SanRa

PRACTICAL BRIEFING / JULY 2026

AI management, *made ready.*

A practical introduction to ISO/IEC 42001 readiness for leaders building trustworthy AI systems.

Why ISO/IEC 42001 matters

AI introduces new ways of creating value — and new ways for controls, accountability and trust to break down. ISO/IEC 42001 provides a management-system framework for addressing that reality systematically.

It is not a technical checklist. The standard asks an organisation to establish, implement, maintain and continually improve an AI management system (AIMS). That puts policy, governance, risk, people, suppliers and evidence in the same frame.

For boards and executive teams, this provides a disciplined way to answer the questions customers, regulators and partners increasingly ask: What AI do you use? Who owns its risks? How do you know your controls work?

Readiness is therefore a design exercise, not a document exercise. It requires a credible view of the system, the people who operate it and the decisions that govern it.

> The aim is not paperwork. It is demonstrable, repeatable judgement around AI risk.

Five conditions for a credible AIMS

01

Context & intent

Define the AI-related objectives, stakeholders, obligations and risk appetite that shape the management system.

02

Accountability

Make decision rights clear: executive sponsorship, AI system ownership, independent challenge and escalation.

03

Risk & control

Assess risks across the AI lifecycle, including security, privacy, fairness, safety, misuse and third-party dependency.

04

Operational evidence

Translate policy into practical procedures, records, monitoring, incident learning and control evidence.

05

People & culture

Equip people to understand limitations, challenge outcomes and use systems safely in real conditions.

The strongest programmes make these conditions visible in everyday decisions — not only in annual reviews.

Start with evidence, not assumptions

PHASE	KEY QUESTION	USEFUL OUTPUT
Discover	Where is AI used, developed, procured or embedded?	System inventory, owners and material use cases
Prioritise	Which systems create the greatest risk or opportunity?	Risk-based scope and implementation roadmap
Design	What controls make policy operational?	Control framework, roles and operating procedures
Prove	What evidence shows that controls are working?	Metrics, reviews, testing records and management reporting
Improve	How will learning change the system?	Corrective actions and continual improvement cycle

> The first useful deliverable is often a defensible map of reality: systems, suppliers, data, decisions and accountable people.

Controls only work when people can use them

AI governance can fail at the point of human judgement: when people over-rely on outputs, lack the confidence to challenge them, or do not understand what a control is asking them to do.

Build AI literacy around actual roles and decisions. A policy is not enough if people cannot recognise an unsafe use case, escalate concern or understand the limits of automated output.

Test how controls behave under pressure. Consider time constraints, competing incentives, handovers and supplier dependencies — the conditions in which security failures often emerge.

Design feedback loops that help the organisation learn from near misses and incidents. Good governance makes it easier to surface concern early.

Make your first *move count.*

A focused readiness review can establish a shared baseline, identify priority gaps and give leadership a proportionate route forward.

SanRa works at the intersection of human factors, AI security and governance — helping organisations make their systems both safer and more usable.

Take the short AI security self-assessment at **sanra.co.uk**, or contact **hello@sanra.co.uk** to discuss a readiness conversation.

This paper is educational and does not constitute legal, technical or certification advice. ISO/IEC 42001 is an International Standard; implementation and certification requirements should be assessed for your organisation's particular context.