STACK CYBERSECURITY

AI HUB • DISCOVERY WORKBOOK

Shadow AI Discovery Checklist

A practical guide to identifying unauthorized AI usage across your organization.

> Use this checklist to identify where employees may be using AI tools outside of approved business processes. Complete this assessment before creating an AI policy or implementing technical controls.

ORGANIZATION	DATE COMPLETED
DEPARTMENT	COMPLETED BY
NUMBER OF EMPLOYEES	VERSION

BEFORE YOU BEGIN

How to Use This Checklist

This is a discovery exercise, not an AI policy or a risk assessment. The goal is to answer one question: do we have shadow AI, and where is it hiding? Work through each section in order, involving the people listed below where relevant.

Estimated Time

30 to 60 minutes, depending on organization size and department count.

What This Checklist Helps You Identify

- Unauthorized AI chatbots
- AI meeting assistants
- AI writing tools
- AI coding assistants and AI agents
- AI image and video generators
- Unsanctioned browser extensions
- AI features embedded in business software
- Unapproved AI integrations and OAuth apps

Discovery comes before governance. Most shadow AI use is accidental rather than intentional. Employees generally adopt these tools to work faster, not to bypass security. This checklist is designed to build visibility first, so any policy or control you put in place afterward is grounded in what is actually happening.

Discovery Process

1. Interview employees
2. Inventory AI tools
3. Review technical logs
4. Identify unknown AI
5. Prioritize risk
6. Plan governance

SECTION 1

Employee AI Usage

Answer each question based on what you currently know or can quickly confirm. Mark Unsure rather than guessing; unsure answers point directly to where discovery work is needed.

DEPARTMENT _____ REVIEWED BY _____ DATE _____

QUESTION	YES	NO	UNSURE
Have employees received formal approval before using AI tools?	☐	☐	☐
Do employees know which AI tools are approved?	☐	☐	☐
Are employees using personal AI accounts for work?	☐	☐	☐
Do employees copy company information into AI chatbots?	☐	☐	☐
Do employees upload spreadsheets into AI tools?	☐	☐	☐
Do employees upload customer information into AI tools?	☐	☐	☐
Do employees upload contracts into AI tools?	☐	☐	☐
Do employees upload source code into AI tools?	☐	☐	☐
Do employees use AI to summarize meetings?	☐	☐	☐
Do employees use AI to write emails?	☐	☐	☐
Do employees use AI to build presentations?	☐	☐	☐
Do employees use AI to draft reports?	☐	☐	☐
Do employees use AI to generate images or video?	☐	☐	☐
Do employees use AI to analyze data?	☐	☐	☐
Do employees use AI agents or autonomous workflows?	☐	☐	☐

SECTION 2

AI Platform Inventory — Core Tools

Work through this list with IT and each department. Check every tool currently found in use, note whether it is approved, and flag anything that still needs a vendor security review.

GENERAL AI ASSISTANTS

PLATFORM	FOUND	APPROVED	VENDOR REVIEWED	REMOVE
ChatGPT	☐	☐	☐	☐
Claude	☐	☐	☐	☐
Microsoft Copilot	☐	☐	☐	☐
Gemini	☐	☐	☐	☐
Perplexity	☐	☐	☐	☐
Grok	☐	☐	☐	☐
Meta AI	☐	☐	☐	☐
Mistral (Le Chat)	☐	☐	☐	☐
DeepSeek	☐	☐	☐	☐
Poe	☐	☐	☐	☐
Character.AI	☐	☐	☐	☐

MEETING ASSISTANTS

PLATFORM	FOUND	APPROVED	VENDOR REVIEWED	REMOVE
Fireflies.ai	☐	☐	☐	☐
Otter.ai	☐	☐	☐	☐
Fathom	☐	☐	☐	☐
MeetGeek	☐	☐	☐	☐
Zoom AI Companion	☐	☐	☐	☐
Microsoft Teams Copilot	☐	☐	☐	☐

WRITING & PRODUCTIVITY

PLATFORM	FOUND	APPROVED	VENDOR REVIEWED	REMOVE
Grammarly	☐	☐	☐	☐
Notion AI	☐	☐	☐	☐
Canva AI	☐	☐	☐	☐
Adobe Firefly	☐	☐	☐	☐
Gamma	☐	☐	☐	☐
Beautiful.ai	☐	☐	☐	☐

SECTION 2, CONTINUED

Emerging & Specialized Tools

These tools are newer or more specialized, but adoption is rising quickly. Many employees pick these up independently for content creation or development work.

CONTENT CREATION: AUDIO, VIDEO & DESIGN

PLATFORM	FOUND	APPROVED	VENDOR REVIEWED	REMOVE
ElevenLabs	☐	☐	☐	☐
Synthesia	☐	☐	☐	☐
VEED	☐	☐	☐	☐
Descript	☐	☐	☐	☐
Runway	☐	☐	☐	☐
Midjourney	☐	☐	☐	☐

CODING & AI AGENTS

PLATFORM	FOUND	APPROVED	VENDOR REVIEWED	REMOVE
GitHub Copilot	☐	☐	☐	☐
Cursor	☐	☐	☐	☐
Windsurf	☐	☐	☐	☐
Replit AI	☐	☐	☐	☐
Bolt.new	☐	☐	☐	☐
Lovable	☐	☐	☐	☐

RESEARCH

PLATFORM	FOUND	APPROVED	VENDOR REVIEWED	REMOVE
NotebookLM	☐	☐	☐	☐
Other: _____	☐	☐	☐	☐
Other: _____	☐	☐	☐	☐

> Need more detail on any single tool? Download the **AI Tool Inventory Template** from the STACK AI Hub for a deeper, tool-by-tool vendor and data-handling review.

SECTION 3

Data Being Shared With AI

For each data type, mark how often it is entered into AI tools based on what you learn from interviews and technical review. This section often surfaces the highest-priority findings.

DATA TYPE	NEVER	SOMETIMES	FREQUENTLY
Customer names and information	☐	☐	☐
Employee information	☐	☐	☐
Financial reports	☐	☐	☐
Contracts	☐	☐	☐
Source code	☐	☐	☐
Healthcare information	☐	☐	☐
Personally identifiable information	☐	☐	☐
Controlled Unclassified Information (CUI)	☐	☐	☐
Passwords or API keys	☐	☐	☐
Internal procedures and documentation	☐	☐	☐
Marketing plans	☐	☐	☐
Sales proposals	☐	☐	☐

Any item marked Frequently for regulated or sensitive data warrants immediate follow-up. This includes healthcare information, CUI, financial data, and anything covered by a client contract or compliance framework.

SECTION 4

AI Meeting Assistant Audit

Meeting assistants often introduce risk quietly, since they can join calls automatically and retain recordings or transcripts without a clear review process.

- ☐ AI meeting assistants automatically join meetings
- ☐ Meetings contain customer information
- ☐ Meetings discuss financial information
- ☐ Meetings discuss legal matters
- ☐ Meetings discuss HR issues
- ☐ Meetings discuss intellectual property
- ☐ Meeting recordings are retained indefinitely
- ☐ Employees understand where recordings are stored
- ☐ Meeting transcripts are reviewed before distribution
- ☐ External meetings are recorded by an AI assistant
- ☐ The meeting assistant vendor has been security reviewed
- ☐ Meeting assistants have been approved by IT

SECTION 5

Browser & Device Review

Walk through one representative workstation per department and record what is actually installed, including browser extensions that are easy to overlook.

EXTENSION OR APPLICATION	FOUND	APPROVED	REMOVE
ChatGPT desktop or extension	☐	☐	☐
Claude desktop or extension	☐	☐	☐
Grammarly extension	☐	☐	☐
AI search extensions	☐	☐	☐
AI sidebar extensions	☐	☐	☐
AI translation tools	☐	☐	☐
AI coding extensions	☐	☐	☐
AI screenshot or OCR tools	☐	☐	☐
AI email assistants	☐	☐	☐
AI PDF reader or summarizer	☐	☐	☐
Local AI applications	☐	☐	☐
Other: _____	☐	☐	☐

SECTION 6

Existing Software Review

Many AI features are already built into software your organization uses today. Confirm what is enabled and whether it has been formally approved.

APPLICATION	AI FEATURE	ENABLED	APPROVED
Microsoft 365	Copilot	☐	☐
Microsoft Word	Copilot	☐	☐
Microsoft Excel	Copilot	☐	☐
Microsoft PowerPoint	Copilot	☐	☐
Microsoft Teams	Copilot	☐	☐
Microsoft Edge	Copilot	☐	☐
Microsoft Fabric	Copilot	☐	☐
Power BI	Copilot	☐	☐
Google Workspace	Gemini	☐	☐
Google Chrome	Gemini	☐	☐
Zoom	AI Companion	☐	☐
Slack	AI features	☐	☐
Dropbox	Dash	☐	☐
Atlassian	Rovo	☐	☐
Adobe Acrobat	AI Assistant	☐	☐
Canva	Magic Studio	☐	☐
Adobe	Firefly	☐	☐
Salesforce	Einstein AI	☐	☐
Notion	Notion AI	☐	☐
HubSpot	Breeze AI	☐	☐
Other: _____	_____	☐	☐

SECTION 6, CONTINUED

Department Interviews

Confirm findings directly with each department. A short conversation often surfaces tools that never show up in a technical scan.

DEPARTMENT	INTERVIEWED	AI FOUND	FOLLOW-UP	MANAGER
Executive Team	☐	☐	☐	
HR	☐	☐	☐	
Finance	☐	☐	☐	
Marketing	☐	☐	☐	
Sales	☐	☐	☐	
Operations	☐	☐	☐	
IT	☐	☐	☐	
Engineering	☐	☐	☐	
Legal	☐	☐	☐	
Customer Service	☐	☐	☐	

SECTION 7

Technical Discovery

Work with your internal IT team or managed provider to confirm each item below. This is where quiet or unapproved AI usage is most reliably surfaced.

LOGS & SYSTEM REVIEW

- [ ] DNS logs reviewed
- [ ] Firewall logs reviewed
- [ ] Web proxy reviewed
- [ ] CASB enabled and reviewed
- [ ] CASB discoveries documented
- [ ] Microsoft Defender reviewed
- [ ] Microsoft Purview reviewed
- [ ] Browser history sampled
- [ ] Browser sync settings reviewed
- [ ] Endpoint software inventory completed
- [ ] AI mobile applications reviewed

ACCESS & ACCOUNT REVIEW

- [ ] SaaS inventory completed
- [ ] Shadow SaaS inventory completed
- [ ] Browser extensions inventoried
- [ ] OAuth applications reviewed
- [ ] OAuth grants audited
- [ ] API tokens reviewed
- [ ] SSO applications reviewed
- [ ] Microsoft Entra reviewed
- [ ] Google Admin console reviewed
- [ ] Personal Microsoft accounts identified
- [ ] Personal Google accounts identified
- [ ] Unknown AI domains identified

REVIEWED BY _____ DATE COMPLETED _____

SECTION 8

Risk Scoring

Score each factor using your findings from Sections 1 through 7, then add the points to reach an overall score. This is a directional tool to help prioritize next steps, not a formal risk assessment.

FACTOR	1 POINT	3 POINTS	5 POINTS
Unknown AI tools discovered	☐ 0 to 5	☐ 6 to 15	☐ 16+
Meeting assistants in use	☐ None	☐ Some	☐ Many
Sensitive data uploaded to AI	☐ Never	☐ Sometimes	☐ Frequently
Unreviewed vendors	☐ Few	☐ Some	☐ Many
Unapproved browser extensions	☐ Low	☐ Medium	☐ High

Total Score (max 25) _____ / 25

Risk Level Reference

SCORE RANGE	RISK LEVEL	RECOMMENDED RESPONSE
0 to 10	Low Risk	Continue monitoring on a regular cadence
11 to 20	Moderate Risk	Review vendors and build formal AI governance
21 to 25	High Risk	Conduct a formal AI risk assessment and review technical controls

Recommended Next Steps

- ☐ Create an AI Acceptable Use Policy
- ☐ Complete a full inventory of AI tools
- ☐ Review vendor security postures
- ☐ Enable ongoing AI usage monitoring
- ☐ Train employees on approved AI use
- ☐ Review data retention practices
- ☐ Block unapproved AI where appropriate
- ☐ Implement a formal AI approval process

OPTIONAL WORKSHEET

Executive Summary

A one-page takeaway for leadership. Complete this after finishing Sections 1 through 8 to summarize findings without requiring anyone to read the full workbook.

OVERALL AI RISK SCORE _____ / 25	OVERALL RISK LEVEL ☐ Low ☐ Moderate ☐ High
DEPARTMENTS REVIEWED _____	TOTAL AI TOOLS FOUND _____
APPROVED TOOLS _____	UNKNOWN TOOLS _____
HIGH-RISK FINDINGS	

Immediate Actions

PRIORITY	ACTION	OWNER
1		
2		
3		

PREPARED BY _____ DATE _____

SUMMARY

FINAL STEP

Action Plan

Turn your findings into next steps. List each priority, who owns it, and when it is due.

PRIORITY	ACTION	OWNER	DUE DATE
1			
2			
3			
4			
5			

Next Review Date _____

Once this discovery exercise is complete, STACK Cybersecurity can help translate the findings into an AI Acceptable Use Policy, a formal AI inventory, and a vendor security review process. Visit the AI Hub at stackcyber.com/ai-hub for related governance resources, or reach out to schedule time with our team.

ACTION PLAN