Service Description

Privacy Maturity Modelling Assessment

Scope

A Privacy Maturity Modelling Assessment (PMMA) evaluates how effectively an organisation governs personal information, benchmarking its policies, processes, and technical controls against recognised privacy and security standards. It provides a structured and measurable evaluation of privacy capability and resilience, determining how well the organisation upholds transparency, accountability, and data protection in practice.

This assessment aligns with the OAIC's Australian Privacy Principles (APPs) to ensure lawful, fair, and secure management of personal information, the NIST Privacy Framework which is structured around the functions Identify, Govern, Control, Communicate, and Protect, and the Information Security Fundamentals of Confidentiality, Integrity, and Availability. Together, these frameworks create a standards-based evaluation that strengthens both privacy governance and data protection.

The Privacy Maturity Modelling Assessment examines how effectively privacy is embedded across people, processes, and technology. It reviews governance structures, accountability roles, and policy frameworks, assesses how personal information is collected, classified, used, retained, and destroyed, and evaluates whether privacy and security controls operate as intended. The assessment measures maturity across governance, risk, and operational layers, producing a quantified model typically ranging from Level 1 (Ad Hoc) to Level 5 (Optimised).

It also evaluates privacy risk management practices, compliance alignment with OAIC's APPs and the NIST Privacy Framework, the role of technology and automation such as data discovery or consent management tools, and the organisation's privacy culture, awareness, and training. The outcome provides a clear benchmark, identifies improvement priorities, and delivers a roadmap for enhancing privacy capability and resilience over time.

This service is particularly valuable for:

- Organisations managing large volumes of regulated, customer, or employee data
- Enterprises integrating AI, analytics, cross border processing, or third-party ecosystems.
- Businesses seeking audit readiness for OAIC, APRA CPS 230, 234 or 235, ISO or NIST, or GDPR/International Privacy requirements
- Organisations commencing projects involving AI or automated decision making

Approach

A structured method to assess, measure, and enhance organisational privacy maturity through defined phases that combine governance review, control evaluation, cultural analysis, and practical improvement planning – is further outlined below:

Initiation & Statement of Applicability

- Define scope, business units, data domains, and applicable frameworks (OAIC APPs, NIST Privacy).
- Establish stakeholder group(s) (Privacy Officer, CISO, Risk, IT, Legal).

Discovery & Evidence Collection

- Review policies, procedures, system controls, and operational practices.
- Conduct interviews and workshops to gauge process maturity.

Maturity Benchmarking & Analysis

- Assess each NIST PF category against a 5-level maturity model:
- Level 1 – Ad hoc, 2 – Developing, 3 – Defined, 4 – Managed, 5 – Optimised.
- Integrate CIA security principles into scoring - e.g., strength of data protection (C), accuracy and reliability (I), system availability and resilience (A).

Validation & Review

- Validate scoring and findings with stakeholders.
- Identify gaps, strengths, and dependencies across privacy and security domains.

Reporting & Roadmap Development

- Provide a visual maturity heatmap, detailed findings, and prioritised recommendations.
- Develop a staged roadmap for improvement (people, process, technology).

Value

- Regulatory Assurance: Demonstrates OAIC compliance and NIST PF alignment, proving active privacy governance.
- Strategic Clarity: Provides a measurable view of privacy maturity, highlighting where investment yields the greatest risk reduction.
- Integration with Security: Strengthens synergy between privacy and security controls through the CIA triad.
- Audit & Certification Readiness: Establishes evidence base for ISO 27701 or APRA CPS compliance audits or the NIST Framework adoption.
- Trust & Reputation: Shows customers, boards, and regulators that privacy and security are embedded, measurable, and improving.

Benefits

The PMMA directly enhances:

- Information Security & Risk Functions - aligning privacy controls with Confidentiality, Integrity and Availability security objectives.
- Data Governance Programs - providing a privacy maturity lens across data stewardship.
- Digital Transformation / Cloud Services - ensuring privacy governance keeps pace with technology adoption.
- AI and Analytics Functions - establishing baseline governance before introducing automated decision-making.
- Aligns technical safeguards with OAIC APP 11 (security of personal information) and NIST PF “Protect” and “Control” functions.

Outputs

These outputs are provided as part of this service:

- Privacy Maturity Assessment Report with detailed scoring by domain
- Maturity heatmap and summary of strengths, weaknesses, and improvement priorities.
- Benchmarking Dashboard – a representation of current vs. target maturity (mapped to OAIC APPs and NIST PF).
- Comparative analysis against industry peers or regulatory expectations.
- A proposed Risk Register & Improvement Roadmap
- Where relevant – An Integration pathway for AI-driven DPSM or automation tooling.
- Executive Summary, as a concise board-level view of privacy posture, key risks, and investment priorities.

- OPTIONAL: Privacy Toolkit - templates for policy updates, privacy metrics, training plans, and PIA triggers.

Relationship to other Genesys Data Services

The Privacy Maturity Modelling Assessment provides an enterprise-wide view of privacy capability and governance effectiveness. It differs from other Genesys Data privacy services in focus and depth, such as:

The Privacy Impact Assessment (Comprehensive) focuses on specific projects or technology initiatives, assessing privacy risks and mitigations prior to implementation. The PMMA instead evaluates organisational maturity, culture, and systemic governance strength.

The Data Privacy Assessment reviews operational compliance, data flows, and technical controls across systems. The PMMA extends beyond compliance validation to provide strategic benchmarks, maturity scoring, and long-term improvement pathways.

Together, these services form a cohesive privacy assurance framework: the Data Privacy Assessment confirms operational control strength, the Privacy Impact Assessment (Comprehensive) manages project-level risk, and the Privacy Maturity Modelling Assessment measures and guides enterprise-wide privacy capability and resilience.