AI Security Readiness Checklist

Use this checklist to evaluate your organisation's readiness for safe and responsible AI adoption.

Check each item currently in place.

AI Security Readiness Assessment

☐ 1. We have identified approved AI tools for employee use.

☐ 2. Employees understand what information should never be entered into AI systems.

☐ 3. We prohibit employees from entering passwords or credentials into AI tools.

☐ 4. Customer data handling rules apply to AI usage.

☐ 5. We maintain an internal AI usage policy.

☐ 6. Employees understand the risks of shadow AI usage.

☐ 7. We provide employee awareness training covering AI-related cybersecurity threats.

☐ 8. AI-generated content is reviewed before external distribution.

☐ 9. Employees understand AI hallucinations and misinformation risks.

☐ 10. We have procedures for verifying sensitive or unusual requests.

☐ 11. We review AI vendors before approving business use.

☐ 12. We understand how approved AI platforms process and store data.

☐ 13. Employees know how to report suspicious AI-related activity.

☐ 14. Remote employees receive AI security awareness guidance.

☐ 15. Managers reinforce responsible AI usage expectations consistently.

☐ 16. Multi-factor authentication is enabled across critical systems.

☐ 17. Sensitive legal, HR, financial, and customer data is restricted appropriately.

☐ 18. Employees understand phishing, impersonation, and deepfake risks.

☐ 19. AI usage expectations are communicated clearly in practical language.

☐ 20. We regularly review and update AI governance procedures.

☐ 21. Employees understand when human review is required.

☐ 22. Approved AI tools are monitored and governed operationally.

☐ 23. Vendor risk and privacy considerations are included in AI evaluations.

☐ 24. Verification culture is encouraged across departments.

☐ 25. Leadership treats AI governance as an ongoing operational responsibility.

Scoring Guide

Strong Maturity

20–25 checked items

Your organisation demonstrates strong readiness for responsible AI adoption.

You likely have:

- effective governance,
- operational visibility,
- employee awareness,
- and leadership engagement supporting safe AI usage.

Continue focusing on:

- policy refinement,
- awareness updates,
- vendor oversight,
- and evolving operational safeguards.

Moderate Exposure

12–19 checked items

Your organisation has meaningful awareness of AI-related risk, but important governance gaps remain.

You may need stronger:

- employee training,
- verification procedures,
- operational oversight,
- or vendor governance.

Improving consistency and visibility should become a near-term priority.

High Vulnerability

0–11 checked items

Your organisation may face significant exposure from uncontrolled or unsafe AI usage.

Employees may currently use AI tools without:

- sufficient oversight,
- practical guidance,
- or operational safeguards.

Immediate improvement is recommended in:

- governance,
- employee awareness,
- sensitive data handling,

and AI-related cybersecurity readiness.