Genesys DATA

Service Description
M365 Data Risk Snapshot

Scope

The M365 Data Risk Snapshot is a fast, high-impact engagement designed to assess the visibility, exposure, and risk of sensitive and business-critical data across Microsoft 365 SharePoint Online or OneDrive. The service uncovers how data is created, shared, and retained - and identifies security, privacy, and compliance risks due to over-exposure, lack of classification, weak permissions, or poor lifecycle controls.

It is particularly useful as a precursor to Data Governance, Privacy improvement, AI adoption and management, or compliance uplift initiatives.

Approach

The assessment is delivered over five phases, aligned to DSPM (Data Security Posture Management) principles and best practices drawn from APRA's CPG 235 (Managing Data Risk), Electronic Discovery Reference Model (EDRM) and NIST Cyber Security, Privacy and AI management frameworks.

Initiation & Scope Confirmation

This phase establishes scope, stakeholders, and priorities to guide the assessment.

- Confirm objectives: security uplift, privacy assurance, governance maturity, compliance, e.g. APRA CPG 235, Australian Privacy Act.
- Identify key business units, user groups, and M365 workloads (in scope Data-Sets) to be assessed.
- Map data custodians across IT, legal/privacy, compliance, records, and business owners.
- Agree success criteria, reporting outputs, and remediation thresholds.

Discovery & Data Collection

This phase collects data from in scope Data-Sets to assess usage, exposure, and sharing.

- Configure and scan – CRUD (Create, Read, Update, Delete), metadata, and sharing activity from in scope Data-Sets.
- Analyse sharing patterns (internal/external/anonymous), file types, potential PII/PCI data, and permissions inheritance.

- Identify stale data, ROT (Redundant, Obsolete, Trivial), and overshared content and identify expected storage management charges.
- Review audit logs, classification labels, and sharing policies where enabled.
- Conduct simple lightweight interviews to validate findings and contextualise risk

Risk & Control Evaluation

Here we assess risks and controls to benchmark security posture and governance gaps.

- Assess data risk by content sensitivity, exposure level, user roles, and collaboration.
- Align risks to the NIST Privacy, Security and AI management frameworks, along with The Privacy Act's APPs.
- Provide a scorecard, visualising top risks identified

Validation & Stakeholder Review

This step confirms findings with stakeholders and shapes remediation priorities.

- Present findings to IT, compliance, and data/business owners.
- Validate identified issues and prioritise based on operational and compliance exposure.

Reporting & Recommendations

We summarise findings and define a roadmap for capability uplift, aligned to objectives.

- Conclude executive-ready report and recommendations for security, privacy, and governance enhancements.
- Provide a roadmap for short-term remediation and longer-term governance uplift (e.g. metadata, classification, lifecycle policies).
- Recommend cadence for repeat assessments (e.g. quarterly or semi-annually).

Value

A Data Risk Snapshot empowers organisations to understand and act on data risks in M365 - without requiring long-term consulting engagements or enterprise tooling rollouts.

- **Fast Insight, Immediate Action:** Identifies data exposure risks in days, not months.
- **Improves Compliance & Security Posture:** Aligns M365 data and configuration with best practice frameworks.
- **Enables Informed Governance:** Provides hard data to support prioritised action on oversharing, stale data, and weak permissions.

- **De-risks AI & Automation:** Reduces exposure of sensitive data that may be used in LLMs, automation workflows, or AI tools like Copilot and ChatGPT.
- **Supports Enterprise Uplift:** Lays the foundation for classification, retention, and lifecycle governance and highlights the business value in the adoption of automation and DPSM technologies to address the Confidentiality, Integrity and Availability of data as part of fundamental security principles.

Benefits

These are the key advantages of undertaking this service offering.

- Rapidly identifies high-risk oversharing and poorly protected sensitive data
- Reduces privacy, IP leakage, and compliance breach risks
- Strengthens Microsoft 365 tenant configuration and access control
- Supports privacy-by-design, AI risk management, and DSPM principles
- Builds the case for structured data governance investments

Outputs

These outputs are delivered to support implementation and forward planning.

- **Data Risk Snapshot Report:** Executive summary, key findings, risk insights
- **Risk Scorecard:** with source, severity, exposure, and suggested actions
- **Content & Exposure Inventory:** Summary of top content types, sharing patterns, and sensitive data locations
- **Remediation Action Plan:** Prioritised tasks, responsible owners, and recommended timelines
- **Governance Uplift Roadmap:** Optional next steps for classification, retention, lifecycle, and metadata strategy

Capabilities & Constraints

In Scope Data-Sets

In scope Data-Sets comprise the information repositories, systems, and storage locations included for discovery 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 DPSM 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 (Data Security Posture Management) platform will be provisioned to enable data discovery, 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 Data Risk Snapshot engagement. The anticipated data volume is expected to fall within the range of 1 to 10 TB, which will be discussed, priced and agreed prior to commencement of scanning activities.

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 is not included within the current scope of this engagement; however, Genesys Data may provide further consultation or advisory services in relation to the potential implementation or enablement of DCI capabilities as part of future phases or separate engagements.

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**