Shadow AI Risk Assessment Checklist

aona.ai

Aona's free interactive Shadow AI risk assessment scores your exposure from 0 to 100. This checklist turns the same dimensions into audit questions you can work through with IT, security and compliance. Your organisation's size and industry set the context; the six areas below are the ones you can actually change.

1 Visibility and discovery

- [ ] **Inventory every AI tool in use**
  Can you produce a list of every AI tool employees have used in the last 30 days, including free browser-based tools?
- [ ] **Move beyond surveys**
  Is your visibility based on real usage telemetry rather than self-reporting or an annual questionnaire?
- [ ] **Map the data flows**
  Do you know which AI tools receive company data via typed prompts, copy-paste or file uploads?

2 Policy and acceptable use

- [ ] **Publish a written AI policy**
  Is an AI acceptable-use policy written, communicated and acknowledged by every employee?
- [ ] **Name approved tools and banned data**
  Does the policy list approved tools, prohibited data categories and an approval path for new tools?
- [ ] **Enforce it technically**
  Is the policy backed by controls at the point of use, rather than relying on trust alone?

3 Controls at the point of use

- [ ] **Block sensitive data in real time**
  Can you stop PII, client data, credentials or source code before it reaches an AI tool?
- [ ] **Redact instead of banning**
  Can you redact sensitive fields so employees keep the productivity without the exposure?
- [ ] **Cover files, not just prompts**
  Do your controls inspect file uploads as well as typed text?

4 Sanctioned AI adoption

- [ ] **Offer approved alternatives**
  Have you sanctioned enterprise-grade options for the ChatGPT, Copilot, Gemini and Claude use cases employees already have?
- [ ] **Retire consumer accounts**
  Are enterprise tiers, with training-data opt-outs, SSO and data residency, replacing personal accounts?
- [ ] **Make approval fast**
  Is there a well-known, fast route to request a new AI tool so employees do not route around IT?

5 Incident readiness

- [ ] **Have a response plan**
  Is there a documented plan for an AI-related data exposure, with named owners and timelines?
- [ ] **Test your detection**
  Would your monitoring actually flag sensitive data pasted into an unsanctioned AI tool today?
- [ ] **Learn from near-misses**
  Are past AI incidents and near-misses reviewed for root cause and fed back into controls?

6 Device and identity foundations

- [ ] **Enrol devices**
  Are endpoints under MDM or Intune so AI controls can be deployed and enforced at scale?
- [ ] **Centralise identity**
  Is access to sanctioned AI tools governed through SSO, with Entra or a similar identity provider?
- [ ] **Account for unmanaged devices**
  Do you know how much AI usage happens on BYOD and unmanaged devices, and is it in scope?

Score your exposure interactively: aona.ai/tools/shadow-ai-risk-assessment
Free, 2 minutes, no email required. 0 to 100 score with tailored recommendations.