

Service Description

Data & AI Risk Register as a Service

Scope

The Data & AI Risk Register as a Service offering provides ongoing support for documenting, maintaining, and maturing a unified view of risks across data governance, privacy, and AI systems. It enables organisations to proactively identify, track, prioritise, and mitigate risks associated with sensitive data use, automated decision-making, and digital operations.

This service includes design, population, and monthly or quarterly maintenance of a fit-for-purpose risk register - aligned with frameworks such as ISO 27001 (Information Security Management), NIST Privacy / AI RMF (AI Risk Management Framework), APRA CPS 234 (Information Security), and the Australian Privacy Act. It integrates privacy, security, AI ethics, and data lifecycle risks into a unified governance artefact that supports compliance, audit, and board-level reporting.

Approach

Delivered in five structured phases, this service balances practical delivery with governance uplift - offering a reusable foundation for compliance, audit, and operational assurance.

Initiation & Design

Define the purpose, categories, and roles required to support a tailored risk register.

- Define register purpose - compliance readiness, risk visibility, audit preparation, AI governance uplift.
- Confirm inclusion criteria - data-related risks, privacy risks, AI/ML system risks, automated decision systems, third-party data exposure.
- Review existing risk frameworks (e.g. enterprise risk register, privacy risk register, AI logs).
- Agree register structure: fields, categories, scoring logic, ownership model, update cadence.

Risk Identification & Population

Populate the register based on identified data and AI risks.

- Conduct discovery interviews and system reviews to identify existing and emerging risks.
- Map risks across data lifecycle stages (collection, access, storage, use, retention, deletion).
- Capture AI-specific risks: bias, model drift, explainability, third-party vendors, shadow AI.
- Score risks using likelihood × impact × detection difficulty (or aligned to enterprise matrix).

Validation & Alignment

Ensure organisational stakeholders have reviewed and validated inputs.

- Review draft register with key stakeholders (risk, privacy, data governance, IT security, AI leads).
- Confirm accuracy, relevance, and ownership of each risk entry.
- Align with enterprise risk taxonomy and scoring methodology (where required).
- Agree risk prioritisation and remediation urgency.

Ongoing Maintenance & Reporting

Establish mechanisms to maintain, review, and use the register going forward.

- Deliver monthly or quarterly updates to the register based on incidents, audits, new systems, or regulatory changes.
- Facilitate regular risk reviews and stakeholder validation cycles.
- Track changes in risk profile over time (risk trending, mitigation progress).
- Support executive reporting and board-level summaries as required.

Governance Integration & Roadmap

Embed the register within existing governance structures and planning cycles.

- Integrate risk register into broader governance systems (GRC) - privacy, cyber, compliance, AI governance.
- Recommend owners, update cadence, and reporting workflows for internal teams.
- Identify tooling options: Excel, SharePoint, GRC tools, or lightweight SaaS platforms.
- Provide guidance on integration with incident response, procurement, or PIA processes.



Value

The Data & AI Risk Register as a Service transforms fragmented data and AI risks into a unified, visible, and actively managed governance tool.

- Proactively surfaces risks across privacy, security, and AI before they escalate.
- Supports compliance with CPS 234, Privacy Act reforms, ISO 27001, NIST AI RMF, and emerging AI legislation.
- Builds risk literacy across data owners, IT, and compliance teams.
- Enables audit-readiness and improves confidence of executive and board stakeholders.
- Integrates seamlessly with broader enterprise risk management efforts.

Benefits

The service delivers the following strategic and operational benefits.

- Centralises and continuously updates risks related to data and AI systems.
- Improves regulatory compliance posture and audit preparedness.
- Enhances communication between governance, IT, privacy, and executive teams.
- Reduces duplicated effort across privacy, AI, and cyber risk registers.
- Provides a platform for prioritising remediation and demonstrating accountability.

Outputs

Final deliverables will include the following items to drive ongoing action.

- Data & AI Risk Register: Populated register with fields, scoring, owners, and mitigation notes.
- Risk Heatmap: Visual prioritisation of risks by severity and likelihood.
- Register Design Template: Customisable format for internal re-use.
- Risk Summary Briefings: Executive-level slides for monthly or quarterly updates.
- Governance Integration Guide: Instructions for embedding register into BAU workflows.



Genesys Data stands with you to transform how to measure, approach and harness the power of your data, offering a portfolio of services that address the complexities of - getting data right! By integrating cutting-edge AI data-discovery techniques, advancing maturity modelling, and offering Data, Privacy and Security by Design, you'll be able to demonstrate appropriate duty-of-care, exceed privacy obligations, effectively gain control of data and understand how to become more cyber resilient and AI ready!

Learn more at www.genesysdata.com.au

Copyright © 2025 Genesys Data. All rights reserved. Other names may be trademarks of their respective owners.