GUIDE

Shadow AI Risk Assessment Checklist

Help your organization identify and govern unauthorized AI deployments. A practical checklist for CISOs, compliance leaders, and security teams.

For CISOs, Compliance Leaders, IT Security Teams
March 2026 | v2.0

73%	3-5x	82:1	$4.5M
Shadow AI Incidents	More AI Than IT Sees	Agent-to-Human Ratio	Avg. Breach Cost

OVERVIEW

Table of Contents

EXECUTIVE SUMMARY

The Shadow AI Problem

Shadow AI is enterprise AI that exists outside approved governance channels. It's the #1 blind spot in enterprise governance today. While executives invest in enterprise AI programs, teams deploy unauthorized assistants, tools, and services—often with direct access to sensitive data and systems. Enterprise AI adoption has outpaced governance by 3-5x. This gap creates risk: data exfiltration, IP leakage, compliance violations, and audit failures. This checklist helps you quantify your exposure in 5 categories and provides a remediation roadmap.

What You'll Find in This Guide:

> *A scored 0-100 risk assessment across AI Tool Inventory, Access Governance, Data Protection, Cost Visibility, and Audit Trail. Each category scored 0-20. A remediation framework mapping scores to specific next steps.*

LANDSCAPE

What Shadow AI Looks Like

- ✓ Unauthorized AI coding assistants (ChatGPT, Claude, GitHub Copilot used on corporate work)
- ✓ Unmanaged API keys and credentials stored in code repos and configuration files
- ✓ Direct LLM access that bypasses enterprise governance and approval workflows
- ✓ Personal AI accounts used for work data—contractors, partners, consultants
- ✓ Unregistered MCP servers connecting external services to AI agents

Primary Risk Categories

01 Data Exfiltration

Sensitive data exposed to external LLM providers without consent

02 IP Leakage

Proprietary code and internal strategies exposed in training data

03 Compliance Violations

Personal data processed outside regulated channels

04 Cost Overruns

Untracked spend on multiple AI subscriptions across the org

05 Audit Gaps

No evidence trail for regulatory, compliance, or security reviews

ASSESSMENT

Risk Assessment Scoring

Score your organization across 5 categories. Each category is 0-20 points. Total score 0-100 indicates your governance posture. Use this assessment to identify gaps and prioritize remediation.

1. AI Tool Inventory (0-20)

- ✓ Do you have a complete inventory of all AI tools in use?
- ✓ Can you identify which teams use which AI tools?
- ✓ Do you know where data is going when teams use personal AI accounts?

2. Access Governance (0-20)

- ✓ Are all AI tools provisioned through approved channels?
- ✓ Do you have approval workflows for new AI tool adoption?
- ✓ Can you prevent unauthorized tools from being used on corporate networks?

3. Data Protection (0-20)

- ✓ Is sensitive data protected from exposure to external AI models?
- ✓ Do you classify data before it reaches AI systems?
- ✓ Can you audit what data was sent to each AI tool?

4. Cost Visibility (0-20)

- ✓ Do you know total AI spend across the organization?
- ✓ Can you break down cost by team, tool, and use case?
- ✓ Do you have token-level visibility into model usage?

5. Audit Trail (0-20)

- ✓ Can you produce evidence of every AI interaction for compliance review?
- ✓ Do you have logs showing who accessed which AI tools and when?
- ✓ Can you trace sensitive data flow through AI systems?

Your Score

Score Range	Governance Level	Interpretation
80-100	Governed	Strong controls; continue monitoring & optimization
60-79	Gaps Identified	Significant controls; prioritize identified gaps
40-59	Significant Risk	Major controls missing; urgent remediation needed
0-39	Critical Exposure	Minimal controls; shadow AI poses organizational risk

REMEDIATION

Fix the Gaps

Use your assessment score to target your remediation roadmap. Organizations using Reign achieve full AI visibility in an average of 8 weeks. Below are the key priorities for each risk level.

Critical Exposure (0-39)

- ✓ Conduct immediate shadow AI audit across all endpoints and accounts
- ✓ Deploy endpoint detection to identify unauthorized tool usage
- ✓ Lock down API access and require approval for external integrations

Significant Risk (40-59)

- ✓ Implement approved AI tool catalog with procurement workflows
- ✓ Enable data classification and prevent sensitive data flows
- ✓ Deploy guardrails for all AI-adjacent systems

Gaps Identified (60-79)

- ✓ Strengthen cost attribution and chargeback models
- ✓ Expand audit trails to token-level visibility
- ✓ Establish governance committee to review AI tool adoption

> *Organizations using Reign achieve full AI visibility in an average of 8 weeks. The platform provides complete audit trails, governance automation, and cost transparency—built for enterprise.*

NEXT STEPS

Start Governing AI Today

Take the next step toward governed AI. Every day without visibility is another day of unaudited AI actions and blind spend.

01 **Assess (24 hours)**

Get a free governance assessment with AI adoption metrics

02 **Plan (1-2 weeks)**

Custom remediation roadmap with cost, timeline, and ROI

03 **Govern (8 weeks)**

Deploy Reign with full audit trails and cost visibility

Included with Reign

- ✓ Full audit trail of every AI agent action
- ✓ MCP connection governance and approval workflows
- ✓ Real-time cost dashboards with token-level visibility
- ✓ 24/7 enterprise support with dedicated TAM

Schedule a demo: itmethods.com

Join 100s of enterprises building with the Fortress Family | AI-Native backed by 21+ Years Enterprise Trust