Shadow AI risk audit

Thirty-six percent of respondents to our benchmark survey of 3,000 knowledge work professionals[1] said their organizations have already experienced a measurable AI policy violation. Yours may have, too — even if you don't know about it, yet.

See where you stand in mitigating this risk. Below are 10 questions for CIOs, CTOs, and chief risk officers. Take two minutes and check each item that, to your present knowledge, your organization has proactively addressed.

- [ ] We have documented and enforce a policy governing the use of publicly available AI tools (ChatGPT, Claude, Gemini, Copilot, etc.) by all employees.

  Twenty-five percent of organizations allow public AI use with little to no oversight.

- [ ] We have conducted a complete inventory of every AI tool currently in use across all practice groups and departments — including tools IT did not purchase.

  Shadow AI tools are an active operational reality — not a future risk.

- [ ] We have vetted the security and data handling posture of every AI tool in use —including what data is retained, who can access it, and how it is used for model training

  Vendor security assessment is a governance prerequisite, not a post-deployment activity.

- [ ] Client documents, privileged communications, and sensitive or matter-related content cannot be pasted into or processed by any AI tool outside our governed platform without an explicit exception process.

  A single policy violation involving client data can have significant legal and reputational consequences.

- [ ] We maintain audit trails for AI-generated or AI-modified content that would satisfy a regulatory or legal discovery request today.

  Audit trail requirements are present-tense under GDPR, DORA, HIPAA, and emerging AI regulations.

- [ ] A named individual is accountable for AI governance — not a committee, not a shared reasponsibility, but a specific person with defined authority and reporting lines.

  Diffused governance ownership is one of the most common antecedents to policy violations.

- [ ] We have ethical walls and matter or project level confidentiality controls that prevent AI from surfacing documents across client matters where conflicts exist.

  AI operating across an ungoverned DMS can surface confidential content across matter or project boundaries.

- [ ] Our AI usage policy has been communicated to all employees, not just IT and leadership — and we have a mechanism for reporting potential violations.

  Policies that exist only in a governance document are not enforced policies.

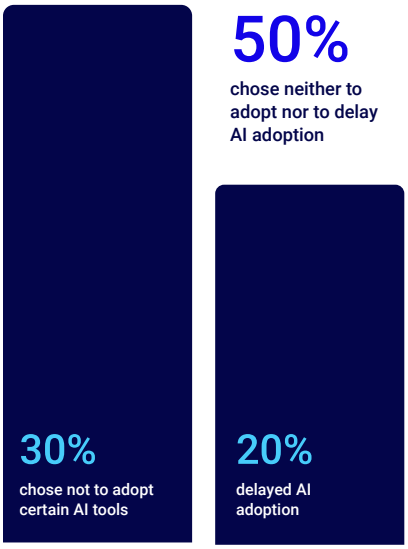
- [ ] We have assessed our exposure under current AI regulations (EU AI Act, DORA, applicable data privacy laws) and can demonstrate compliance if a regulator asks today.

  Regulatory exposure from AI tools is a current, not future, scenario for organizations operating in regulated jurisdictions.

- [ ] If a client asked us today to describe exactly how their data is handled by our AI tools — including what is retained, where it is processed, and who can access it — we could answer accurately and completely within 24 hours.

  Among the most mature organizations, 75% say clients actively shape their AI strategy. Client scrutiny is already here.

Security concern impact on AI adoption



36% of respondents say AI has led to **document policy violation**

25% report publicly available AI usage **with little oversight**

[1]iManage Knowledge Work Benchmark Report 2026: Global findings on AI adoption, governance and business performance. https://imanage.com/benchmark-report-2026/