

10 Signs Shadow AI May Already Exist in Your Organization

- 1 Employees use public AI tools to summarize emails, documents, contracts, or customer communications.
- 2 Teams have adopted AI-powered note-takers or meeting assistants without IT review.
- 3 Staff are uploading spreadsheets, reports, or operational data into AI tools to accelerate analysis.
- 4 Multiple departments use different AI tools for similar purposes.
- 5 Employees regularly use browser extensions that leverage AI functionality.
- 6 AI-generated content appears in proposals, marketing materials, or reports, but no formal AI policy exists.
- 7 Managers cannot confidently list all AI tools being used by their teams.
- 8 There is no approval process for evaluating new AI applications.
- 9 Sensitive business information is shared through consumer-grade cloud services.
- 10 Employees believe AI use is "personal productivity" rather than a technology decision that impacts the organization.

Scoring

0-3 Checks: Low Risk

4-6 Checks: Moderate Risk

7-10 Checks: High Risk

The higher the score, the more likely AI adoption is happening outside organizational visibility and governance.

Practical Governance Measures

Establish an AI Use Policy:

Define what tools are approved, what data can be shared, and acceptable use expectations.

Train Continuously:

Regular education helps employees recognize risks before they become incidents.

Provide Approved Alternatives:

When employees have trusted solutions, they are less likely to seek workarounds.

Classify Your Data:

Ensure employees know the difference between public, internal, confidential, regulated, and customer data.

Monitor Adoption:

Understand which tools are being used, who is using them, and where sensitive data may be flowing.

Create a Simple Approval Process:

Employees should have an easy way to request and evaluate new AI tools.