AI Cybersecurity Readiness Assessment Checklist

Use this checklist to evaluate your organisation's readiness for AI-powered cybersecurity risks and opportunities.

Check each item that is currently in place.

AI Cybersecurity Readiness Checklist

☐ 1. We have identified our most critical systems, data, and business processes.

☐ 2. We understand which cyber incidents would create the greatest operational disruption.

☐ 3. We have visibility across endpoints, cloud platforms, email systems, and identity systems.

☐ 4. We use multi-factor authentication for all critical business accounts.

☐ 5. We monitor suspicious login activity and abnormal user behaviour.

☐ 6. We have reviewed whether AI-powered detection tools could reduce alert fatigue.

☐ 7. We have a documented incident response plan.

☐ 8. Our incident response plan includes account compromise, ransomware, phishing, and business email compromise scenarios.

☐ 9. Employees are trained to recognize AI-generated phishing and social engineering attempts.

☐ 10. Employees know how to report suspicious messages or unusual activity.

☐ 11. We have verification procedures for payment changes, vendor updates, and executive approvals.

☐ 12. We restrict privileged access to only those who genuinely need it.

☐ 13. We regularly review user permissions and remove unnecessary access.

☐ 14. We have a process for prioritizing vulnerabilities based on business risk.

☐ 15. We understand which vendors process or access sensitive business data.

☐ 16. We evaluate vendor cybersecurity practices before adopting new AI-enabled tools.

☐ 17. We have a written policy for employee use of AI tools.

☐ 18. Employees are prohibited from entering confidential or sensitive data into unapproved AI platforms.

☐ 19. Security alerts are prioritized based on risk, not simply volume.

☐ 20. Automated security actions are reviewed and governed by human oversight.

☐ 21. Leadership receives regular cybersecurity risk updates in business language.

☐ 22. Cybersecurity investments are aligned with business continuity priorities.

☐ 23. We test our incident response process through tabletop exercises or simulations.

☐ 24. We regularly review and update cybersecurity awareness training.

☐ 25. We treat cybersecurity as an ongoing resilience program, not a one-time technology purchase.

Scoring Guide

Strong Maturity

20–25 checked items

Your organisation demonstrates strong readiness for AI-powered cybersecurity challenges. You likely have solid visibility, leadership awareness, identity controls, employee training, and incident response discipline.

Your next step should be continuous improvement:

- refine automation,
- test incident response,
- review vendor risk,
- and strengthen AI governance.

Moderate Exposure

12–19 checked items

Your organisation has meaningful cybersecurity foundations, but important gaps remain.

You may have some technical controls in place, but readiness may be uneven across:

- employee awareness,
- incident response,
- AI governance,
- identity protection,
- or vendor oversight.

Your next step should be prioritizing the highest-risk gaps and improving operational consistency.

High Vulnerability

0–11 checked items

Your organisation may be significantly exposed to modern AI-enhanced cyber threats.

This does not mean a serious incident is inevitable, but it does indicate that current defences may be too limited, reactive, or inconsistent.

Your next step should be immediate improvement in:

- identity protection,
- employee awareness,
- incident response planning,
- security visibility,

and executive-level cyber risk understanding.