.), legal research platforms (Westlaw, Lexis, vLex, CoCounsel), document management, email, cloud storage (Dropbox, Box, SharePoint, OneDrive), Zoom, RingCentral, Adobe, Calendly, Mailchimp or other marketing platforms, website chat tools, transcription services, answering services, CRM tools, intake tools, e-signature platforms (DocuSign, Clio Sign, PandaDoc), PDF tools, and payment processors (LawPay, AffiniPay). Payment processors should be reviewed because they touch financial, trust, and client payment data.

For each vendor, capture:

Field	What to Capture
Vendor name	Microsoft, Google, Clio, Dropbox, Zoom, LawPay, QuickBooks, etc.
Product/service	Email, document storage, billing, intake, research, transcription, scheduling, marketing, payments.
Business owner	Who in the firm uses it most.
Admin owner	Who controls settings.
Data touched	Client documents, emails, billing data, trust data, intake data, financial records, medical records.
AI features present	Copilot, Gemini, drafting, summarization, transcription, predictive search, classification.
AI features enabled?	Yes / No / Unknown.
Client confidential data processed?	Yes / No / Unknown.
Contract/DPA available?	Yes / No.
Last reviewed	Date.
Risk tier	Low / Medium / High / Critical.
Decision	Approved / Approved with limits / Not approved / Needs follow-up.

Stage 2: Classify Vendors by Risk Tier

Not every vendor deserves the same scrutiny. The firm's coffee supplier does not need an AI questionnaire unless the espresso machine is uploading client intake notes to a model. If so, stop using it and start over. Use the data map to make an initial tier assessment here. Check AI features in Stage 3, then finalize the tier and minimum standards in Stage 4.

Tier	Vendor Type	Examples	Review Level
Tier 1: Low	No client or confidential data.	Office supplies, general vendors, generic scheduling pages with no matter details.	Basic vendor file.
Tier 2: Medium	Firm business data or limited client contact data.	Newsletter platform, CRM, payment processor, appointment scheduler.	Short questionnaire.
Tier 3: High	Client files, matter	Practice management, cloud storage,	Full audit.

	data, email, pleadings, contracts, discovery, billing.	email, document management, e-signature, transcription.	
Tier 4: Critical	Privileged/ confidential material plus AI processing, financial/trust data, health data, criminal/family/immigration data, or large-scale document review.	Legal AI, Microsoft Copilot or Gemini on client files, e-discovery AI, intake bots, outsourced answering/intake.	Full audit plus partner approval plus contract review.

Stage 3: Identify AI Features

For each Tier 3 and Tier 4 vendor, identify which AI features are present in the platform and whether they are enabled. Check:

— The vendor's product changelog and recent release notes

— The admin settings panel, many AI features are enabled by default in admin settings without requiring explicit activation

— The vendor's trust page or AI-specific documentation

— The vendor's AI addendum or AI terms of service (often a separate document from the main contract)

> **IMPORTANT**
>
> Do not rely on a sales representative's answer to questions about AI features. Ask the question in the questionnaire and require it to be answered by someone from the security, legal, privacy, compliance, or trust team.
>
> Save PDFs or screenshots with dates. Vendor pages change. Memory changes. Sales reps change. The PDF sits there quietly and does its job.

Stage 4: Assign Risk Tiers and Define Minimum Standards

After the AI-feature check, revisit the initial classification from Stage 2 and finalize each vendor's risk rating. Then set your firm's written minimum standards before sending questionnaires. Without standards defined in advance, every vendor response becomes a debate about what is acceptable. The Vendor Minimum Standards table gives you the baseline. Adapt it to your practice area and client base.

Stage 5: Build the Evidence File

Open the evidence file before sending the questionnaire. Save the existing contract, DPA, AI terms, privacy policy, and any current admin-setting screenshots. Add the vendor's response, internal review, and decision as later stages finish. For each Tier 3 and Tier 4 vendor, the completed file should contain:

- Vendor questionnaire response
- Name, title, and email of respondent
- Date of response
- Vendor contract, MSA, or order form
- Data processing addendum
- AI addendum or AI terms
- Privacy policy
- Security whitepaper or trust center PDF
- SOC 2 Type II report or bridge letter, if available
- ISO 27001 certificate, if available
- Subprocessor list
- Data retention and deletion policy
- Screenshots of admin settings
- Internal review memo
- Approval or limitation decision
- Calendar reminder for re-review

Organize the evidence file by vendor, with subfolders matching the folder structure in Stage 10.

Stage 6: Send the Vendor Request Email and Questionnaire

The copy-ready vendor request emails are in Appendix D. For major vendors, send to the account representative and ask that it be routed to the vendor's security, legal, privacy, compliance, or trust team. A response from a sales representative guessing from a script is not a vendor questionnaire response. It is a sales call. The questionnaire in Appendix C is built to identify whether you are getting a real answer or a scripted one.

RED FLAGS IN VENDOR RESPONSES

'We use AI but cannot disclose the model provider.' Hard to assess confidentiality and data flow.

'Data may be used to improve services.' Could include model training or product analytics.

'Customer data may be reviewed by humans.' Need scope, controls, logging, and opt-out.

'Deleted data may remain in backups indefinitely.' Retention problem.

'Terms may change at any time.' Ongoing risk.

'We do not sign DPAs.' Problem for any vendor touching sensitive data.

'Ask your sales rep.' Not an answer.

'See our website.' Not sufficient for Tier 3 or Tier 4 vendors.

'AI features are enabled by default.' Risk of accidental disclosure without configuration.

'No breach notice period stated.' Weak incident response protection.

'No subprocessor list.' Unknown downstream exposure.

Stage 7: Review the Responses

Assign one person in the firm to review each vendor. In a small firm, this can be the managing partner, office manager, outside consultant, or designated technology lead. But someone owns it. For each response, check:

— Are the responses complete? Or are critical questions answered with “see our website” or left blank?

— Does the response address AI training, specifically whether client inputs are used to train, fine-tune, or improve models?

— Is retention clearly stated for each data category, active data, deleted files, backups, logs, AI interaction data?

— Is deletion on demand available? Is it in the contract?

— Are subprocessors identified? Are AI model providers named?

— Can AI features be disabled or limited at the admin level?

— Is there a meaningful breach notification process?

Compare the questionnaire responses against the actual contract, DPA, AI addendum, and privacy policy. Questionnaire responses that conflict with actual terms are a red flag. The contract governs.

Stage 8: Send Follow-Up Questions

If a response is incomplete, vague, or conflicts with the vendor’s published terms, send the follow-up email in Appendix D. The follow-up asks for direct written answers to the specific questions that were not clearly answered in the first response. Keep a record of follow-up requests and responses in the vendor evidence file.

Stage 9: Approve, Limit, or Reject Each Vendor

For each Tier 3 or Tier 4 vendor, create a short internal decision memo. The memo is not a lengthy document. It is a one-page record of what you reviewed and what you decided.

Section	Content
Vendor	Name and product.
Use case	What the firm uses it for.
Data involved	Categories of client and firm data.
AI features	Enabled, disabled, or limited.
Key documents reviewed	Contract, DPA, AI terms, privacy policy, SOC 2, questionnaire.
Key risks	Training, retention, human review, subprocessors, data location.
Safeguards	MFA enabled, AI disabled, opt-out confirmed, access limits, retention settings.
Decision	Approved, approved with limits, or not approved.

Limits	No privileged documents, no client names, no financial records, etc.
Approver	Name, title, and date.
Next review date	Usually annual; sooner for high-risk vendors.

The three decision categories:

APPROVE

- Written vendor responses are complete.
- Client data is not used for public or shared AI model training without written consent.
- Retention and deletion are clear.
- Confidentiality obligations are contractual.
- Security documentation is acceptable.
- AI settings can be controlled.
- Subprocessors are disclosed.
- Breach notice exists.
- The firm can document the review.

APPROVE WITH LIMITS

Vendor Issue	Limitation
AI terms unclear	No client confidential data in AI features.
Retention too long for high-sensitivity data	Use only for administrative data.
Human review of data possible	Do not upload privileged documents.
No SOC 2 available	Use only for low-risk, non-confidential data.
AI enabled by default	Disable AI features before use; document configuration.
Subprocessors unclear	No sensitive client or matter data.

REJECT OR PAUSE

- Vendor refuses written responses.
- Vendor uses customer data for AI training with no opt-out.
- Vendor cannot explain retention.
- Vendor cannot explain deletion.
- Vendor allows broad human review with weak controls.
- Vendor changes terms unilaterally without meaningful notice.
- Vendor refuses confidentiality obligations.

— Vendor has no meaningful breach notice process.

— Vendor answers conflict with its published terms.

Stage 10: Configure Settings and Document Them

After the decision memo is signed, configure the vendor's admin settings to implement the firm's decision. Take screenshots of key settings and save them with dates in the vendor's evidence folder. The evidence folder structure below is the recommended standard:

Vendor Due Diligence/

01 Vendor Inventory/

Vendor Inventory.xlsx

02 Approved Vendor Standards/

Firm Vendor AI and Data Governance Policy.pdf

03 Vendor Files/

Microsoft 365/

01 Contract Terms/

02 Security Documents/

03 AI Terms/

04 Vendor Questionnaire/

05 Admin Settings Screenshots/

06 Internal Decision Memo/

[Clio, Google Workspace, Dropbox, Zoom, etc.]

04 Annual Reviews/

2026 Review/

2027 Review/

05 Rejected or Restricted Vendors/

Stage 11: Train Staff

The governance policy in Appendix A and the Practical Vendor Rules for Law Firm Staff table give staff the substance they need. The training should cover:

— Which tools are approved for client data, and which are not

— What the data tiers mean in plain terms, what can and cannot go into each tool

— The rule that no AI-generated legal research or document is filed without attorney review

— The rule that new AI features in existing tools are unapproved until reviewed

— Who to ask when a new vendor or tool comes up, the AI Policy Supervisor

— Where the approved tool list lives and how to find the current version

Training does not require a dedicated session. A 30-minute staff meeting with the practical rules table and a few live examples, one safe use, one requiring caution, one prohibited, is this firm's minimum initial training step. Additional training may be appropriate depending on role, tool, and data sensitivity. Document who attended and when.

Stage 12: Set the Re-Review Schedule

Vendor Type	Review Frequency
Tier 1	Every 2 years.
Tier 2	Annually.
Tier 3	Annually.
Tier 4	Every 6–12 months.
Any vendor with major AI, security, or privacy changes	Immediate review.
Any vendor after a material AI, security, privacy, or contract change, or after a breach or security incident	Immediate review.

Add re-review reminders to the firm's calendar at the time of each vendor decision. The review is not a full re-audit. It is a check: have the vendor's AI terms, privacy policy, DPA, or subprocessor list changed? If yes, what changed and does the original decision still hold?

NEXT STEP

The practical rollout plan for a firm doing its first vendor audit is in Appendix E. It runs four weeks for the initial review and converts to an ongoing cadence.

Start this week with Stage 1: pull a complete vendor list, identify which vendors touch client data, and assign a risk tier to each. That single output tells you where the Tier 4 work begins.

Prompts Library

HOW TO USE THIS LIBRARY

Strip all client identifiers before pasting into any tool, even approved enterprise tools. Use anonymized matter descriptions.

Verify every output against the vendor's actual contract, DPA, and terms before relying on it. AI outputs are first drafts.

These prompts are calibrated for small Florida law firms. Treat outputs as working drafts that require attorney review.

Document AI use in the firm's governance file, including which tool was used and what review the output received.

PROMPT 01: BUILD A VENDOR INVENTORY · VENDOR DISCOVERY

```
You are helping a small Florida law firm build a complete vendor inventory for a
vendor AI and data governance audit.

Using the firm description below, generate a comprehensive list of vendor
categories and example vendors that commonly process law firm data.

For each vendor category, provide:
1. Category name
2. Example vendor names common in small Florida firms
3. Data categories likely processed (client documents, email, billing, trust data,
etc.)
4. Whether AI features are commonly present in this vendor type
5. Default risk tier (Tier 1/2/3/4) based on typical data handling

[PASTE FIRM DESCRIPTION: practice areas, size, current known tools]
```

PROMPT 02: IDENTIFY AI FEATURES IN A VENDOR PLATFORM · VENDOR DISCOVERY

```
You are helping a small Florida law firm identify which AI features exist in a
specific vendor platform and whether they may be enabled by default.

For the vendor described below:
1. List known AI-enabled features as of your knowledge cutoff
2. Identify which features are typically enabled by default versus requiring
activation
3. Identify what data categories each AI feature may process
```

```
4. List where in the admin settings AI features can typically be enabled or disabled
5. Note any known opt-out mechanisms for AI model training

Note what you do not know and flag any features that should be verified directly with the vendor.
Do not make definitive claims about current settings, vendor platforms change. This is a starting point for the questionnaire, not a substitute for it.

[PASTE VENDOR NAME AND PRODUCT]
```

PROMPT 03: CLASSIFY A VENDOR BY RISK TIER · RISK ASSESSMENT

```
You are helping a small Florida law firm classify a vendor into the appropriate risk tier for vendor AI and data governance purposes.

The four tiers are:
- Tier 1 (Low): No client or confidential data
- Tier 2 (Medium): Firm business data or limited client contact data
- Tier 3 (High): Client files, matter data, email, pleadings, contracts, billing
- Tier 4 (Critical): Privileged/confidential plus AI processing, OR financial/trust data, health data, or large-scale document review

For the vendor below:
1. Recommend a risk tier with one-sentence rationale
2. List the specific data categories that drive the tier assignment
3. List any AI features present that elevate the tier
4. Identify any gaps in the information provided that would affect the classification
5. Recommend the review level required (basic vendor file / short questionnaire / full audit)

[PASTE VENDOR NAME, PRODUCT, AND WHAT DATA IT PROCESSES]
```

PROMPT 04: MAP DATA CATEGORIES TO VENDOR ACCESS · RISK ASSESSMENT

```
You are helping a small Florida law firm identify which categories of firm and client data a specific vendor may access.

For the vendor and use case below:
1. List the data categories this vendor likely processes (client documents,
```

emails, billing records, trust data, intake data, medical records, financial records, etc.)
2. Identify which data categories are most sensitive for a law firm
3. Flag any data categories that trigger elevated review requirements under Rule 4-1.6 of the Florida Rules of Professional Conduct
4. Identify which data categories, if used for AI model training, would create the highest confidentiality risk
5. Recommend any data categories that should be excluded from this vendor's access as a precondition to approval

[PASTE VENDOR NAME, PRODUCT DESCRIPTION, AND HOW THE FIRM USES IT]

PROMPT 05: CUSTOMIZE THE VENDOR QUESTIONNAIRE · QUESTIONNAIRE PREP

You are helping a small Florida law firm customize the standard vendor AI and data governance questionnaire for a specific vendor type.

The standard questionnaire covers: vendor identity, data handled, AI use, confidentiality, data retention and deletion, security controls, subprocessors and third parties, legal process and government requests, contract and policy changes, and vendor certification.

For the vendor below, adapt the standard questionnaire by:
1. Adding three to five vendor-specific questions that address the specific AI features or data risks of this vendor type
2. Identifying which standard sections are most critical for this vendor and should be marked as required answers
3. Flagging any questions where the vendor's standard contract typically leaves gaps that the questionnaire should surface
4. Suggesting the appropriate respondent title (security, legal, privacy, compliance, or trust team) for this vendor type

[PASTE VENDOR NAME, PRODUCT TYPE, AND PRIMARY DATA HANDLED]

PROMPT 06: ANALYZE A VENDOR CONTRACT FOR DATA HANDLING TERMS · DOCUMENT REVIEW

You are helping a small Florida law firm review a vendor contract for data handling, confidentiality, AI, and privacy provisions.

For the contract text below:
1. Identify and quote the key provisions governing confidentiality, data use, and

```
data protection
2. Identify whether the contract restricts the vendor from using firm or client data for AI model training
3. Identify the data retention and deletion terms, including what happens on termination
4. Identify whether subprocessors are addressed, and whether the firm receives notice of changes
5. Identify whether breach notification is defined, and the required notice period
6. Flag any provisions that conflict with the minimum standards for a Florida law firm vendor

Flag gaps where standard protections are absent. Do not make a legal determination, flag issues for attorney review.

[PASTE ANONYMIZED CONTRACT TEXT OR RELEVANT SECTIONS]
```

PROMPT 07: ANALYZE A DATA PROCESSING ADDENDUM FOR GAPS · DOCUMENT REVIEW

```
You are helping a small Florida law firm review a vendor's Data Processing Addendum (DPA) for adequacy.

For the DPA text below:
1. Identify whether it restricts use of firm/client data to service delivery only
2. Identify whether it addresses AI model training, fine-tuning, or improvement using firm data
3. Check whether deletion is addressed on termination, timeline, certification, and backup scope
4. Check whether subprocessors are listed and whether there is a notice requirement for changes
5. Check whether breach notification obligations are defined, with a specific notice period
6. Flag any provisions that fall below the minimum vendor standard for a Florida law firm
7. Note any provisions that are absent and should be present for Tier 3 or Tier 4 vendor approval

Do not make a legal determination. Flag issues for attorney review.

[PASTE ANONYMIZED DPA TEXT]
```

PROMPT 08: ANALYZE AN AI ADDENDUM OR AI TERMS SECTION · DOCUMENT REVIEW

```
You are helping a small Florida law firm review a vendor's AI-specific terms, AI
addendum, or AI policy.

For the AI terms text below:
1. Identify whether firm or client data is used to train, fine-tune, test,
improve, or evaluate AI models
2. Identify whether there is an opt-out mechanism, and whether it is affirmative
or automatic
3. Identify whether outputs from one customer can be used to improve responses for
another customer
4. Check whether AI interaction logs (prompts, outputs, embeddings) are retained,
and for how long
5. Identify whether humans employed by the vendor or third-party AI providers may
review firm prompts, outputs, or uploaded documents
6. Flag any provisions that would conflict with a small law firm's confidentiality
obligations under Florida Bar Ethics Opinion 24-1 and Rule 4-1.6
7. Identify any features that are enabled by default that should require explicit
firm consent

[PASTE ANONYMIZED AI TERMS TEXT]
```

PROMPT 09: IDENTIFY RED FLAGS IN VENDOR QUESTIONNAIRE RESPONSES · RESPONSE REVIEW

```
You are helping a small Florida law firm review a completed vendor questionnaire
for red flags and incomplete answers.

For the questionnaire responses below:
1. List any responses that are evasive, incomplete, or answered with "see our
website" or similar deflections
2. Identify any answers that conflict with the vendor's published terms, DPA, or
AI addendum
3. Flag any answers that indicate the vendor uses customer data for AI training
without a clear opt-out
4. Flag any answers where retention periods are unclear, unlimited, or extend
indefinitely into backups
5. Flag any answers where human review of firm data, prompts, or outputs is
possible without meaningful controls
6. Provide a risk summary: high / medium / low, with the top three concerns listed

[PASTE QUESTIONNAIRE AND RESPONSES]
```

PROMPT 10: DRAFT FOLLOW-UP QUESTIONS FOR VAGUE VENDOR RESPONSES · RESPONSE REVIEW

```
You are helping a small Florida law firm draft follow-up questions for a vendor
whose questionnaire responses were incomplete or vague.

Based on the original questionnaire responses below, draft a follow-up email that:
1. Acknowledges the initial response professionally
2. Identifies the specific questions that were not directly answered
3. Asks for direct written answers to each gap item
4. Requests that the response come from the vendor's legal, privacy, security,
compliance, or product policy team
5. Requests that the respondent include their name, title, department, email
address, and date of response
6. States that general references to the vendor's website or public documentation
are not sufficient for this review

Keep the tone professional and direct. Do not threaten or characterize the initial
responses as deceptive.

[PASTE ORIGINAL QUESTIONNAIRE RESPONSES WITH GAPS NOTED]
```

PROMPT 11: DRAFT AN INTERNAL VENDOR DECISION MEMO · DECISION AND DOCUMENTATION

```
You are helping a small Florida law firm draft an internal vendor decision memo
for its governance file.

Using the information below, draft a decision memo that covers:
1. Vendor name and product
2. Use case (what the firm uses it for)
3. Data categories involved
4. AI features reviewed (enabled, disabled, or limited)
5. Key documents reviewed (contract, DPA, AI terms, privacy policy, security
documentation, questionnaire)
6. Key risks identified (training, retention, human review, subprocessors, data
location)
7. Safeguards implemented (MFA, AI disabled, opt-out confirmed, access limits,
retention settings)
8. Decision: Approved / Approved with limits / Not approved
9. Any limits on use (e.g., no privileged documents, no client names, no financial
records)
10. Approver name, title, and date
11. Next review date
```

```
Use plain language. The memo is an internal record, not a legal document.

[PASTE VENDOR SUMMARY, QUESTIONNAIRE RESPONSES, AND KEY DOCUMENTS REVIEWED]
```

PROMPT 12: GENERATE A VENDOR RISK SUMMARY FOR THE EVIDENCE FILE · DECISION AND DOCUMENTATION

```
You are helping a small Florida law firm generate a one-page risk summary for a vendor's evidence file.

Using the information below, create a vendor risk summary that includes:
1. Overall risk rating (Low / Medium / High / Critical) with a one-sentence rationale
2. Top three risks identified in the review
3. Safeguards in place or required before approval
4. Whether the vendor meets the firm's minimum standards in each of the twelve areas (confidentiality, AI training, retention, deletion, human review, subprocessors, security, breach notice, legal process, data location, contract priority, change notice)
5. One-sentence recommendation: approve, approve with limits, reject, or request additional information

Keep to one page. This summary goes in the vendor evidence folder alongside the full questionnaire and decision memo.

[PASTE VENDOR QUESTIONNAIRE RESPONSES AND REVIEWED DOCUMENTS SUMMARY]
```

PROMPT 13: DRAFT PRACTICAL AI USE RULES FOR LAW FIRM STAFF · STAFF TRAINING AND POLICY

```
You are helping a small Florida law firm draft practical, plain-language AI use rules for staff.

Based on the firm's approved vendor list and data classification framework below, draft a one-page staff rule sheet that covers:
1. Which tools are approved for client data and at what tier
2. Specific prohibitions: what data can never go into unapproved tools
3. The rule for AI-generated work product requiring attorney review before use
4. The rule for new AI features in existing tools (treat as unapproved until reviewed)
5. Who to contact when a new tool, vendor, or AI feature arises (the AI Policy Supervisor)
6. The consequence of an unapproved disclosure: what the staff member should do
```

```
immediately

Use short sentences. Write for a non-technical audience. Avoid legal jargon.
Do not include banned words: delve, deep dive, leverage, robust, pivotal,
groundbreaking, supercharge, revolutionize, harness, nuanced, multifaceted, or
corporate filler phrases.

[PASTE APPROVED TOOL LIST AND FIRM'S RISK TIER SUMMARY]
```

PROMPT 14: DRAFT A VENDOR RE-REVIEW AGENDA AND NOTICE · ONGOING COMPLIANCE

```
You are helping a small Florida law firm prepare for a scheduled annual vendor re-
review.

For the vendor below, draft a re-review agenda that includes:
1. What has changed since the last review (check the vendor's changelog, recent
product updates, and revised terms if available)
2. Key questions to verify: Has the AI training policy changed? Have new
subprocessors been added? Have retention or deletion terms changed? Have security
certifications lapsed or been renewed?
3. Documents to re-pull and compare to the prior review: current DPA, AI terms,
privacy policy, subprocessor list
4. Any settings to re-verify in the admin panel
5. A decision prompt: does the prior approval still hold, require modification, or
require a new full review?

Also draft a brief internal re-review notice (2–3 sentences) that can be sent to
the managing partner or AI Policy Supervisor to kick off the review.

[PASTE VENDOR NAME, PRODUCT, DATE OF LAST REVIEW, AND KEY PRIOR DECISION NOTES]
```

Appendix A: Sample AI Governance Policy

Adapt this policy to your firm's jurisdiction, clients, vendor contracts, and applicable obligations. Have a Florida-licensed attorney review it before adoption. Have all staff sign the acknowledgment page.

Purpose

This policy governs the use of artificial intelligence tools and AI-enabled vendor platforms by all lawyers, paralegals, law clerks, administrative staff, and contractors of [Firm Name] (the Firm). Its purpose is to ensure that AI use is consistent with the Firm's obligations under the Florida Rules of Professional Conduct, applicable Florida Bar ethics opinions, and the Firm's duty to protect client confidential information.

General Principles

— Client confidential information is the Firm's most critical protected asset. No AI tool may process client confidential information unless the tool has been reviewed and approved under this policy.

— AI tools assist lawyers. They do not replace lawyer judgment, supervision, or professional responsibility.

— AI-generated work product is a first draft. Every output used in a client matter must be reviewed and verified by a lawyer before use.

— Vendor governance is an ongoing obligation. Approved vendor status does not last indefinitely. Vendor terms change, AI features expand, and subprocessors change.

Definitions

— **AI-enabled tool:** Any software platform, feature, or service that uses artificial intelligence, machine learning, generative AI, large language models, automated classification, prediction, summarization, transcription, or similar technology to process or generate content.

— **Client confidential information:** All information relating to the representation of a client, including documents, communications, financial data, medical records, matter notes, billing records, and intake data.

— **Approved tool:** An AI-enabled tool that has been reviewed under the Firm's vendor governance process and approved for use with client confidential information.

— **AI Policy Supervisor:** The lawyer designated by the managing partner to oversee AI governance, maintain the approved tool list, and serve as the point of contact for AI-related questions.

Permitted Uses

— Using approved enterprise AI tools within the approved workspace or account

— Using any AI tool for firm administrative tasks that do not involve client confidential information

— Using AI for legal research verification (not as the sole source of authority)

— Using AI to draft documents and communications, subject to attorney review before use or delivery

Prohibited Uses

— Entering client names, matter facts, documents, pleadings, transcripts, financial records, medical records, or any client confidential information into any unapproved AI tool

— Using free or consumer AI tools for any task involving client confidential information

— Filing any AI-generated legal research, citation, or document without independent attorney verification

— Using any vendor platform whose AI features have not been reviewed under this policy

— Using any new AI feature that appears in an existing tool until it has been reviewed and approved

Confidentiality and Data Handling

The firm may not enter, upload, transmit, or process client confidential information, privileged communications, client documents, matter materials, financial information, personal information, or other sensitive data in any vendor platform or AI-enabled feature unless the vendor has been reviewed and approved under the Firm's vendor due diligence process. Approval must be documented in writing and must address confidentiality, AI training, data retention, deletion, security, human review, subprocessors, and breach notification.

Before an approved third-party generative AI tool is used in a particular matter, the responsible lawyer must determine whether the use would disclose confidential information to a third party and whether the disclosure is authorized by informed consent or an applicable Rule 4-1.6 exception. The firm will consider Opinion 24-1's recommendation to obtain informed consent for covered third-party use. Vendor approval alone does not decide that matter-specific question (Florida Bar Ethics Op. 24-1, p. 2).

Court and Tribunal Filings

No AI-generated legal authority, citation, or case description may be filed with any court without independent verification against a primary source by the responsible attorney. For Florida state court filings: follow amended Rule 2.515(d)(2) under SC2026-0673 and AOSC26-12 (effective June 15, 2026). The statewide order bars court-imposed circuit-level AI disclosure and certification requirements; review circuit orders for unrelated procedural requirements. For federal court filings: check the assigned judge's current standing order. Florida state court AI disclosure requirements do not govern federal courts. (AOSC26-12, pp. 2–3)

Incident Response

Any lawyer or staff member who discovers or suspects that client confidential information has been shared with an unapproved AI tool or vendor must immediately report the incident to the AI Policy Supervisor and the managing partner. The managing partner will assess client and Bar disclosure with counsel. If Florida residents' personal information may have been accessed without authorization, bring in Florida breach counsel immediately. Statutory notice turns on the definitions and conditions in Fla. Stat. § 501.171, not on a discretionary firm preference (Fla. Stat. § 501.171(1), (3)–(4)).

FIPA's "personal information" includes a Florida individual's first name or initial and last name together with specified data elements, such as a Social Security number, driver license number, qualifying financial-account access information, or medical information. It also separately covers a user name or email address with credentials permitting online-account access. The statute excludes specified public or unusable

secured information; do not assume that a bare account number or every piece of health data automatically meets the definition (Fla. Stat. § 501.171(1)(g)).

A covered entity must notify affected Florida individuals as expeditiously as practicable and without unreasonable delay, no later than 30 days after it determines or has reason to believe a breach occurred, unless the statutory law-enforcement delay or documented no-likely-harm waiver applies. The waiver requires an appropriate investigation, consultation with relevant law enforcement, a written determination retained at least five years, and delivery of that determination to the Department of Legal Affairs within 30 days. The entity must notify the department of a breach affecting 500 or more Florida individuals as expeditiously as practicable, no later than 30 days after determination or reason to believe (Fla. Stat. § 501.171(3)(a), (4)(a)–(c)).

The entity may receive 15 additional days for individual notice under subsection (4) if it provides written good cause to the department within the initial 30 days. That extension is not automatic and does not extend the department-notice deadline. If the breached system is maintained by a third-party agent, the agent must notify the covered entity as expeditiously as practicable, no later than ten days after determination or reason to believe, and supply the information needed for the entity's notices. Confirm the applicable clock and response with Florida breach counsel (Fla. Stat. § 501.171(3)(a), (6)(a)).

Acknowledgment

I acknowledge that I have read and understand the Firm's AI Governance Policy. I agree to comply with its requirements and to immediately report any violation or suspected violation to the AI Policy Supervisor.

[Signature] _____

[Printed Name] _____

[Title] _____

[Date] _____

Appendix B: Client AI Disclosure Statement

Add to engagement letters or retainer agreements. Adapt to your practice and AI use. Have a Florida attorney review before adoption.

> **AI DISCLOSURE**
>
> Our firm uses artificial intelligence tools to assist with certain legal work. Here is what that means for you:
>
> 1. AI tools may assist with tasks such as legal research, document drafting, and communication preparation. A licensed attorney reviews all AI-assisted work before it is used in your matter.
> 2. We do not enter your confidential information, documents, or privileged communications into any AI tool unless that tool has been reviewed and approved under our vendor governance process.
> 3. AI tools can make errors, including incorrect legal citations or inaccurate summaries. We verify AI outputs before relying on them.
> 4. If you do not want AI tools used in your matter, please let us know in writing and we will accommodate that preference where reasonably practicable.

Implementation Notes

— Add this disclosure to all new engagement letters. For existing clients, consider adding it in the next substantive communication or at renewal.

— If a client specifically asks about AI use, Rule 4-1.4 requires an honest answer. The disclosure is your starting point, not your limit.

— Update the disclosure if your AI practices change materially.

— The disclosure need not name specific tools, your practices matter more than the brand.

— This sample disclosure is not blanket informed consent. Before a covered third-party generative AI use discloses confidential matter information, the responsible lawyer should assess authorization under Rule 4-1.6 and Opinion 24-1's informed-consent recommendation. Approved vendor status is a separate gate (Florida Bar Ethics Op. 24-1, p. 2).

Appendix C: Vendor AI, Data Retention, Confidentiality, and Security Questionnaire

Send this as an attachment or online form. For Tier 3 and Tier 4 vendors, require written completion by the vendor's security, legal, privacy, compliance, or trust team. A response from a sales representative is not sufficient.

Section A: Vendor Identity

Question	Vendor Response
Legal name of vendor	
Product/service reviewed	
Name, title, and email of person completing response	
Department of person completing response	
Date completed	
Does the vendor authorize the law firm to rely on these responses for vendor due diligence?	

Section B: Data Handled

Question	Vendor Response
What categories of firm data may be processed by your product?	
What categories of client data may be processed?	
Can users upload documents, emails, pleadings, contracts, discovery, transcripts, recordings, or other client materials?	
Does the product process metadata, usage data, search queries, prompts, outputs, chat history, support tickets, or audit logs?	
Is any data processed outside the United States? If yes, where?	
Is data segregated by customer/tenant? Explain.	

Section C: AI Use

Question	Vendor Response
Does your product use artificial intelligence, machine learning, generative AI, large language models, automated classification, prediction, summarization, drafting, or transcription?	
Identify each AI-enabled feature currently available in the product.	
Are AI features enabled by default?	
Can the firm disable AI features globally?	
Can the firm disable AI features by user, workspace, matter, client, or data type?	
What AI models are used? Identify whether they are proprietary, third-party, open-source, or hosted by another provider.	
Are prompts, inputs, uploaded documents, outputs, embeddings, metadata, or usage logs used to train, fine-tune, improve, evaluate, or test AI models?	
If yes, can the firm opt out? Describe the process and provide written confirmation of opt-out status.	
Are firm/client inputs used to train models available to other customers or the public?	
Are outputs generated for one customer used for another customer?	
Are prompts or outputs reviewed by vendor personnel or contractors?	
Are prompts or outputs reviewed by third-party AI providers?	
Are AI interactions logged? If yes, what is logged and for how long?	
Can the firm export AI interaction logs?	
Can the firm delete AI interaction logs?	
Does the product warn users about AI limitations, hallucinations, or the need for human review?	

Does the product provide citations, source references, audit trails, or confidence scores?	

Section D: Confidentiality

Question	Vendor Response
Does the vendor agree that firm/client data remains confidential?	
Does the vendor contractually restrict use of firm/client data to providing and supporting the service?	
Can vendor employees access firm/client data?	
If yes, under what circumstances?	
Are vendor employees and contractors bound by confidentiality obligations?	
Are access logs maintained for vendor employee access?	
Can the firm receive access logs upon request?	
Does vendor use customer data for advertising, marketing, benchmarking, analytics, product improvement, or AI development?	
If yes, identify what data is used and whether it is de-identified, aggregated, or customer-specific.	

Section E: Data Retention and Deletion

Question	Vendor Response
How long is active customer data retained?	
How long are deleted files retained before permanent deletion?	
How long are backups retained?	
How long are logs retained?	
How long are AI prompts, outputs, chat history,	

embeddings, transcripts, or summaries retained?	
Can the firm set custom retention periods?	
Can the firm delete specific client/matter data?	
Can the firm delete all firm data upon termination?	
What data remains after account termination?	
Can the vendor certify deletion after termination?	
How long does deletion from backups take?	
Does the vendor support legal hold?	
Does the vendor support export of firm data in a usable format before termination?	

Section F: Security Controls

Question	Vendor Response
Is data encrypted in transit?	
Is data encrypted at rest?	
Does the product support multi-factor authentication (MFA)?	
Does the product support SSO/SAML?	
Does the product support role-based access controls?	
Does the product support matter-level or client-level access restrictions?	
Does the product provide firm admin audit logs?	
Does the product alert admins to suspicious login or access activity?	
Does vendor perform background checks on personnel with access to customer data?	
Does vendor conduct regular penetration testing?	

Will vendor provide SOC 2 Type II, ISO 27001, or equivalent security documentation?	
Does vendor maintain cyber insurance?	
Does vendor have a written incident response plan?	
What is vendor's breach notification period?	

Section G: Subprocessors and Third Parties

Question	Vendor Response
Does vendor use subprocessors or third-party providers to process firm/client data?	
Provide current subprocessor list.	
Identify any AI model providers, cloud providers, transcription providers, analytics providers, or support providers.	
Does vendor require subprocessors to meet confidentiality and security obligations?	
Does vendor notify customers before adding or changing material subprocessors?	
Can the firm object to a new subprocessor?	

Section H: Legal Process and Government Requests

Question	Vendor Response
Will vendor notify the firm if it receives a subpoena, court order, search warrant, government request, or other legal demand for firm/client data?	
Are there exceptions to notice?	
Does vendor have a law enforcement request policy?	
Does vendor publish a transparency report?	

Section I: Contract and Policy Changes

Question	Vendor Response
Which terms govern the firm's use: order form, MSA, online terms, privacy policy, DPA, AI terms, or other documents?	
Can online terms be changed unilaterally?	
How will vendor notify the firm of material changes to privacy, AI, security, retention, or subprocessor terms?	
Does continued use equal acceptance of new terms?	
Can the firm reject material changes and terminate?	

Section J: Vendor Certification

CERTIFICATION

The undersigned represents that the responses above are accurate and complete to the best of vendor's knowledge as of the date signed, and that the law firm may rely on these responses for vendor due diligence, subject to the governing contract between the parties.

Field	Response
Name	
Title	
Company	
Email	
Date	
Signature / typed authorization	

Appendix D: Copy-Ready Vendor Emails and Decision Memo Template

Initial Vendor Request Email

For major vendors, send to the account representative and ask that it be routed to security, legal, privacy, compliance, or the trust team.

SUBJECT: VENDOR AI, DATA RETENTION, CONFIDENTIALITY, AND SECURITY DUE DILIGENCE REQUEST

Hello,

Our firm is conducting a vendor due diligence review of products and services that may process law firm data, client information, confidential materials, or AI-related inputs and outputs.

Because we are a law firm, we need written confirmation of your company's policies and practices regarding confidentiality, data retention, AI use, security, subprocessors, deletion, and related matters. We are not able to rely on verbal statements from sales or support representatives for this review.

Please complete the attached Vendor AI, Data Retention, Confidentiality, and Security Questionnaire and provide copies or links to the following current documents, if available: (1) master services agreement or governing terms; (2) data processing addendum; (3) privacy policy; (4) security documentation or trust center materials; (5) AI-specific terms, addendum, or policy; (6) data retention and deletion policy; (7) subprocessor list; (8) SOC 2 Type II report, ISO 27001 certificate, or equivalent security documentation; (9) incident response or breach notification policy; (10) any documentation showing whether customer data, prompts, outputs, files, metadata, logs, or support materials are used to train, fine-tune, test, improve, or evaluate AI models.

Please have the questionnaire completed by someone authorized to speak for the company on legal, privacy, security, compliance, or product policy matters.

We are specifically asking for written confirmation on whether firm/client data is used for AI model training or product improvement; how long each category of data is retained; whether humans employed by your company or third parties may review our data; whether third-party AI model providers or subprocessors process our data; whether AI features can be disabled or limited at the admin level; whether data can be deleted and deletion certified upon request or termination; and whether you will notify us of material changes to AI, privacy, security, retention, or subprocessor terms.

Please include the name, title, department, and email address of the person completing the response and confirm whether our firm may rely on the response for vendor due diligence purposes.

Thank you.

[Name] | [Title] | [Law Firm] | [Phone] | [Email]

Follow-Up Email for Incomplete or Vague Responses

SUBJECT: FOLLOW-UP: WRITTEN VENDOR DUE DILIGENCE RESPONSES NEEDED

> Hello,
>
> Thank you for the response.
>
> For our vendor due diligence file, we need direct written answers to the specific questions in the questionnaire. General links to public materials or statements that your company 'takes security seriously' are not sufficient for our review.
>
> In particular, please provide direct written answers to: (1) Is our firm's data, client data, uploaded content, prompts, outputs, metadata, logs, or support content used to train, fine-tune, test, improve, or evaluate AI models? (2) Are any AI features enabled by default? (3) Can AI features be disabled or limited by an administrator? (4) How long are prompts, outputs, uploaded files, metadata, logs, backups, and deleted data retained? (5) Can our data be deleted and deletion certified upon request or termination? (6) Can vendor personnel or third parties review our data, prompts, outputs, files, logs, or support materials? (7) What subprocessors or third-party AI providers may process our data? (8) Will you notify us of material changes to AI, privacy, retention, security, or subprocessor terms?
>
> Please have someone from legal, privacy, security, compliance, or product policy provide the response, including their name, title, department, email address, and date of response.
>
> Thank you.
>
> [Name] | [Title] | [Law Firm]

Decision Memo Template

Use this for each Tier 3 or Tier 4 vendor. File it in the vendor's evidence folder.

Section	Content
Vendor	[Vendor name and product]
Use case	[What the firm uses it for]
Data involved	[Categories of client and firm data]
AI features	[Enabled / Disabled / Limited, specify]
Key documents reviewed	[Contract, DPA, AI terms, privacy policy, SOC 2, questionnaire. With dates]
Key risks identified	[Training, retention, human review, subprocessors, data location. Be specific]
Safeguards implemented	[MFA enabled, AI disabled, opt-out confirmed, access limits, retention settings. With screenshots on file]
Decision	[Approved / Approved with limits / Not approved]
Limits on use	[No privileged docs, no client names, no financial records, etc.]
Suggested internal policy language	The firm may not enter, upload, transmit, or process client confidential information, privileged communications, client documents, matter materials, financial information, personal information, or other sensitive data in any vendor

	platform or AI-enabled feature unless the vendor has been reviewed and approved under the firm's vendor due diligence process. Approval must be documented in writing.
Approver	[Name, title, date]
Next review date	[Usually annual; every 6–12 months for Tier 4]

Appendix E: 90-Day Vendor Governance Rollout Plan

Firms fail at governance when they try to do everything at once. Start with the highest-risk vendors. Document as you go. Then expand.

Week 1: Build the Inventory and Triage

— Build the complete vendor list. Include every tool that touches client data, not just the AI-specific ones.

— Identify which vendors touch client data. Identify AI features in each.

— Assign a risk tier to every vendor. Flag all Tier 4 and Tier 3 vendors for immediate review.

— Prioritize: the top three to five vendors where client confidential data is most at risk.

Week 2: Send Vendor Requests

— Send the questionnaire to top Tier 4 and Tier 3 vendors using the email templates in Appendix D.

— Save all current contracts, privacy policies, AI terms, and DPAs. Download from the vendor's website with dates.

— Screenshot key admin settings for each priority vendor.

— Set a two-week deadline for vendor responses.

Week 3: Review Responses

— Mark questionnaire responses complete or incomplete. Send follow-up emails where needed.

— Review each response against the Vendor Minimum Standards table.

— Identify red flags. Prepare decision memos for the highest-risk vendors.

— Note any AI features that are enabled by default and require immediate configuration.

Week 4: Decide, Configure, and Train

— Approve, limit, reject, or pause each reviewed vendor. Complete the decision memo for each.

— Disable risky AI features where needed. Enable MFA and SSO. Restrict user permissions.

— Document settings with dated screenshots. File in each vendor's evidence folder.

— Run a 30-minute staff training session. Cover the approved tool list, the data tier rules, and who to ask when a new tool comes up.

— Post the Practical Vendor Rules for Law Firm Staff table where staff can access them.

Weeks 5–8: Expand to Remaining Tier 3 and Tier 4 Vendors

— The managing partner or designated technology lead assigns an owner to every remaining Tier 3 and Tier 4 vendor, sends the questionnaire, and records a response deadline. Start each vendor's evidence file with current contracts, terms, and settings.

— Track missing responses and unresolved red flags weekly. Pause new client-data access for any vendor still awaiting approval under the firm's policy.

Weeks 9–13: Close the Remaining Decisions

— The assigned owner completes the questionnaire and evidence file for each remaining Tier 3 and Tier 4 vendor, documents limits or remediation, and routes a signed decision memo to the designated approver.

— The managing partner checks the inventory against the completed files before Day 90. Escalate vendors that will miss the target, assign interim limits, and record a dated completion plan.

Ongoing: Sustain the Program

- — Re-review Tier 4 vendors every 6–12 months. Re-review Tier 3 vendors annually.
- — Review immediately when a vendor announces major AI, privacy, or security changes.
- — Add vendor review to the onboarding checklist for every new tool.
- — Add an AI-feature review to monthly or quarterly admin check-ins.
- — When a new vendor is proposed, no client data until the vendor review is complete.

WHAT SUCCESS LOOKS LIKE AT DAY 90

Every lawyer and staff member knows which tools are approved and which are not.

Every Tier 3 and Tier 4 vendor has a completed questionnaire, evidence file, and signed decision memo.

Every AI feature that was enabled by default in a priority vendor has been reviewed and either confirmed or disabled.

The firm has a re-review calendar in place. Governance does not stop at Day 90. It becomes routine.

If The Florida Bar asked what the firm did before giving a vendor access to client data, the answer is a file, not a memory.

About Actionable AI

Actionable AI is a solo AI-adoption consultancy for small law firms. Founded by Greg Yates, a former Big Law corporate equity partner at Steptoe (NYC Managing Partner) and Seyfarth Shaw, it exists because most firms have nowhere to turn for honest, practice-area-specific AI guidance. The big consultancies do not know your practice. The vendors are not neutral. The CLEs are too general.

The firm works only with small law firms in Florida. Not tech companies. Not generic small businesses. Law firms. The specificity is the point. Every recommendation, questionnaire, and policy template is tested against actual Florida Bar guidance, actual Florida and federal rules, and the actual workflow of the firms it was written for.

What We Do

— **AI readiness assessments:** where your firm is, where the governance gaps are, and what to fix first.

— **Vendor governance support:** running the audit, reviewing questionnaire responses, drafting decision memos, and building the evidence file.

— **AI governance policy and training:** building the firm-specific policy and delivering the staff training that actually gets used.

— **Ongoing advisory:** as vendor terms, Bar guidance, and AI capabilities change, your governance program changes with them.

Who This Playbook Is For

The managing partner of a small Florida firm who knows AI matters and wants a defensible vendor-governance record, built by someone who has done the work, who respects the obligations, and who does not treat ethics compliance as a feature to be unlocked. If that is you, this playbook is the first step. The conversation about your specific vendor stack is the next one.

READY TO BUILD YOUR VENDOR GOVERNANCE RECORD?

Book a free 15-minute assessment call to discuss (https://actionableai.s.gy/9Ei2uw):

— Which vendors in your stack carry the highest governance risk right now.

— Which AI features in your existing tools are enabled by default and have never been reviewed.

— How to build a governance program your firm can actually maintain.

— Florida-specific ethics guardrails for your practice and your vendor relationships.

No pitch. No deck. No obligation.

actionableai.net · Greg Yates · gyates@actionableai.net

Sources and Ethics Anchors

— ABA Model Rule 1.6, Confidentiality of Information: https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/

— ABA Model Rule 5.3, Responsibilities Regarding Nonlawyer Assistance: https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_5_3_responsibilities_regarding_nonlawyer_assistant/

— ABA Formal Opinion 512, Generative Artificial Intelligence Tools (July 29, 2024): https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba-formal-opinion-512.pdf

— Florida Bar Ethics Opinion 24-1, Lawyers' Use of Generative AI (January 19, 2024): https://www.floridabar.org/etopinions/opinion-24-1/ [official opinion PDF]

— Florida Rules of Professional Conduct: Rules 4-1.1, 4-1.4, 4-1.5, 4-1.6, 4-1.18, 4-3.3, 4-5.1, 4-5.3 [current Chapter 4 rules]

— NIST AI Risk Management Framework: https://www.nist.gov/itl/ai-risk-management-framework

— In re Amendments to Rules Regulating The Florida Bar – Chapter 4, 393 So. 3d 137 (Fla. 2024) (SC2024-0032, decided August 29, 2024, effective October 28, 2024): amending the Comments to Rules 4-1.1, 4-1.6, 4-5.1, and 4-5.3 to address generative artificial intelligence [official opinion PDF]

— Florida Supreme Court Opinion SC2026-0673 (May 28, 2026, eff. June 15, 2026), amending Rule of General Practice and Judicial Administration 2.515(d)(2) for Florida state courts [official opinion PDF]

— Florida Supreme Court Administrative Order AOSC26-12 (May 28, 2026; effective June 15, 2026), barring the covered circuit-level AI disclosure and certification requirements: official order PDF

— Florida Information Protection Act, Fla. Stat. § 501.171 (2026), definitions and breach-notice provisions: official statute

— Capital Standard, LLC v. U.S. Bank National Association, No. 2D2024-1392, 2026 WL 2450571 (Fla. 2d DCA Aug. 21, 2026): referral of counsel to The Florida Bar after 46 fabricated or unsupported citations appeared across two briefs

NOTE

This playbook is a practical risk-management resource, not legal advice. Firms should adapt it to their jurisdiction, clients, vendor contracts, and applicable privacy and security obligations. Have a Florida-licensed attorney review all policy templates, questionnaires, and disclosure language before adoption or use.

Actionable AI

Download the free Florida AI Starter Playbook.

Eight practical resources for managing partners and firm administrators: a readiness checklist, five pilot workflows, a tool-approval scorecard, a lawyer verification checklist, and a 90-day plan. It is free, and the button below downloads it directly.

Scan to download the Starter Playbook

Download the Starter Playbook (PDF)

Direct download: Florida AI Starter Playbook (PDF)

Want a second set of eyes on which workflow to pick?

I take 15-minute calls with managing partners and administrators. I will tell you whether there is a fit. No deck.

Book a 15-minute introductory call

Book a 15-minute introductory call