

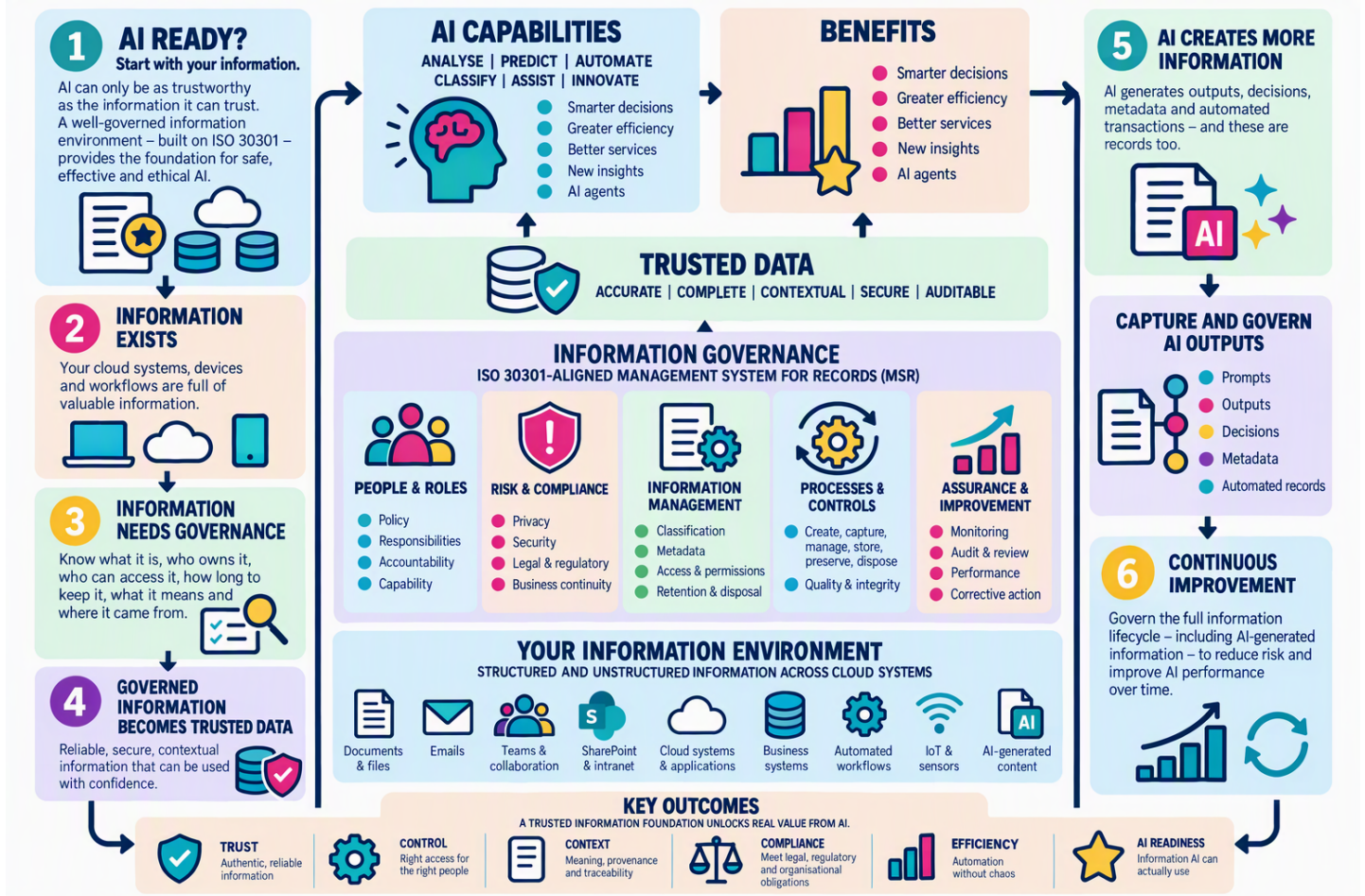


Information Governance

The foundation for AI readiness

Strategic Implementation Plan for an ISO 30301-Aligned Management System for Records (MSR)

AI does not magically know what is reliable, appropriate or safe. It works with the information it can reach across cloud platforms, business systems, documents, workflows and other digital environments. If that information is messy, poorly governed or open to the wrong people, AI can scale the problem fast, spreading inconsistencies, stripping away context and making it much harder to see who did what and why.



Govern the information → enable the AI → govern the information AI creates.



Executive Overview

AI is turning up in everyday work fast. The real question is no longer whether an organisation can switch it on. It is whether the information underneath it is organised, trustworthy and properly controlled so AI can use it without creating a bigger mess.

A Management System for Records (MSR) gives that work a practical backbone. It sets out who is responsible, how information is handled, which controls apply and how the organisation checks that its information stays authentic, reliable, complete, usable, secure and traceable.

This plan turns AS/NZS ISO 30301:2020 and AS/NZS ISO 30302:2023 into a roadmap an organisation can actually use. ISO 14641:2018 also comes into play when electronic documents need to survive for the long haul. Before using the plan for certification, audit, procurement or legal assurance, check it against the organisation's jurisdiction, operating environment, risks and licensed copies of the relevant standards.

THE STRATEGIC LOGIC

Information exists → governance makes it trustworthy → AI can use it with more confidence → AI creates new information → that information is captured and governed too → the organisation learns and improves.

What this plan is designed to achieve



- Build one clear information governance foundation across cloud platforms, business systems, workflows and every other place information lives.
- Make ownership, accountability, access, metadata, classification, retention, preservation and audit requirements clear.
- Build records controls into the work and the technology from the start, instead of bolting them on later.
- Create a controlled path for useful AI, including classification, metadata tagging, information discovery and workflow automation.
- Capture and govern the information AI creates, along with any automated actions that matter.
- Measure what is working, audit what is not and keep improving.

1. Understand the Information Environment

WHY THIS COMES FIRST

Start by working out what information the organisation creates, captures, stores, uses, shares and disposes of, and where all of that happens. The original plan rightly begins with the organisational, legal, operational and technology context. This version makes the next part explicit: the same environment is where AI finds information, produces outputs and triggers actions. If you do not understand that environment, you are asking AI to navigate the shed with the lights off.

External context

Dimension	What to examine
Legislative & regulatory environment	Statutory requirements, industry regulator rules, codes of practice, governance directives and jurisdictional boundaries.
Litigation profile	Historical and potential litigation profiles, legal precedents and regulatory enforcement actions.
Market & economic factors	Economic and competitive pressures, market dynamics and public/media scrutiny.
Technology environment	Cloud services, emerging digital platforms, AI, machine learning, automated workflows and other technologies creating or processing information.

Internal context

Dimension	What to examine
Governance & strategy	Strategic plans, governance structures, executive roles and delegations of authority.
IT infrastructure & architecture	System inventories, information architecture, enterprise data models, network security and legacy capabilities.
Culture & capability	Skills, business process maps, conduct expectations and staff capability to manage information correctly.
Operational governance	Project methods, procurement, contracts and existing retention/access commitments.
Assurance & compliance	Audit reports, enterprise risk registers and complementary management systems such as quality and information security.



The standards tell you what good looks like.

Working out how that applies to your organisation is the hard part.

What you've just read is only a small section of a much larger implementation guide. The full framework covers the people, processes, technology, governance and controls needed to support both compliant information management and responsible AI adoption.

If you'd like help turning principles into practical action, **let's talk.**

[Book a discovery session.](#)