AS Aaron Soto
AI CONSULTING

DOCUMENT FOR LEADERSHIP

Judgment first

Why govern artificial intelligence before you automate, and how to do it with ISO/IEC 42001

Aaron Soto · Soto AI Consulting

AI governance and process automation

2026

EXECUTIVE SUMMARY

The question is no longer whether to adopt AI—it is how to do it with judgment

Artificial intelligence is already part of daily work in most organizations. What separates them is not how much AI they use, but whether they use it with clear rules, named owners, and risks under control. This brief explains why that order matters—and how to start.

01 **AI is already inside**

Teams, vendors, and pilots bring it in—whether leadership made a formal call or not.

02 **The risk is how you use it**

Leaked confidential data, unchecked outputs, and vendor lock-in are the usual consequences of running AI without rules.

03 **There is a standard for this**

ISO/IEC 42001—the international standard for AI management systems—defines how to govern AI in a way you can show.

04 **Govern first, then accelerate**

With the framework in place, each automation is evaluated, approved, and scaled with less friction.

THE CORE IDEA

Responsible AI adoption is not slowing innovation. It is giving innovation a base that can hold.

AI is already here—with or without a decision

In most organizations, AI did not arrive through a board strategy. It walked in through three doors at once—usually before anyone had the full picture.

— Through teams

People using generative AI to draft, summarize, or analyze—often on personal accounts, with no shared rules on what may be shared.

— Through vendors

AI features in email, CRM, ERP, or collaboration tools you already pay for—often on by default.

— Through projects

Pilots each area runs on its own, without shared criteria to approve, measure, or scale them.

None of that is bad on its own. The problem starts when nobody can say which AI is in use, with what information, and under whose accountability.

> **78%** of people who use AI at work do so with their own tools, not ones the company provided.

Four risks that are easy to miss

01

Information leaving the building

Client data, financial figures, or strategy pasted into external tools without clear terms. When personal data is involved, data-protection rules in your jurisdiction apply. In a Cisco study, 42% of professionals surveyed said they had entered non-public company information into generative AI tools.

02

Decisions nobody checked

AI outputs landing in reports, client replies, or internal decisions without anyone verifying accuracy.

03

Dependency without terms

Tools adopted without asking what the vendor does with data, what happens if terms change, or how you exit.

04

Investment that never scales

Promising pilots that stall because nobody defined how to approve, supervise, and measure them. Gartner estimated that at least half of generative AI projects were abandoned after proof of concept by end of 2025—often for weak risk controls, among other reasons.

Doing nothing is also a risk. Banning AI does not fix it: teams keep using it—now out of sight—and you give up productivity gains competitors are already taking.

Four reasons this is the moment

01

An international standard

ISO/IEC 42001, published in December 2023, is the first standard with requirements for an AI management system. It applies whether you build, sell, or simply use AI—any size, any sector.

02

A shared language

ISO/IEC 42001 gives leadership, auditors, and partners a common way to talk about AI policy, owners, risk, and controls—without reinventing the vocabulary for every market.

03

Clients and partners are asking

Corporate clients, parent companies, and international partners increasingly want evidence of how you manage AI and data.

04

Regulation keeps moving

Data-protection law already reaches AI use; AI-specific rules keep evolving; markets such as the EU already have their own regimes. A management system gives you a base to respond without scrambling.

> Organizations that put AI use in order today walk into those conversations prepared. Those that wait will do it under pressure.

Governance is not a brake

A governance framework is not extra bureaucracy. It replaces improvisation with a known path. You feel the difference in how the organization decides—and how it scales.

AUTOMATE WITHOUT A FRAMEWORK	AUTOMATE WITH JUDGMENT
Every area picks its own tools.	Authorized tools with shared use rules.
Nobody knows which AI is in use—or with what data.	An inventory of AI uses, with an owner per system.
Risks show up when something breaks.	Risks are assessed before a use case goes live.
Every pilot restarts the debate.	Shared criteria to approve, measure, and scale.
Hard to explain to clients or auditors.	Ordered, verifiable evidence.

With the framework in place, automations stop being one-off bets. Every use case follows the same path: evaluate, approve, build with human oversight, measure. That is the difference between experimenting with AI and adopting it.

What an AI management system is

It is how the organization directs and oversees its use of AI. ISO/IEC 42001 organizes that around five elements:

01 **A policy leadership signs**
What AI is for, on which principles—and what is off-limits.

02 **Clear owners**
Who decides, who supervises each system, and who can stop it.

03 **Risk and impact assessment**
Sized to the use: a writing assistant is not governed like a system that affects customers.

04 **Operational controls**
Over data, vendors, and the lifecycle of each AI system.

05 **Measurement and improvement**
Indicators, internal audit, and regular leadership review.

The standard does not demand a big structure or a new department. You set the scope with the organization: one area, one process, or a group of systems—and expand later.

AI with Judgment: from the standard to practice

AI with Judgment is Soto AI Consulting's methodology for adopting AI responsibly. It turns ISO/IEC 42001 into five phases with concrete deliverables, following Plan–Do–Check–Act.

PHASE 01

Context and scope

Which AI is in use today—and how far the system reaches.

PHASE 02

Leadership and policy

Usage rules and owners set by leadership.

PHASE 03

Risk and impact

Each use assessed and treated for its risk.

PHASE 04

Controlled operation

Controls in place; use cases inside the rules.

PHASE 05

Evaluation and improvement

Verify compliance and plan the next cycle.

Cross-cutting · People and culture: training, communication, and change support in every phase.

The first step is usually a gap assessment: a full review against the standard that shows where you stand, what is missing, and where to begin. It starts with a free conversation that includes a quick AI maturity check, so we understand business context and priorities.

07 · SELF-CHECK

Five questions for leadership

A fast way to gauge the starting point: try to answer these five with certainty.

- ☐ Do we know which AI tools our teams use—and which AI features our vendors already include?
- ☐ Are there written rules on what information may be shared with AI tools?
- ☐ Does each AI system have an owner who can supervise, correct, or stop it?
- ☐ Do we assess risk and impact before a use case goes into production?
- ☐ Could we show a client, partner, or regulator today how we govern AI?

> **If any answer is "no" or "I'm not sure,"** you already have a starting point. A gap assessment turns those answers into a plan.

SOTO AI CONSULTING

Responsible AI adoption based on ISO/IEC 42001

We help organizations adopt artificial intelligence responsibly, with a governance framework based on ISO/IEC 42001: from defining where it creates real value to implementing it in concrete processes and sustaining results over time. The practice works with a limited number of clients, which allows close, direct support with full confidentiality.

aaron@sotoaiconsulting.com · sotoaiconsulting.com/en/

ISO/IEC 42001 is published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This document is for information only: it does not reproduce the standard or replace legal advice.