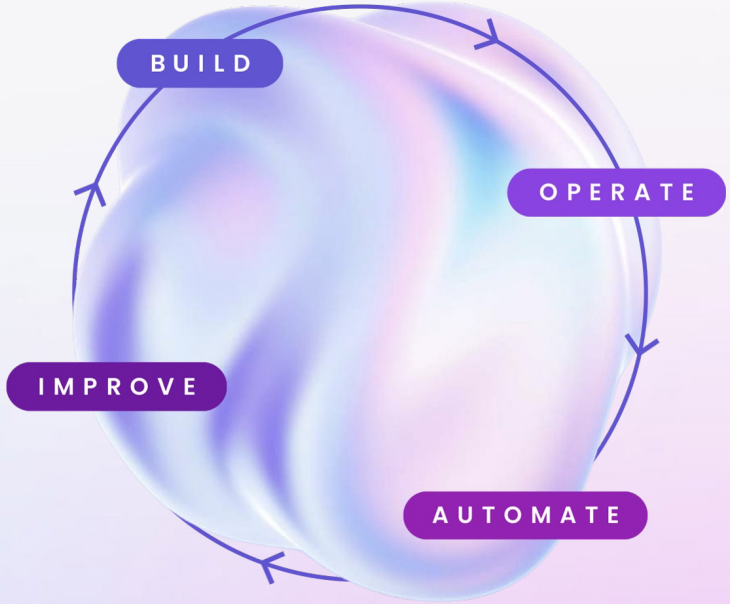
GUIDE · VINT TECHNOLOGIES

ISO 42001: certify or not?



A need-assessment guide to AI governance.

A clear way to make a well-founded decision, even if your company is not an IT company.

Vint

WHO THIS GUIDE IS FOR

A guide for leadership, not just IT

AI is coming to the daily work of every industry. This guide helps leadership decide whether the company needs AI governance in line with ISO 42001, and a certificate. No IT background required.

It answers three questions:

- What is ISO 42001, and what does a certificate prove?
- Is it worth pursuing in our company?
- How is the decision made, and where do we start?

CONTENTS

How the guide progresses

01 **Starting point**
Who leads AI use, and what the standard is

02 **Assessment**
Benefits, limits, regulation and risks

03 **Decision**
Readiness check and three options

04 **In practice**
First steps



Vint

SUMMARY

Decide first, implement after

Good AI governance is the goal. Certification is one possible way to demonstrate it.

- Decide separately whether you need better AI governance and whether you need an independent certificate for it
- Start from the current state, not from documents
- Build in phases, so cost and risk stay under control

A certificate is not a business benefit. The benefit comes from what you improve.

Vint

01

PART 1

Starting point

AI is already in use. Does it have a leader?

STARTING POINT

AI is in use, but who leads it?

AI often enters companies on the initiative of individual employees. That is a good start. As use grows, you need shared principles for tool use, risk assessment, procurement and responsibilities.

The problem often shows only at a decision point: who approves a new use, who handles the risk, and who steps in when something goes wrong?

At the same time, customers increasingly expect evidence that the use of AI is under control.

If the answers cannot be found, the issue is not technology but leadership.

THE STANDARD

ISO 42001 is a management system for AI

ISO/IEC 42001 is an international standard published in 2023. It describes how an organization leads its use of AI: objectives, responsibilities, risk management, monitoring and improvement.

It belongs to the same family as ISO 9001 (quality) and ISO 27001 (information security). The idea is the same: agreed ways of working whose effectiveness can be demonstrated.

The standard does not say which AI you may use, but how its use is led.

BASIC GLOSSARY

Six terms worth knowing

Term	In plain language
Management system	Agreed objectives, responsibilities and ways of working that guide the work
Certification	An independent party checks that the management system meets the requirements of the standard
Gap analysis	A comparison: where current practice is already enough and what is missing
Risk-based	The bigger the risk, the stronger the safeguards
Audit	A systematic check that the system works in practice
AI Act	The EU law on the use of AI. A different thing from the standard

LIMITS

What a certificate proves and what it does not

Proves

- The management system meets the requirements of the standard
- Responsibilities, risk management and monitoring are defined
- There is evidence, assessed by an independent party, that the practices work

Does not prove

- That an individual AI model is error-free or safe
- That all legal requirements are met automatically
- That responsibility for leading AI passes to the auditor or a consultant

Vint

TWO DECISIONS

Better governance and a certificate are separate decisions

1

Do we need better AI governance?

Responsibilities, risks and shared ground rules. The answer can be yes even if a certificate is not yet relevant.

2

Do we need an independent certificate for it?

External evidence of governance for customers and other stakeholders. This is decided separately.

Vint

02

PART 2

Assessment

Benefits, limits, regulation and risks.

BENEFITS

Five reasons to consider certification

- Evidence of governance for customer and supplier discussions
- Responsibilities for AI become clearer
- Risk handling becomes repeatable
- Decisions and monitoring are more transparent
- Improvement does not depend on a single project

Choose first the benefit you are after. Set a measurable goal for it.

FIT

When certification is worth it and when it is not

Justified

- AI is central to the business or customer deliveries
- Customers require reliable evidence
- There are many internal processes, and AI can significantly improve knowledge work
- Small size alone is no reason to give up

Not yet

- Use is limited and the business case is weak
- Basic governance is missing
- There is no time for maintenance
- First build the prerequisites for governance

REGULATION

The standard and the AI Act are different things

Source of the requirement	What it means
Legal obligations	For example the EU AI Act. Clarified use case by use case and according to the organization's role.
Customer and contract requirements	Evidence the customer requires that the use of AI is under control.
Own governance goals	The company's own intent: clear responsibilities, managed risks, shared ways of working.

A requirements map keeps actions that arise for different reasons separate. The standard supports building governance, but does not by itself show that the law is met. This guide is not legal advice. Always check the currency of regulation separately.

Vint

HEAD START

ISO 27001 gives a good starting point, not a ready solution

Already works

- Policies and objectives
- Roles and responsibilities
- Risk-based control
- Internal audits and management reviews
- Continual improvement

New in AI

- Impact on people
- Transparency
- Human oversight
- Defining intended uses
- The AI system lifecycle

Make two lists. That way you do not build two disconnected systems.

Vint

RISKS

The bigger the risk, the stronger the safeguards

Not all use of AI is treated the same way. Governance is scaled to risk: the greater the risk, the stronger the safeguards and the more detailed the procedures.

Risks are identified and anticipated in advance. Procedures are agreed in case they materialize.

Public and fast-evolving AI tools need particular attention: where data is stored, how it is protected, and how confidential information is kept from outside parties. It must also be possible to remove data from external environments.

TOOL EVALUATION

A new tool is assessed with a shared model

1

Approve

The tool is approved for production use when the assessed risk is acceptable.

2

Restrict

The tool is allowed for internal use only.

3

Reject

The risk is too high, so the tool is not adopted.

Vint

PROJECT FLOW

A certification project proceeds in four phases

1

Current state and direction

Gap analysis: are we ready, and would certification bring real value?

2

Risk level

Choose the appropriate level of control according to risk.

3

Into own processes

AI requirements are linked to existing processes.

4

Completed in phases

Internal audits verify that it works before the certification audit.

Vint

COST AND SCHEDULE

An exact price requires knowing the current state

Cost is not only the certification body's invoice. It includes your own work, external support and maintenance.

What affects the workload:

- number and variety of use cases
- organizational structure and documentation
- a possible ISO 27001 foundation
- staff time to participate

Phasing limits financial risk and leaves room to change direction.

03

PART 3

Decision

A readiness check and three options.

Vint

READINESS CHECK

Is your company ready for the project?

Question	Yes	Partly	No
1 Why is certification being pursued?	○	○	○
2 Are the main use cases and their owners known?	○	○	○
3 Are management support and decision-making agreed?	○	○	○
4 Is the basic structure of risk management and documentation in use?	○	○	○
5 Is there time for later maintenance too?	○	○	○

Several "no" answers do not mean the standard is the wrong choice. They mean the first phase is building readiness.

Vint

BASIS FOR THE DECISION

Five things the decision rests on

- The importance of AI to the business
- Stakeholder expectations
- Risks and impacts
- The current state of governance
- Benefits relative to total cost

Make the choice deliberately. Responsibility for leading AI cannot be outsourced to an audit or a consultant.

OPTIONS

Three ways forward



A: Certification readiness

Build governance so that you can proceed to certification.



B: Governance first

Develop governance in line with ISO 42001 without an immediate certification goal.



C: A limited model

Build a light governance model that fits the business and reassess the need later.

Vint

BENEFIT IN DAILY WORK

The benefit shows as smoother customer projects

Clearer responsibilities, risk assessment and ways of working. You see better where and how AI is used.

- Fewer surprises in customer projects, because risks are recorded and prepared for
- A way of responding to a deviation is already agreed
- Decision-making power and responsibility stay with people

Certification is not the end point. The results are put to active use.

START THIS WEEK

Five steps for the first week

- Record which AI tools your company already uses
- Name an owner for AI governance
- Record what certification is meant to achieve, and for whom
- Go through the five readiness questions in the management team
- Agree whether to do a limited gap analysis

A small first step is enough.

HOW VINT HELPS

We help you choose the right path

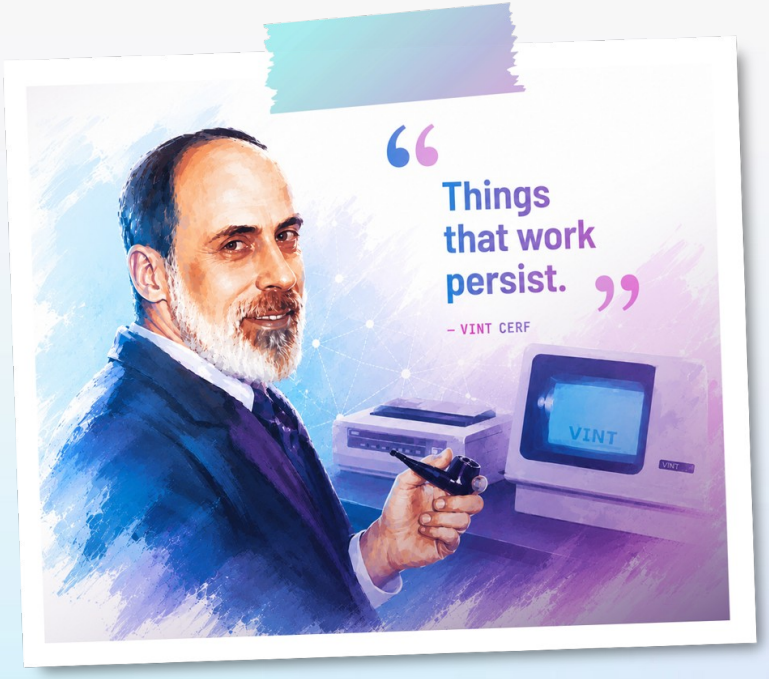
We help assess the current state, choose a suitable approach and put AI governance into practice. We have built an ISO 42001 management system for, among others, Siili Solutions Oyj.

A successful project requires expertise in management systems, data protection, risk management, AI and technology at the same time. We combine the requirements of the standard with the technology in use and your own processes.

We start with a gap analysis.

The result is an auditable system that also works in daily operations.

Vint



VINT TECHNOLOGIES

Thank you

Start with one step: map your current AI use and agree responsibilities. More information: vint.tech

Vint