THE AIMS SERIES

An AI Management System Is Not a Policy Binder.

It's the machine ISO/IEC 42001 actually audits, and most organisations only find that out the hard way.

Four things this deck covers

01 What an AIMS actually is, and what it isn't

02 Why most organisations have policy without a system

03 The seven clauses an auditor actually checks

04 How to build evidence from day one, not before the audit

350+

organisations certified to ISO/IEC 42001 worldwide as of April 2026

Still a small fraction of enterprises already running AI in production. Doppel / PR Newswire, April 2026.

75%→12%

have a dedicated AI governance body, but only 12% call it mature

A committee is easy to stand up. A working management system isn't. Cisco 2026 Data and Privacy Benchmark Study.

69%

of compliance leaders say AI adoption is outpacing their controls

Only 6% say their governance is ahead of their adoption. Thoropass 2026 State of Audit and Compliance Report.

An AIMS is a system, and the policy is one part of it

- Seven clauses, **context to improvement**, that have to run continuously, not once
- Annex A: **nine control areas** covering resources, data, life cycle, and third parties
- A **statement of applicability** tying risk assessment to every control chosen or excluded
- The AI policy is **one document inside that system**, not the system itself

Documented information, not intention

- Can the **risk assessment** be re-run and reach a consistent, comparable result?
- Was the **impact assessment** run at scoping, and is it still on file?
- Has an **internal audit** already run against the ISO 42001 clauses themselves?
- Is there a **closed-loop record** from nonconformity to corrective action?

A statement of applicability signed once at kickoff and never touched again is the single most common gap an ISO 42001 auditor finds.

It's the fastest way to check whether the rest of the system is actually current.

Build the evidence as you go

1. Log the **system, data, and tooling inventory** the day a use case is scoped
2. Design the **risk assessment** to be repeatable, not a one-off workshop
3. Run the **impact assessment** before deployment, and keep it on file
4. Treat the **SoA** as a living document, updated every time risk changes
5. Audit against **the standard's clauses**, not just your own policy

Evidence built on day one beats evidence reconstructed before the audit.

An AIMS is a management system to run, not a certificate to earn once. Every risk assessment, every impact assessment, every internal audit is a record worth keeping from the day it happens.

Terence Kok
AI & Innovation Strategist

SAVE · COMMENT · FOLLOW