keep aware

AI tool checklist

AI Tool Security Audit Checklist

How exposed is your organization to AI tool risk?

Most security teams know employees are using AI tools. Few know which ones, with which accounts, and what data is going in. Use this checklist as a point-in-time audit or quarterly review. Tally your score at the end to assess your AI visibility posture.

TOOL DISCOVERY & INVENTORY

1. ☐ **I have real-time visibility into which AI tools employees are actively using**
   Includes ChatGPT, Copilot, Gemini, Claude, Perplexity, Grok, and the growing wave of new AI tools emerging every day.
2. ☐ **I can identify new AI tools as employees begin using them**
   Reactive discovery means risk exposure windows stretch for weeks or months.

ACCOUNT & IDENTITY CONTEXT

3. ☐ **I can differentiate between corporate and personal AI account usage, and which is used for work tasks**
   Personal accounts operate under different data retention and compliance terms than enterprise accounts.
4. ☐ **I can enforce policies that restrict AI usage to corporate-only accounts**
   Visibility without enforcement leaves the risk unaddressed.

DATA EXPOSURE IN AI PROMPTS

5. ☐ **I know what data employees are entering into AI prompts**
   PII, source code, financial data, legal documents, and M&A; details are commonly entered into AI tools without awareness of the risk.
6. ☐ **I have controls to warn or block users before sensitive data is submitted to an AI tool**
   Inline enforcement stops the risk at the point of interaction, not after data has already been processed.
7. ☐ **I can detect when sensitive data categories (PII, uploads, documents) are submitted to an AI tool**
   Without prompt-level visibility, you have no way to know what's leaving the organization through AI inputs.

POLICY & GOVERNANCE

8. ☐ **I have a GenAI Acceptable Use Policy in place**
Employees need clear guidance on which tools are approved and what data may not be shared with AI.

9. ☐ **Our GenAI AUP is actively enforced through technical controls, not just documentation**
Policy without enforcement is not a security control. Browser-native controls can enforce at the point of use.

10. ☐ **I have audit logs that can prove policy adherence for compliance or legal purposes**
Forensic evidence of what employees accessed and submitted to AI tools is increasingly required for compliance.

Add up your total score and assess your AI visibility posture.

Total: _____ 9+ Low risk 5-8 Medium risk 4 or less High risk

Not sure how you'd score in a real audit?

Keep Aware's **free AI Tool Audit** surfaces exactly what this checklist asks about —which tools are active, which accounts are in use, and what data is being shared. Most teams are up and running in under 15 minutes.

Request your free audit at keepaware.com/free-ai-audit