

AI and IG Governance Checklist

Governance and Accountability

- ☐ Clear Accountability: Roles and responsibilities are formally assigned across the AI lifecycle, including design, procurement, deployment, monitoring, and decommissioning.
- ☐ Governance Oversight: The AI Governance Committee or Governing Authority/Board receives regular assurance reports and maintains visibility of system performance and compliance.
- ☐ Escalation and Decision-Making: Defined escalation pathways exist for issues such as data breaches, ethical concerns, or model drift.

Notes:

Policy, Standards, and Documentation

- ☐ AI Policy Alignment: The AI Policy aligns with NAIC 2025 Guidance, Australian Privacy Principles, and AS ISO/IEC 42001 and 5338 standards.
- ☐ Supporting Standards: Procedures exist for risk management, privacy, data governance, cybersecurity and model assurance.
- ☐ Comprehensive Documentation: Policies, approvals, model testing results, and audit findings are recorded and accessible for verification.

Notes:

Risk and Impact Assessment

- ☐ Privacy Impact Assessment (PIA): Completed before system procurement or design, updated at key milestones.
- ☐ Ethical and Records Impact Assessment: Identifies fairness, bias, explainability, and records-management risks.
- ☐ Legal and Regulatory Compliance: Reviews obligations under the Privacy Act 1988 (Cth)/applicable state privacy legislation, Cybersecurity, Competition and Consumer Act 2010, WHS obligations, and other relevant sectoral laws.

Notes:

Data Governance

☐ Data Catalogue and Classification: All datasets are documented, classified by sensitivity, and linked to purpose and lawful basis for processing.

☐ Data Minimisation and Quality: Only necessary data is collected and maintained; quality and accuracy controls are in place.

☐ Retention and Disposal: Data is managed under approved retention and disposal authorities consistent with records legislation.

☐ Data Provenance and Lineage: Sources, transformations, and uses of data are recorded and traceable throughout the lifecycle.

☐ Security Controls: Data is protected under APP 11 security requirements and aligned with organisational cybersecurity policies.

Notes:

AI Register and System Inventory

☐ Comprehensive Register: Each AI system is recorded with details of its owner, purpose, data sources, suppliers, risk rating, and assurance status.

☐ Linked Records: Each entry links to its PIA, impact assessments, approvals, and monitoring outcomes.

☐ Currency and Accuracy: The register is reviewed at least annually and before any major system change.

Notes:

Human Oversight and Audit

☐ Defined Oversight Roles: Named accountable officers are responsible for reviewing AI outputs and ensuring ethical use.

☐ Human-in-the-Loop Verification: Critical decisions are subject to documented human review.

☐ Independent Audit: Internal or external audits assess compliance with AI governance standards, accuracy, and fairness metrics.

Notes:

Records and Information Management

☐ AI Interactions as Records: AI-generated outputs, relevant prompts or inputs, and evidence of human review that generate, influence, or are relied upon as organisational records are captured as official records

☐ Retention and Disposal: Records are retained or disposed of according to approved schedules.

☐ Metadata and Audit Trails: Decision logs, datasets, and model documentation are retained as metadata for accountability and future review.

☐ Continuity and Preservation: Long-term preservation plans exist for AI records needed for evidence or accountability.

Notes:

Transparency and Communication

☐ Disclosure and Awareness: Staff, customers, and stakeholders are informed when AI is used in decisions affecting them.

☐ Explainability: AI decision processes can be explained in plain language, with evidence available for review.

☐ Public Confidence: Public-facing disclosures (where appropriate) demonstrate compliance and responsible use.

Notes:

Monitoring and Review

☐ Performance Testing: Systems are tested regularly for accuracy, bias, and reliability.

☐ Model Drift and Change Control: Changes in performance or data triggers formal review and revalidation.

☐ Ongoing Assurance: Monitoring reports are tabled with the AI Governance Committee and Governing Authority/Board.

Notes:

Training and Capability

- ☐ Competency Development: Staff involved in AI design, procurement, or oversight receive regular training on governance, privacy, and records obligations.
- ☐ Awareness for All Users: All employees interacting with AI systems understand their responsibilities, limitations, and escalation pathways.
- ☐ Continuous Learning: Lessons from incidents, audits, or reviews are integrated into training programs and policy updates.

Notes: