ISO 42001 for Growing Companies:

A practical reference for companies using, developing or deploying AI

fortifai

What ISO 42001 Is and Why It Matters Now

ISO 42001 is the world's first international standard for AI Management Systems (AIMS). Published in December 2023 by the International Organisation for Standardisation, it establishes the requirements for how organisations develop, deploy, and govern AI systems responsibly — with documented controls, clear accountability, and auditable evidence.

The standard applies to any organisation that develops AI systems, deploys AI systems built by others, or both. Given how rapidly AI tools have been integrated into products and operations across every sector, that covers the vast majority of growing tech companies today.

First — EU AI Act Urgency

The EU AI Act entered into force in August 2024 with a phased implementation timeline. ISO 42001 is explicitly positioned as the governance framework that supports EU AI Act compliance — making certification a credible fast track to regulatory readiness.

Second — Enterprise Procurement

Enterprise procurement teams are already asking AI governance questions in vendor security reviews. ISO 42001 gives you a documented, internationally recognised answer.

Third — Board-Level AI Risk

AI risk is now a board-level topic. The absence of a documented AI governance framework is increasingly a due diligence red flag for investors and acquirers.

ISO 42001 and the EU AI Act — how they connect

The EU AI Act classifies AI systems by risk level — unacceptable, high, limited, and minimal — and imposes obligations on both providers (those who develop or place AI systems on the market) and deployers (those who use AI systems in their operations). ISO 42001 provides the governance infrastructure that satisfies many of the Act's documentation, risk assessment, and oversight requirements. They are complementary rather than duplicative — the Act defines the regulatory obligation, ISO 42001 provides the management system to meet it.

fortifai

Who ISO 42001 Applies To

ISO 42001 is relevant to three types of organisation:

AI Developers

Companies building AI models, training data pipelines, or developing AI-powered features. If you have an ML team or use foundation models to build your product, you are an AI developer under this standard.

AI Deployers

Companies integrating third-party AI tools into their product or operations. Using OpenAI, Anthropic, Google Gemini, Microsoft Copilot, or any other AI service in a way that affects your customers makes you an AI deployer with governance obligations.

Both

Most growing tech companies sit here. You use third-party AI in your product and may also fine-tune models or build proprietary AI features on top of foundation models.

The EU AI Act adds a supply chain dimension that mirrors NIS2's supply chain pull-in. If you supply AI-enabled products to regulated sectors — financial services, healthcare, critical infrastructure, public sector — your customers' AI Act obligations are already flowing into your vendor relationships. Procurement teams at large European companies are adding AI governance requirements to supplier agreements now.

What ISO 42001 Requires From You as Leadership

ISO 42001 requires top management to approve the AI policy, lead management reviews, ensure the AIMS has adequate resources, and be accountable for AI risk decisions. This is not a standard that can be fully delegated to an engineering or data science team.

These are the key approvals ISO 42001 requires from executive leadership:

What You're Signing or Owning	When	What the Auditor Checks
AI Policy	Before certification, reviewed annually	Signed version, approval date, version history, top management sign-off
AIMS Scope Document	Start of implementation	Which AI systems and use cases are in scope, rationale for exclusions
AI Risk Assessment Methodology	Before assessments begin	Documented approach, consistent application, signed off
AI System Risk Register	Before controls implemented, updated ongoing	Each AI system risk-scored, treatment decisions documented, owner named
AI Impact Assessments	For high-risk AI applications	Documented assessment, sign-off, evidence of review
Supplier AI Governance Policy	Before certification	Vendor inventory, AI-specific questionnaires, contractual requirements
Management Review	Annually minimum	Minutes, decisions, action items, resource commitments, top management sign-off
Incident and Near-Miss Log Sign-off	Following any AI-related incident	Investigation outputs, corrective actions, named approver

The AI impact assessment is the sign-off most leaders underestimate. For any AI application that could meaningfully affect people — hiring decisions, credit assessments, customer communications, content moderation — ISO 42001 requires a documented impact assessment covering bias risk, transparency obligations, human oversight mechanisms, and corrective action procedures. These assessments require executive sign-off and must be maintained as the AI system evolves.

What ISO 42001 Looks Like in Practice

For SaaS and Digital Companies Using Third-Party AI

AI System Inventory

The first requirement is knowing what AI you actually use. Most companies are surprised by how many AI-dependent tools and integrations are in their stack when they actually map it. Every AI system that touches customer data, influences product outputs, or affects business decisions needs to be inventoried, classified by risk level, and governed accordingly.

Third-Party AI Governance

Using a foundation model API doesn't transfer the governance obligation to the model provider. Your organisation is responsible for how that AI is used in your product, what safeguards are in place, how outputs are monitored, and what happens when the AI behaves unexpectedly. ISO 42001 requires documented policies for how you select, assess, and oversee third-party AI providers.

Human Oversight Mechanisms

For any AI-influenced decision that matters — customer-facing recommendations, automated workflows, content generation — ISO 42001 requires documented human oversight. Who reviews AI outputs? What are the escalation thresholds? How are errors identified and corrected? These need to be written down and auditable.

Transparency and Explainability

Where AI influences outcomes for your customers, ISO 42001 requires documented transparency practices — how customers are informed that AI is involved, how decisions can be explained, and how customers can challenge AI-influenced outcomes. This directly overlaps with EU AI Act obligations for deployers.

Data Governance for AI

The data used to train, fine-tune, or prompt AI systems carries its own governance requirements — particularly around bias, representativeness, and GDPR compliance. ISO 42001 requires documented data governance practices for AI-specific data handling.

fortifai

For Companies Developing AI Systems

→ ### Model Development Governance

Documented development lifecycle controls — training data management, model validation, bias testing, performance monitoring, and version control. Each stage requires documented outputs and sign-offs.

→ ### Model Risk Assessment

For each model in production, a documented risk assessment covering potential failure modes, impact on affected parties, bias risks, and performance degradation scenarios. Named owners for each risk.

→ ### Model Monitoring and Drift Detection

Ongoing monitoring of model performance in production, with documented thresholds for when retraining or human review is triggered. Evidence that monitoring is operating must be maintained continuously.

→ ### Incident Response for AI Failures

A documented procedure for responding to AI system failures, unexpected outputs, or bias incidents — including investigation process, customer notification where required, and corrective action with evidence of closure.

High-Level Implementation Checklist

1

Phase 1 — Foundations and AI Inventory

- Define AIMS scope — which AI systems, use cases, and business units are in scope
- Appoint AI governance owner — with executive sponsor named at board level
- Build complete AI system inventory — every AI tool, model, API, and integration used in product or operations
- Classify each AI system by risk level using EU AI Act categories as a guide
- Complete gap assessment against ISO 42001:2023
- Select certification body and confirm audit dates
- Set up document management system with version control

2

Phase 2 — Risk Assessment

- Document AI risk assessment methodology
- Complete risk assessment for each in-scope AI system
- Identify bias risks, transparency obligations, and human oversight requirements for each system
- Complete AI impact assessments for high-risk applications
- Leadership signs off on risk register and impact assessment outputs
- Document residual risk acceptance with named executive owner

3

Phase 3 — Policy and Governance Documentation

- Draft and approve AI Policy — top management sign-off required
- Draft supporting policies: Third-Party AI Governance, Data Governance for AI, Human Oversight Policy, AI Incident Response, Transparency and Explainability Policy, AI Development Lifecycle Policy (if applicable)
- Document supplier AI governance requirements and update vendor agreements
- Build AI system transparency documentation for customer-facing applications
- Obtain formal sign-off from named approver for each document

4

Phase 4 — Control Implementation

- Implement human oversight mechanisms for all high-risk AI applications
- Deploy AI system monitoring — performance tracking, drift detection, bias monitoring
- Complete third-party AI provider assessments — send governance questionnaires, document responses
- Implement AI incident reporting system
- Deliver AI governance awareness training to all relevant staff — record completions
- Review and update data governance practices for AI-specific data handling
- For AI developers: implement model validation, bias testing, and version control procedures

5

Phase 5 — Internal Audit

- Conduct internal audit — auditor must be independent of AI development and deployment activities
- Produce internal audit report with findings rated by severity
- Assign corrective actions with owners and due dates
- Close corrective actions and document evidence of closure

6

Phase 6 — Management Review and Certification

- Conduct management review covering: AIMS performance, audit results, AI incident trends, EU AI Act regulatory developments, resource requirements, objectives for coming period
- Document all outputs — decisions, actions, resource commitments, top management sign-off
- Compile full evidence file — every required document, current and retrievable
- Stage 1 audit — document review by certification body
- Remediate any Stage 1 findings
- Stage 2 audit — system walkthroughs, staff interviews, evidence testing
- Certificate issued — surveillance audits follow annually

Manual vs. Automated: What Good Looks Like

ISO 42001 Requires	Manual Reality	With Governance Automation
AI system inventory with risk classifications	Spreadsheet, incomplete, not updated when new tools added	Live register with tracked classifications and review dates
AI impact assessments with sign-offs	Document created once, never updated as system evolves	Version-controlled with change history and re-approval triggers
Third-party AI provider assessments	Questionnaire sent once, response filed, never revisited	Recurring workflow tied to contract renewal and material changes
AI incident log with investigation outputs	Email thread, inconsistent, no trend analysis	Structured log with status tracking and management reporting
Management review with documented outputs	Meeting happened, notes dispersed across email	Structured review with timestamped sign-off and action log
Audit evidence on request	Week-long scramble across engineering, product, and compliance	Retrievable in minutes, maintained continuously

AI systems evolve continuously — new model versions, new use cases, new integrations. Manual governance frameworks that were accurate at certification become stale within months. Companies that treat AI governance as a continuous workflow rather than a point-in-time project enter surveillance audits and regulatory reviews with current, accurate evidence.

Multi-Framework Advantage

ISO 42001 has the strongest overlap with other frameworks of any standard in this set:

ISO 42001 + ISO 27001

Information security and AI governance share data governance, access control, incident management, and supplier oversight workflows. The evidence base is largely shared.

ISO 42001 + NIS2

AI systems in scope of NIS2 (particularly for essential and important entities using AI in operational technology) require governance that satisfies both frameworks. The risk assessment and incident reporting workflows overlap directly.

ISO 42001 + GDPR

AI systems processing personal data require GDPR-compliant data governance. The AI impact assessment under ISO 42001 and the Data Protection Impact Assessment under GDPR address overlapping questions. A unified workflow handles both.

ISO 42001 + EU AI Act

As noted throughout, these are designed to work together. ISO 42001 certification provides documented evidence for many EU AI Act compliance obligations, particularly around risk management, transparency, and human oversight.

For companies managing multiple frameworks, Fortifai's governance platform handles all of them from a single evidence base — which means each additional framework after the first costs a fraction of the original.

How Fortifai Supports This

Fortifai is governance workflow infrastructure built for growing companies. The platform automates the three workflows ISO 42001 requires:

Sign-off Routing and Tracking

For AI policy approvals and impact assessment sign-offs

Disclosure Document Management

For AI system transparency documentation and regulatory submissions

Information Request Handling

For third-party AI provider assessments and audit evidence requests — pre-configured for ISO 42001 with templates ready on day one

The same platform supports ISO 27001, SOC 2, NIS2, ISO 45001, GDPR, and ESG frameworks simultaneously. For tech companies managing multiple compliance obligations across a growing AI-enabled product stack, the governance workflows overlap significantly and the evidence base is shared.

Used by teams at **Cognite**, **Aker BioMarine**, and **Telenor**.

> **Book a 30-minute walkthrough at fortifai.co**

fortifai