



The Manager Playbook

Find AI Risk in 30 Minutes






Goal

To identify which AI tools are currently in use so the organization can provide official, secure versions and prevent data leakage.

Step 1: The "No-Judgment" Discovery






Employees often hide AI use because they fear being seen as "lazy" or "cheating." Start by removing that barrier.

-  **Run an Anonymous Survey:** Ask: "Which AI tools (ChatGPT, Claude, Canva AI, etc.) have helped you save at least 30 minutes this week?"
-  **Slack/Teams Search:** Search internal channels for keywords like "ChatGPT," "Prompt," or "Generated by AI" to see where conversations are already happening.
-  **Review Browser Extensions:** Ask IT to pull a report on the most common browser extensions. Look for AI-powered grammar checkers, coding assistants, or research tools.

Step 2: Identifying the "High-Risk" Workflows



Audit where the most sensitive data is likely being "pasted" into AI.



-  **The "Code Leak" Check:** Are developers using AI to debug proprietary code?
-  **The "Customer PII" Check:** Is the CS or Sales team using AI to summarize meeting notes or draft emails that contain client names/emails?
-  **The "Financial Data" Check:** Is anyone using AI to analyze spreadsheets or create projections from internal revenue data?



Step 3: The Productivity Audit



Understand why they are using Shadow AI so you can provide a better alternative.

-  **Identify the "Pain Point":** Is the team using AI because an official process is too slow? (e.g., waiting for a copywriter or a data analyst).
-  **Cost Analysis:** Is the team paying for "Pro" accounts on personal credit cards? This is a major red flag for unmanaged data.

Step 4: The Action Plan



-  **Bridge the Gap:** If a tool is highly used and helpful, move it from "Shadow AI" to "Approved AI" by upgrading to an Enterprise/Team version with a Data Processing Agreement (DPA).
-  **Update the "Approved Tools" List:** Share the results of this audit and tell the team: "We see you love [Tool X]. We've secured an official version for everyone—please move your work there."

Manager's Pro-Tip:

When you find Shadow AI, **don't ban it immediately**. If it's providing value, your job is to find a **secure way** to keep that value. Banning a helpful tool without providing an alternative only drives the risk further underground.

Most companies think they have AI under control. Until they test it.

Run a simulation or training to see where your team actually stands.

[Run Simulation](#)

