Data Governance and Compliance Product

An enterprise-grade Information Lifecycle Governance product designed to help regulated organisations govern, protect and manage information throughout its entire lifecycle.

29 July 2026

The Problem

Data retention is a governance, compliance and risk problem that needs ongoing focus and maintenance not only within e5, but across all applications that store data, particularly personally identifiable information (PII).

Data growth

Information continues to accumulate across repositories, legacy platforms and business systems.

Manual sentencing

Retention and disposal decisions are often tracked through spreadsheets, emails and ad-hoc approvals.

Limited proof

When audit questions arise, it is difficult to show who approved what, when and why.

Compliance exposure

Inconsistent controls increase risk against records, privacy, ISO and APRA-aligned obligations.

Security risk

Retaining unnecessary data increases the exposure surface for cyber, privacy and operational incidents.

No operational owner

Policies exist, but accountability and day-to-day control are fragmented across business teams.

The key question becomes:

What data should we keep, what should we dispose, who approved it and can we prove it?

The e5 Solution

The e5 Data Governance product, built on e5connect.ai, gives you operational control for data retention, data sentencing and defensible data disposal. It is designed with security, authorization and auditability at its core.

Traditional approach	e5 Data Governance
Retention policies sit on paper	**Retention policies are operationalised.** Every destruction activity originates from an approved Policy. No destruction occurs outside Policy governance.
Manual reviews and approvals	**Workflow-driven review and sentencing**
Limited visibility across systems	**Dashboards, status, logs and audit views**
Disconnected decisions	**End-to-end governance with ownership.** Every destruction activity must be independently verified before governance is considered complete.
Difficult audit preparation	**Complete, searchable audit history.** Every destruction activity is supported by sufficient evidence to withstand regulatory review and legal scrutiny.
Reactive compliance	**Continuous control and compliance management**
	Legal Hold, preventing modification or destruction during legal obligations
	Destruction Certificate, provides a permanent evidentiary record demonstrating that destruction occurred in accordance with the approved Policy and governance controls with immutable audit references.

Govern — Assess — Approve — Audit — Execute — Report

Maintain Control

Security first

- Microsoft Entra ID authentication
- Role and permission-based access
- Server-side authorisation
- Safe error handling and correlation IDs

Governance controls

- Enterprise inclusion management
- Configuration governance
- Audit event tracking
- User, role and permission management

Compliance alignment

- ISO 27001 aligned controls
- APRA CPS 230 / CPS 234 alignment
- Defensible disposal and evidence
- Complete audit history

Business outcomes

- Reduce risk
- Gain visibility
- Improve compliance
- Operationalise retention
- Increase accountability

Learn more: e5connect.com