

FICTIONAL CASE STUDY

AI Exposure Audit Case Study

How a 38-person law firm discovered where AI was already touching its business

Prepared by CAVA Suite LLC

Engagement \$4,500 fixed fee | 1 week

Client profile 10 lawyers | 28 support staff | 38 total personnel

Date September 2026

Use limitation This case study is fictional and illustrative. The organization, interviews, findings, scores, costs, decisions, and outcomes are invented to demonstrate the CAVA Suite LLC AI Exposure Audit methodology. It does not describe an actual client engagement.

Executive case study summary

A 38-person law firm knew employees were experimenting with artificial intelligence, but management could not answer basic questions about which tools were being used, what information was being entered, or whether AI-generated legal work was being reviewed consistently.

A one-week AI Exposure Audit found elevated exposure driven by unmanaged accounts, potentially sensitive information handling, inconsistent verification, and unreviewed AI features inside existing software. The same audit also identified several bounded opportunities that could create value once basic controls were in place.

Audit disposition: Contain and assess

Control current AI use before expanding access or adding connected workflows. The illustrative exposure index was 4.1 of 5, while the opportunity index was 3.8 of 5.

1. The Challenge

AI adoption had occurred organically. Lawyers and staff were using consumer AI services, AI-assisted legal research, meeting transcription, productivity features, and potentially AI capabilities embedded inside document-management and other business software.

Management did not have a reliable inventory of tools, approved account types, vendor AI features, or handling rules. Some users relied on personal, free, or individually paid accounts. Interviews also described matter-related prompts, draft sections, summaries, and case-file extracts being entered into AI systems.

The central problem was not whether the firm should begin using AI. AI was already present in day-to-day work. Management needed visibility before it could govern, expand, or restrict that use.

2. The One-Week Audit

The AI Exposure Audit is a diagnostic engagement. It identifies current use, exposure paths, priority risks, practical opportunities, and the next management actions. It stops before full policy development, technical implementation, procurement, legal conclusions, or production-system validation.

- Anonymous employee survey covering current tools, tasks, account types, data handling, verification, and errors.
- Representative interviews with management, administration, IT, lawyers, and support personnel.
- Review of up to 10 relevant policies and records, including technology, confidentiality, vendor, records, billing, and training materials.
- Screening of current vendor product categories for embedded AI capabilities and unanswered control questions.
- Management workshop to confirm facts, rank priorities, assign owners, and agree on a 30, 60, and 90-day action plan.

Evidence discipline

Material observations are classified as confirmed, self-reported, inferred, or unresolved. Unresolved facts become follow-up actions rather than allegations or conclusions.

3. What the Audit Found

The audit produced a compact scorecard showing both exposure and opportunity. Exposure scores run from 1, controlled, to 5, acute. Opportunity is scored separately because business value does not reduce risk.

Dimension	Score	Level	Immediate implication
Employee AI use	4.0	Elevated	Create a complete register and move firm work to approved accounts.
Data sensitivity exposure	4.5	High	Use confidential follow-up and minimum-necessary handling rules.
Vendor AI exposure	3.5	Elevated	Inventory AI features and obtain retention, training, logging, and change information.
Governance maturity exposure	4.5	High	Assign an interim owner and establish basic controls.
Business opportunity	3.8	Promising	Evaluate bounded opportunities after immediate containment.

Top five immediate risks

Rank	Risk
1	Potential client-information entry into unapproved services
2	Unverified legal content reaching clients, filings, or decisions
3	Unreviewed AI features inside existing vendor products
4	Inconsistent supervision of support-staff AI use
5	No designated AI owner or incident-reporting route

A hidden source of exposure

The audit also showed that AI exposure did not come only from employees opening public chat tools. AI capabilities were appearing inside software the firm already licensed, including legal research, productivity, document management, billing, and meeting applications. That created a second governance problem: ordinary vendor approval did not necessarily answer AI-specific questions about retention, model training, logging, feature changes, or administrative controls.

4. Opportunity After Containment

The engagement was not designed only to identify problems. Five use cases appeared suitable for controlled follow-on evaluation because the tasks could be bounded and outputs could be checked against authoritative sources or established records.

Rank	Opportunity	Potential benefit
1	Approved legal research assistance	Faster issue framing and search development
2	Brief issue and outline support	Faster first outlines and counterargument development
3	Controlled case chronology extraction	Reduce manual event extraction and organization
4	Internal procedure assistant	Reduce repetitive administrative questions
5	Administrative and billing narrative drafting	Improve clarity and reduce editing time

5. The 30, 60, and 90-Day Management Plan

Period	Management action
Days 1 to 10	Appoint an interim AI owner; move firm work to approved accounts; establish a reporting route; require lawyer verification for substantive AI-assisted work; conduct confidential follow-up on potentially sensitive prior use.
Days 11 to 30	Complete the tool, account, extension, integration, and embedded-feature inventory; review priority vendor terms and control settings; brief personnel on permitted use and reporting.
Days 31 to 60	Adopt basic AI-use rules and an intake route; choose up to two opportunities for structured evaluation with a sponsor, baseline, risk screen, and acceptance criteria.
Days 61 to 90	Run bounded pilots if authorized; maintain correction logs and decision dates; determine whether further governance, roadmap, vendor evaluation, or validation work is needed.

6. The Business Value

The most important outcome was management visibility. At the beginning of the week, leadership knew AI was entering the business but could not see the full footprint. At closeout, management had a current-use snapshot, exposure map, vendor exposure list, scorecard, prioritized risk and opportunity registers, and an action plan with owners and completion evidence.

The audit gave leadership a practical basis for answering six questions:

1. Where is AI already being used?
2. What information and business decisions are exposed?
3. Which vendor products already contain AI capabilities?
4. Which activities require immediate control or follow-up?
5. Which use cases are promising enough to evaluate?
6. Who owns each next action, and when should it be complete?

7. The Lesson

For many small and mid-sized organizations, AI adoption is happening from the bottom up. Employees experiment, vendors add new features, and workflows change before management creates a formal AI strategy. Waiting for a strategy does not stop that process.

The first step is visibility. The CAVA Suite AI Exposure Audit is designed to show management where AI already touches the organization, where the largest exposures are, where credible opportunities exist, and what should happen next.

Find where AI is being used. Understand the exposure. Decide what to do next.

The AI Exposure Audit is designed for small and mid-sized organizations that need a fast, bounded view of current AI use before making larger governance, procurement, or implementation decisions.

AI Exposure Audit

One week. Fixed scope. Management-ready findings, priorities, and next actions.

[Schedule an AI Exposure Audit](#) | CAVA Suite LLC

Disclosure

This case study is fictional. Harbor and Pine Law LLP is an invented organization. All personnel counts, interviews, findings, scores, costs, risks, opportunities, management decisions, and outcomes are illustrative examples created to demonstrate the service. The audit does not provide legal, cybersecurity, privacy, compliance, or incident-determination services and does not certify the accuracy, security, compliance, or fitness of any AI system.