

AI Exposure Audit

Find where AI is already being used, what exposure it creates, and what management should do next

AI is often inside a business before leadership has formally approved it. Employees experiment with public AI tools, vendors add AI features to existing software, and generated output begins influencing work without a common set of rules or verification practices.

The CAVA Suite AI Exposure Audit is a one-week, fixed-scope diagnostic for organizations that need visibility before they make larger AI investments or governance decisions.

Best fit	Small and mid-sized organizations, typically 20 to 250 employees, where AI use has begun but management does not have a reliable inventory or control picture.
Engagement	One business week, fixed scope, with preparation completed before Day 1.
Core result	A management-level view of current AI use, exposure, immediate priorities, and practical opportunities.
Typical fee	\$3,500 to \$7,500 for standard SMB scope. Larger or more complex environments are custom scoped.

The Problem It Solves

Most leaders do not need a long AI strategy document as their first step. They need answers to a more immediate set of questions:

- Which AI tools and AI-enabled vendor features are employees already using?
- Are personal, free, or individually purchased accounts being used for company work?
- What company, customer, employee, technical, financial, legal, or other nonpublic information may be entering AI systems?
- Where is AI-generated content influencing decisions, customer communications, analysis, or work product?
- Which vendor features have appeared without an AI-specific review?
- What should management stop, contain, investigate, permit, or evaluate first?

What the Audit Includes

Work area	What CAVA does	Management output
Current-use discovery	Survey and representative interviews to identify tools, accounts, tasks, data, outputs, and review practices.	Current AI use snapshot
Exposure mapping	Map employee-selected tools, uploads, extensions, vendor features, and generated content paths.	AI exposure map
Vendor feature screen	Identify AI capabilities already present in priority software categories and the questions that require follow-up.	Vendor AI exposure list
Evidence analysis	Distinguish confirmed facts, self-reported information, consultant inference, and unresolved questions.	Traceable findings with confidence
Risk and opportunity prioritization	Identify the five most important near-term risks and five practical opportunities.	Priority registers
Action planning	Assign near-term actions, proposed owners, checkpoints, and completion evidence.	30, 60, 90-day action plan

Five-Day Delivery Model

Timing	Focus	Primary output
Before Day 1	Survey, information request, interview schedule, confidentiality instructions	Known-tool list and evidence register
Day 1	Kickoff, sponsor, operations, and IT discovery	Confirmed scope and urgent exposure screen
Day 2	Representative employee and workflow interviews; survey analysis	Use snapshot and unresolved facts
Day 3	Vendor-feature screen, account and data mapping, scoring	Exposure map and draft scorecard
Days 4-5	Management fact check, priority workshop, final report and briefing	Final package, decisions, owners, next actions

What You Receive

- AI Exposure Audit report in editable and presentation-ready form.
- Current-use snapshot and AI exposure map.
- Vendor AI exposure list.
- Five-dimension exposure scorecard and separate business-opportunity indicator.
- Top-five immediate risk register.
- Top-five near-term opportunity register.
- Prioritized 30, 60, and 90-day action plan.
- Executive decision briefing and closeout record.

What the Audit Does Not Do

The audit is deliberately diagnostic. It stops before the larger work begins.

- It does not create a complete AI strategy or enterprise roadmap.
- It does not draft the final policy suite or governance charter.
- It does not provide legal, privacy, cybersecurity, regulatory, or breach determinations.
- It does not perform forensic discovery, penetration testing, or technical configuration.
- It does not complete procurement, implementation, pilot execution, or production validation.
- It is not a compliance certification, security rating, or attestation.

Where It Fits in the CAVA Suite Service Path

1. AI Exposure Audit. Establish visibility, exposure, priorities, and next actions.
2. AI Governance Setup. Build the operating system: roles, policies, intake, vendor review, assurance requirements, and roadmap.
3. AI Validation. Test a selected AI system or workflow against measurable acceptance criteria before production, scale, or continued use.
4. Fractional Chief AI Officer. Operate the program, execute the roadmap, and keep recurring AI decisions moving.

Start with Visibility

If AI is already appearing in employee work or vendor products and management cannot clearly answer where, how, and under what controls, the AI Exposure Audit provides a fast starting point. The objective is not to slow useful AI adoption. It is to give leadership enough evidence to decide what happens next.