Service Description

AI Governance Assessment

Scope

An AI governance assessment is a systematic evaluation of an AI system (or portfolio of systems) to ensure it aligns with your governance objectives, legal and regulatory requirements, risk management, ethics, accountability, and operational integrity. Analogous to privacy or third-party risk assessments but tailored to the particular risks and characteristics of AI.

The assessment establishes a clear understanding of the purpose and scope of the AI system, including its use-case, intent, and business impact. It examines the system's functionality and performance to confirm its accuracy, reliability, and stability. Attention is given to fairness and bias to identify and mitigate any discriminatory or prejudiced outcomes. Privacy and data practices are scrutinised to ensure that data sources, retention, and processing adhere to lawful and ethical standards. Security and access controls are evaluated to confirm that appropriate safeguards, permissions, and resilience measures are in place.

The review also considers governance and accountability structures, ensuring ownership, oversight, and decision authority are well defined. Legal and regulatory compliance is mapped against relevant laws and emerging AI regulations to confirm conformity. Transparency, explainability, and logging are emphasised to ensure that decisions are interpretable, documented, and auditable, particularly in the context of automated decision-making. Finally, the assessment supports ongoing monitoring and continuous improvement by tracking performance, detecting model drift, and recording corrective actions over time.

Approach

Aligned with the IAPP framework, NIST AI Risk Management Framework, ISO/IEC 42001, and leading industry practices, this methodology is expressed through a five-phase execution model that integrates compliance discipline with practical delivery.

Initiation

The initiation phase presents the assessment's purpose, scope, context, key drivers, stakeholders, and success criteria.

- Define the purpose, scope, and business context of the assessment.
- Identify AI systems, models, and use cases in scope (internal or third-party).
- Confirm drivers - regulatory, ethical, operational, or procurement-related.
- Map key stakeholders across data science, compliance, legal, and IT.
- Establish success criteria, deliverables, and reporting format.

Discovery & Data Collection

This phase focuses on gathering evidence through documentation review, stakeholder engagement, and analysis of system design, data, and controls.

- Gather information on system design, model training, and decision logic.
- Review documentation, model cards, and governance artefacts.
- Conduct stakeholder interviews and evidence walkthroughs.
- Collect inputs on data sources, access controls, and monitoring practices.

Risk & Control Evaluation

This phase assesses governance controls and compliance across the AI lifecycle, evaluating fairness, privacy, security, accountability, and explainability to identify, quantify, and prioritise key risks.

- Evaluate governance controls against frameworks (NIST AI RMF, ISO/IEC 42001, IAPP).
- Assess lifecycle stages - design, testing, deployment, monitoring, and decommissioning.
- Examine controls for fairness, privacy, security, accountability, and explainability.
- Map compliance alignment to regulatory requirements (EU AI Act, APRA CPS 230/234).
- Quantify and prioritise risks using likelihood × impact scoring.

Validation & Stakeholder Review

This step validates preliminary findings with key stakeholders, confirming their accuracy and relevance, and prioritises remediation actions based on severity and business impact.

- Review preliminary findings with technical and governance leads.
- Validate accuracy and relevance of identified issues or risks.
- Prioritise remediation based on severity and business impact.
- Document agreed actions, owners, and timeframes.

Reporting & Continuous Improvement

This stage presents findings to senior stakeholders, providing targeted recommendations and integrating outcomes into enterprise governance cycles to support ongoing improvement and reassessment.

- Present findings to executives or governance boards.
- Deliver targeted recommendations for policy, tooling, or process updates.
- Establish reassessment cadence (e.g. annually or after major model updates).
- Integrate findings into enterprise risk, data governance, and audit cycles.

Value

The AI Governance Assessment transforms AI from a compliance risk into a trusted, auditable, and well controlled capability, building trust, ensuring compliance, strengthening oversight, and enabling responsible, efficient, and ethical innovation.

- Reduces Risk & Ensures Compliance: Identifies legal, ethical, and operational risks early, aligning AI use with emerging regulations and organisational policies.
- Builds Trust & Accountability: Demonstrates transparency, explainability, and responsible oversight of automated decisions.
- Enables Responsible Innovation: Creates confidence to scale AI safely while maintaining fairness, integrity, and ethical standards.
- Improves Efficiency & Assurance: Integrates AI oversight into existing risk frameworks, reducing duplication and enhancing decision confidence

Benefits

These are the key advantages of undertaking this service offering.

- Strengthens organisational readiness for evolving AI regulations and compliance obligations.
- Enhances audit and review processes through consistent and structured assessment practices.
- Improves transparency and accountability through documented decision trails and explainability measures.
- Accelerates AI deployment by aligning governance controls with operational workflows.

Outputs

These outputs are delivered to support implementation and forward planning.

- AI Governance Assessment Report: Executive-level summary of findings, risk ratings, and key recommendations.
- Detailed Risk Register: Catalogue of AI-specific risks (e.g. bias, explainability, drift, data provenance) with severity, likelihood, and mitigation actions.
- System Profile / Model Inventory: Structured record describing each AI system's purpose, owners, data inputs, outputs, and lifecycle stage.
- Regulatory Mapping Matrix: Alignment of AI controls to applicable laws and standards (e.g. APRA CPS 230/234, NIST RMF, ISO 42001, GDPR Article 22).

Discovery & Risk Mapping

As part of delivering this service, a secure SaaS tenancy of the Data Governance / DSPM (Data Security Posture Management) platform may be provisioned, or tool connectors may be established through API integrations. This setup enables the registration, monitoring, and inspection of machine learning tools in use, as well as the configuration of governance workflows that support compliance reporting and risk scoring.

The DSPM is IRAP-assessed and SOC 2 Type II certified, ensuring alignment with recognised information-security and assurance frameworks. All traffic is encrypted in transit and governed under the client's enterprise security, privacy, and compliance controls.