Service Description

Information Lifecycle & Retention Review

Scope

The Data Retention Lifecycle Strategy Service establishes a unified and defensible baseline for the responsible management of personal and sensitive information from creation to lawful disposal. It is based upon in scope Data-Sets identified during planning and onboarding, including structured data within databases and enterprise systems such as ERP and CRM, unstructured information stored across file shares, SharePoint, and collaboration platforms, email archives including Exchange, Microsoft 365, and journaling systems, as well as tertiary copies such as backups, snapshots, legacy archives, and disaster recovery Data-Sets.

The strategy defines clear rules for what information must be retained, the duration of retention, and the governing authority or legal basis, ensuring alignment with State and Federal Recordkeeping Acts, Privacy and Financial Regulations (including the OAIC APPs, ASIC, APRA CPS 234 and 235, and GDPR), and any applicable business or legal hold requirements. It delivers a comprehensive lifecycle model that promotes good governance, accountability, and operational efficiency, while supporting automation through DPSM tooling for policy enforcement and retention oversight. The Data Retention Lifecycle Strategy provides a structured and sustainable approach to managing information assets, ensuring compliance, reducing risk, and maintaining transparency throughout the data lifecycle.

Approach

This engagement follows a structured, phased approach designed to assess, refine, and embed effective information lifecycle and retention practices.

Discovery

This phase establishes a clear understanding of the organisation's data environment, existing retention practices, and compliance obligations.

- Identify data types "in scope data-sets", repositories, and storage tiers across structured, unstructured, and tertiary data.
- Review existing retention schedules, legal holds, and destruction processes.
- Assess compliance alignment with legislative recordkeeping obligations.

Risk Profiling

This stage identifies information risks, sensitivity levels, and control gaps to inform classification and governance priorities.

- Map data against sensitivity, business value, and regulatory requirements.
- Define classification categories (e.g. public, confidential, restricted, personal, sensitive).
- Evaluate the role of automated Data Security Posture Management (DSPM) tools for discovery, tagging, and enforcement.

Retention Design & Considerations

This step develops or updates retention policies and schedules to ensure compliance, defensibility, and operational relevance.

- Create or update retention schedules linked to regulatory and operational drivers.
- Define policies for archiving, retention periods, and defensible deletion.
- Address exceptions - legal hold, audit, and disaster-recovery copies.

Implementation Roadmap

This phase defines the steps required to operationalise and embed the retention strategy across people, processes, and technology.

- Define steps to operationalise the retention strategy: roles, processes, and technical integration.
- OPTIONALLY: Align DSPM automation for data sampling, tagging, expiry, and policy compliance alerts.
- Build communication and training plans for data stewards and custodians.

Validation & Governance Integration

This stage confirms alignment with enterprise governance frameworks and establishes measures for continuous oversight and assurance.

- Review alignment with enterprise data governance and privacy frameworks.
- Recommend KPIs and reporting cadence for ongoing assurance.
- Integrate lifecycle oversight into risk and audit programs.

Value

This review provides a clear, compliant, and efficient approach to managing information throughout its lifecycle.

- Compliance Assurance: Aligns data retention and disposal practices with recordkeeping and privacy legislation.
- Risk Reduction: Minimises exposure from over-retention, shadow data, and ungoverned backups.
- Operational Efficiency: Reduces storage and eDiscovery costs through defensible deletion.
- Transparency & Accountability: Provides auditable evidence of lifecycle decisions.
- Automation Enablement: Establishes foundations for continuous retention governance through OPTIONAL, though increasingly required, AI-enabled DSPM tooling.

Benefits

These are the key advantages of undertaking this service offering.

- Regulatory Compliance: Aligns data retention and disposal practices with statutory, recordkeeping, and privacy obligations.
- Risk Reduction: Minimises exposure from redundant, obsolete, or over-retained data, ensuring defensible lifecycle decisions.
- Storage Efficiency: Reduces data volumes and storage growth through the controlled and compliant removal of unnecessary information.
- Operational Confidence: Improves response times to audits, subject access, and regulatory requests through reliable retention evidence.
- Governance Maturity: Strengthens policy enforcement and monitoring capabilities, supporting automation and continuous improvement via DPSM integration.

Outputs

This engagement delivers practical artefacts and reports that enable implementation, automation, and ongoing governance.

- Data Retention Strategy Document – enterprise-wide policy and principles aligned with recordkeeping obligations.
- Retention Schedule & Matrix – mapping of data types to mandated retention periods and disposal actions.
- Lifecycle Governance Model – defined roles, responsibilities, and escalation paths.
- Data Inventory & Classification Report – visibility of data holdings, sensitivity levels, and compliance gaps (optional)

- Implementation Roadmap – prioritised plan for rollout, automation, and governance alignment.
- Executive Summary – concise board-level briefing highlighting compliance uplift and improvements.

Capabilities & Constraints

In Scope Data-Sets

In scope Data-Sets comprise the information repositories, systems, and storage locations included for discovery or sampling under this engagement. For this Data Risk Snapshot, these Data-Sets are limited to one workload, either SharePoint Online or OneDrive. These defined workloads are subject to automated discovery and risk assessment within a secure DSPM tenancy.

Additional Data-Sets can be included as part of a broader Automated Data Discovery Service, available from Genesys Data.

Discovery & Risk Mapping

As part of performing this service - a secure SaaS tenancy of the Data Governance / DSPM platform may be provisioned to enable data discovery, sampling classification, signalling, and file recognition across in-scope Data-Sets.

Connectivity will be established through tenant onboarding, delegated app consent, and Entra ID role-based access, providing controlled and auditable integration with the client environment.

The DPSM 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.

Data Volume Coverage (Scan)

Data volume coverage refers to the total quantity of data, measured in terabytes (TB), scheduled to be scanned to capture metadata and security posture as part of the engagement.

Content Inspection (Classification and Visualisation)

Content Inspection refers to the capability to analyse the actual content within information assets, including but not limited to documents, emails, PDFs, and chat transcripts, to confirm patterns or entities such as personal information, credit card numbers, or business sensitive detail. Examples of such activities include scanning file repositories for personally identifiable information (PII) or identifying sensitive context within legal or commercial documents.

Content Inspection may be OPTIONALLY included within the current scope of this engagement.

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**