NAKEDAI — PILLAR ARTICLE

ISO 42001: A gap discovery, not an audit

What the standard actually examines, what most ISO 42001 programmes do, and where we sit upstream of all of it.

ISO 42001 is the first international standard for AI management systems. It was published by ISO in late 2023, and it has moved quickly from a standard nobody had heard of to a question being asked in tenders, by regulators, and by boards reviewing AI risk. The shift is recent. The pressure is real. And the way most organisations respond to that pressure is wrong.

This is what we do about that, and what we do not do.

What ISO 42001 actually examines

The standard has ten substantive areas. Each one represents a place where an AI management system must demonstrate it is real, not nominal.

Clause 4: Context

What is the scope of the AI management system? Which AI systems are inside it, which are outside, and on what basis?

Clause 5: Leadership

Is governance documented and approved by leadership? Is accountability assigned to named individuals?

Clause 6: Planning

Are risks identified, assessed, and treated through a systematic, documented process?

Clause 7: Support

Are the resources, competencies, and documented information required by the system in place?

Clause 8: Operation

Are AI systems inventoried? Is data lineage tracked? Are vendor and supplier requirements specified?

Clause 9: Performance evaluation

Is human oversight of AI-influenced decisions defined and active? Is internal audit happening?

Clause 10: Improvement

Is there a documented improvement cycle that responds to findings?

A certification audit examines each of these and asks for evidence. Not policy documents alone. Evidence: logs, decisions, records of meetings, examples of overrides, training completion data, supplier reviews, risk register updates. The documentation must be supported by traces of the system actually running.

What most ISO 42001 programmes offer

Most ISO 42001 advisory work is preparation for certification. A typical programme runs for twelve to eighteen months and includes scoping, policy drafting, documentation development, internal audit setup, mock audits, remediation, and finally the certification audit itself with an accredited body.

This is valuable work. It is also, when done well, expensive work. The risk is that organisations enter it before they should: before the underlying governance is real, before accountability is assigned, before the AI systems inside the scope are even properly inventoried. They pay for documentation that papers over governance gaps rather than addressing them, then go into a certification audit and watch the gaps surface anyway, recorded as findings.

We do not do the certification programme. We come earlier.

What gap discovery is

Gap discovery is what happens before the certification programme begins. Its job is to answer one question: where does the organisation actually stand against ISO 42001 today, and what is the work required to close the gaps that matter?

The output is not a certification. It is a clear, evidenced statement of where the organisation is, prioritised against the clauses that carry the most risk given the audit driver. A client tender requirement creates different priorities from a regulator inquiry, which creates different priorities from board pressure for governance maturity. A gap analysis that ignores the driver is a gap analysis that wastes effort.

We assess each of the ten substantive areas of the standard. We look for evidence, not declarations. The questions we ask are deliberately uncomfortable.

Does an AI inventory exist, and does it include the AI features embedded inside SaaS tools the organisation already pays for? This is the most commonly missed scope item. Is governance documented and approved, or does it exist in slide decks and verbal commitments? Is risk assessed across bias, privacy, security, accuracy, and continuity, or only the dimensions that have already caused trouble? Is accountability assigned to named individuals with documented acceptance, or to teams and committees that no one in particular owns? Is there documentation an auditor could read and follow, or documentation that would need translation by the person who wrote it? Are AI-influenced decisions reviewed by humans with the authority and information to overturn them, or by humans who serve as a rubber stamp? Is data lineage traceable, with consent and licensing evidence, or are the training data sources a story that is told rather than evidenced? Is internal audit scheduled and run, with findings tracked through to closure? Has the management review actually happened in the past twelve months, or is it scheduled to happen before the external audit?

These are the questions an auditor will ask. The earlier they are asked internally, the cheaper the answer is.

How we look for gaps

The work runs in three parts.

Discovery

Stakeholder interviews across the leadership, technology, legal and risk, and operations functions. A review of existing documentation. A walk-through of two or three AI systems to see how they actually run, not how they are described. Structured but conversational. The goal is to find what is real and what is nominal, before drawing any conclusions.

Mapping

The findings are mapped to the clauses of ISO 42001. For each clause we identify what is in place, what is partial, and what is absent. We score the readiness position by clause, and we surface the gaps that are most exposed given the audit driver.

Sequencing

Not every gap is equal, and not every gap should be addressed first. Some carry high audit risk and are quick to close. Others carry low risk and are expensive to close. Sequencing the remediation correctly is what separates an efficient certification programme from an exhausting one. We produce a sequenced remediation plan with named owners, time estimates, and the dependencies between gaps.

The output is a Gap Discovery Report and a remediation roadmap. The report is written so that an internal team or an external implementation partner can use it directly as the brief for the work that follows.

What happens after

The handoff is deliberate. The Gap Discovery Report is designed to be picked up by whoever runs the certification programme, whether that is an internal compliance team or an ISO 42001 implementation specialist. We do not insert ourselves into that programme. The reason is structural rather than strategic: the people who identify gaps and the people who close them should be different, because the closing work creates a bias in favour of declaring closure. An independent gap discoverer is more honest precisely because they are not on the hook to mark their own homework later.

Where ongoing oversight is useful, we provide a quarterly review against the original gap report. The review confirms whether the work has actually closed the gaps, or whether documentation has been produced that gives the appearance of closure without the substance. This is also where new AI systems are added to the inventory and assessed against the standard before they enter the management system.

Who this is for

Gap discovery is for organisations that are in one of three positions. A client or tender has asked about ISO 42001 readiness, or is likely to in the next twelve months, and the organisation needs to know where it stands before it commits to a certification programme. A regulator or sector body has signalled that AI

governance maturity will be examined, and the organisation wants a clear picture of its position before that examination happens. The board has asked for evidence of AI governance, and the leadership team needs an objective starting point that is not produced by the team being assessed.

It is also for advisers, lawyers, and compliance leads who need an honest second view before they brief their own boards or clients.

It is not for organisations that have already passed certification and need maintenance support. That is a different conversation.

The principle behind it

ISO 42001 will be earned by organisations whose AI governance is real. It will be failed, or passed in name only, by organisations whose AI governance is documented but not lived. The difference between the two is visible early, before any certification programme begins, if you know where to look.

We know where to look. That is the whole offer.

Find out where your ISO 42001 readiness stands

The ISO 42001 Audit Readiness Assessment is a ten-question diagnostic that maps your current position against the standard's substantive clauses. Three minutes; it returns a readiness score, a zone, and a clause-by-clause analysis showing where the gaps sit.

Take the Assessment at nakedai.io/iso-42001-audit-readiness-assessment