



The 2026 Enterprise AI Governance Checklist

A Guide for Australian
Business Leaders to
Deploy Secure,
Scalable AI.

With AI now outranking inflation as the top boardroom concern, the question is no longer if you should implement AI, but how to do it without compromising your organisation's intellectual property or security. Use this checklist to audit your current AI strategy or vet new solutions.

Access Control & Permissions

AI shouldn't give everyone access to everything.

- ☐ Identity Integration: Does the AI integrate with your existing Identity Provider (e.g., Microsoft Entra ID)?
- ☐ Permission Mirroring: Does the AI respect existing file permissions? (e.g., A junior staff member should not be able to "ask" the AI about executive salary spreadsheets).
- ☐ Audit Logs: Does the system maintain logs of user queries & AI responses for compliance auditing?

Data Sovereignty & Security

The #1 risk in AI implementation is "data leakage" into public models.

- ☐ Private Environment: Is the AI deployed within your own cloud tenancy (e.g., Microsoft Azure), or is your data being sent to a third-party server?
Model Training: Is your data being used to train the provider's public models? (It should not be).
- ☐ Data Residency: Is your data stored and processed in Australian data centres to meet local compliance requirements?
- ☐ Encryption: Is data encrypted both at rest and in transit?
- ☐

Contact Us Today
☎ +61 2 8275 8811

📍 antares.solutions
✉ info@antaresolutions.com.au



Part of the
CLOUD
collective

Accuracy & Risk Mitigation



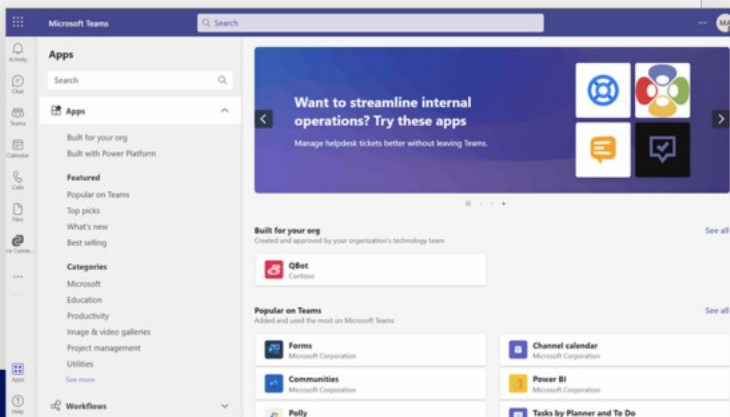
"Hallucinations" can lead to costly business errors.

- ☐ Grounded Responses: Does the AI use "Retrieval-Augmented Generation" (RAG) to answer only based on your specific company documents?
- Source Citation: Does the AI provide links or references to the source documents for every answer it generates?
- Human-in-the-loop: Are there clear protocols for when a human must verify an AI-generated output?

Strategic Alignment & ROI

AI is only useful if it solves a specific business problem.

- ☐ Defined Personas: Have you identified specific "personas" (HR, Sales, IT) where AI can save at least 5+ hours per week?
- ☐ User Adoption: Is the AI accessible within tools the team already uses (like Microsoft Teams or part of your Intranet) to avoid "app fatigue"?
- Scalability: Can the solution scale from a small pilot group to the whole organisation without a complete infrastructure rebuild?



The Verdict:

Is your organisation ready?

If you couldn't tick every box above, your current AI path may be exposing you to unnecessary risk.

How QBot Solves This:

At Antares Solutions, we built QBot to be "Private-by-Design." It sits inside your Azure tenancy, respects your Microsoft 365 permissions, and ensures your data never leaves your organisation.

antares*

**Ready to move
from anxiety to
action?**

**Book a 15-minute
QBot Security Briefing**

Contact Us Today

 +61 2 8275 8811

 antares.solutions

 info@antaresolutions.com.au



Part of the
CLOUD
collective