
# Prompt Engineering Readiness Checklist

Use this checklist to evaluate your organisation's readiness for responsible AI-assisted operations and secure prompt engineering practices.

Check each item currently in place.

## Prompt Engineering and AI Governance Assessment

☐ 1. We maintain approved AI tools for business use.

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

☐ 3. We prohibit entering credentials and sensitive operational data into AI tools.

☐ 4. AI-generated outputs are reviewed before operational use.

☐ 5. Employees understand AI hallucination risks.

☐ 6. We maintain governance standards for AI-assisted workflows.

☐ 7. Employees receive practical AI awareness training.

☐ 8. Prompt engineering practices are standardised where appropriate.

☐ 9. Human oversight remains required for sensitive operational decisions.

☐ 10. AI-generated communication is reviewed before external distribution.

☐ 11. Employees understand shadow AI risks.

☐ 12. We maintain visibility into AI-assisted operational workflows.

☐ 13. Technical teams verify AI-generated troubleshooting guidance before implementation.

☐ 14. Sensitive customer and financial information is restricted appropriately.

☐ 15. Managers reinforce responsible AI usage expectations consistently.

☐ 16. Employees understand prompt injection and manipulation risks.

☐ 17. AI usage aligns with cybersecurity and compliance requirements.

☐ 18. Operational accountability remains clearly defined despite AI assistance.

☐ 19. AI workflow usage is monitored and governed operationally.

☐ 20. Employees understand verification expectations for AI-generated analysis.

☐ 21. We review AI vendors and platforms before approval.

☐ 22. Prompt templates improve workflow consistency across teams.

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

☐ 24. Employees know how to escalate AI-related concerns or suspicious activity.

☐ 25. AI adoption supports operational resilience rather than weakening oversight.

---

# Scoring Guide

## Strong Maturity

**20–25 checked items**

Your organisation demonstrates strong readiness for responsible AI-assisted operations and prompt governance.

You likely maintain:

- effective oversight,
- operational visibility,
- employee awareness,
- and strong verification culture.

Continue strengthening:

- governance refinement,
- cybersecurity monitoring,
- workflow consistency,
- and ongoing employee education.

## Moderate Exposure

**12–19 checked items**

Your organisation has implemented some AI governance and prompt engineering safeguards, but important gaps remain.

You may benefit from stronger:

- visibility,
- employee guidance,
- workflow governance,
- and operational oversight.

Improving consistency and verification culture should become near-term priorities.

# High Vulnerability

**0–11 checked items**

Your organisation may face significant operational and cybersecurity exposure from poorly governed AI usage.

Employees may currently use AI systems without:

- sufficient oversight,
- governance,
- awareness,
- or operational safeguards.

Immediate improvement is recommended involving:

- AI governance,
- employee training,
- prompt standards,
- verification culture,

and operational accountability.