Service Description
Data Protection & Cyber Resilience Exercise

Scope

This assessment will determine the organisation's overall readiness to prevent, detect, respond to, and recover from data loss or cyber incidents, including ransomware, insider threats, and cloud compromise. It will evaluate end-to-end data protection posture across the on-premise and cloud environments, encompassing infrastructure as a service, software as a service, and hybrid workloads.

The review will consider the people, process, and technology dimensions through structured scenario-based questioning, examining the design and enforcement of retention schedules, backup and archival processes, and data immutability controls. The assessment will also validate whether Recovery Point Objectives and Recovery Time Objectives align with business criticality and regulatory expectations.

Finally, governance alignment will be assessed against recognised frameworks such as NIST CSF, Essential 8, ISO 27001 and 27040, and APRA CPS 234 and 235, with optional mapping to privacy and AI governance controls.

Approach

This engagement follows a structured, five-phase approach designed to assess data protection and cyber resilience, balancing practical risk control with user awareness and operational effectiveness.

Pre-Workshop Discovery

We begin by gathering key artefacts and identifying critical applications and data sets essential to the organisation:

- Gather relevant artefacts: incident-response plans, business-continuity documentation, backup architecture diagrams, retention schedules, and vendor SLAs.
- Identify critical applications and data sets (ERP, trading, financial, HR, customer platforms).

Table-Top Session

This phase simulates a realistic data-loss or ransomware event to test the organisation's readiness, coordination, and response effectiveness:

- Over 3-4 hours - simulate a ransomware or data-loss scenario and walk through response and recovery actions step-by-step.

- Engage key stakeholders - IT Ops, Security, Risk, Legal, Compliance, and Business Continuity.
- Explore decision-making, escalation paths, communications, and leadership visibility during an event.

Structured Assessment

This step evaluates data-protection maturity across people, process, and technology through detailed review and performance analysis:

- Measure maturity across People, Process, and Technology using defined risk-posture indicators (e.g., ability to recover, time to restore, dependency on key vendors).
- Evaluate backup-success metrics, failover procedures, and cloud-native recovery methods.
- Review retention-policy design and its enforcement in cloud and on-prem environments, ensuring records, backups, and archives meet compliance retention and defensible-disposal requirements.

GAP & Risk Analysis

This stage identifies weaknesses and deviations from best practice by comparing current capabilities against expected recovery standards:

- Compare current practices with best-practice models and required recovery performance (RPO/RTO).
- Identify systemic weaknesses: dependency on manual recovery, untested playbooks, or lack of immutable storage.

Recommendations & Action Planning

This phase delivers prioritised recommendations and practical actions to strengthen protection, recovery, and governance controls:

- Produce targeted, prioritised recommendations mapped to risk severity and effort.
- Define actions across technology (e.g., adopt Air-Gap / Immutable Storage), process (e.g., formalise retention review cadence), and people (e.g., clarify recovery roles).

Value

This assessment provides measurable insight into resilience, building confidence and alignment across business, risk, and technology functions:

- Provides a clear, evidence-based view of organisational resilience, with quantifiable metrics on data-protection maturity.
- Builds executive and board-level confidence through a realistic, low-impact simulation that tests readiness without operational risk.
- Establishes a common language between Technology, Risk, and Business stakeholders for resilience and recovery priorities.

- Aligns retention, protection, and recovery capabilities to business continuity, regulatory, and customer-trust outcomes.
- Enables continuous improvement tracking over time to demonstrate progress to auditors and regulators.

Benefits

These are the key advantages of undertaking this service offering:

- Validated Recovery Readiness – Confirms ability to recover mission-critical workloads from immutable and tested backups.
- Optimised RPO and RTO Alignment – Ensures backup frequency and recovery performance meet business and compliance needs.
- Reduced Downtime and Data-Loss Risk – Identifies process bottlenecks, automation gaps, and vendor-dependency risks before an event.
- Enhanced Retention and Disposal Compliance – Ensures retention schedules are defensible, cloud-compatible, and aligned with privacy obligations.
- Improved Cloud Resilience – Evaluates cloud data-protection controls (geo-redundancy, snapshot policies, identity segregation).
- Strengthened Governance Posture – Demonstrates tangible evidence of resilience for internal and external assurance reviews.

Outputs

This engagement produces structured reports, actionable plans, and dashboards that summarise findings and guide continuous improvement:

- Executive Summary Report highlighting findings, maturity scores, and key risk observations across People, Process, and Technology.
- Detailed Gap and Risk Matrix mapped against core control domains - Protect, Detect, Respond, and Recover.
- Prioritised Action Plan outlining short-term wins and long-term strategic concepts.
- OPTIONAL: Resilience Roadmap showing a 6 to 12-month improvement pathway with measurable RPO/RTO validation points.
- OPTIONAL: Retention and Recovery Design Recommendations, including enhancements to tiered storage, lifecycle policies, and cloud retention enforcement.