ISO/IEC 42001

Governance Overview

What is ISO/IEC 42001?

ISO/IEC 42001 is a joint publication of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Officially published in 2023, it is the world's first international management system standard dedicated to Artificial Intelligence Management Systems (AIMS).

ISO/IEC 42001 provides a structured framework for governing the secure, fair, transparent, and responsible use of AI across its lifecycle. As AI adoption accelerates across industries, ISO/IEC 42001 is rapidly becoming a recognized benchmark for demonstrating trustworthy AI practices in both domestic and international business environments.

While ISO/IEC 42001 is not a legal requirement, it is increasingly expected by regulators, customers, partners, and investors. Achieving alignment requires establishing governance processes, managing AI-specific risks, and regularly evaluating the effectiveness of the AI Management System. Working with an experienced advisory partner helps organizations design, implement, and maintain an AIMS that is scalable, auditable, and sustainable.

Why Choose ISO/IEC 42001

Organizations that pursue ISO/IEC 42001 demonstrate a clear commitment to responsible and accountable AI practices. The standard helps organizations address key AI risks such as algorithmic bias, transparency, explainability, continuous learning, and ethical use.

ISO/IEC 42001 provides a globally recognized framework for embedding AI governance into organizational decision-making and operations. Independent certification signals to stakeholders that AI systems are governed through defined accountability, risk management, and continuous improvement processes.

ISO/IEC 42001 vs. ISO/IEC 27001

While ISO/IEC 42001 shares a common management system structure with ISO/IEC 27001, it specifically addresses risks unique to AI systems. These include algorithmic bias, explainability, continuous learning, human oversight, and ethical considerations.

ISO/IEC 42001 introduces AI-specific requirements such as AI system impact assessments, governance of AI lifecycle risks, and accountability mechanisms that extend beyond traditional information security controls.

ISO 27001

ISO 42001

Key Clauses of ISO/IEC 42001

The most critical clauses for achieving conformity are Clauses 5 through 10.

Clause 5 | Leadership
Leadership commitment is required to establish AI governance policies, assign accountability, allocate resources, and embed AI management responsibilities across the organization.

Clause 6 | Planning
Organizations must identify AI-related risks and opportunities, define objectives for the AI Management System, and establish action plans to address those risks throughout the AI lifecycle.

Clause 7 | Support
Adequate resources, defined competencies, training programs, and communication processes must be in place to support effective AI governance and AIMS operation.

Clause 8 | Operation
AI systems must be operated and controlled through defined lifecycle processes, including risk management activities and AI impact assessments, to ensure systems perform as intended.

Clause 9 | Performance Evaluation
Organizations are required to monitor, measure, and evaluate the effectiveness of their AIMS through internal audits, reviews, and performance metrics, including coordination with broader IT and cybersecurity activities.

Clause 10 | Improvement
Organizations must commit to continual improvement by addressing nonconformities, implementing corrective actions, and adapting governance practices as AI risks and use cases evolve.

The RSI Security 5-Step ISO/IEC 42001 Certification Process

ISO/IEC 42001 alignment is a structured, multi-phase journey. Organizations establish an Artificial Intelligence Management System (AIMS) to manage AI governance risks and demonstrate conformity with ISO/IEC 42001 requirements.

Governance Alignment

Defined scope of the AI Management System, AI system inventory, governance roles and responsibilities, and documented management system policies and procedures.

Stage 1 Audit

Evaluation of AIMS documentation, governance structure, and scope to confirm management system readiness for the certification audit.

Stage 2 Audit

Assessment of governance processes, operational controls, and supporting evidence to verify conformity with ISO/IEC 42001 requirements.

Certification Decision

Independent certification review of audit results, nonconformity resolution, and confirmation that the AIMS meets ISO/IEC 42001 requirements.

Surveillance Audits

Periodic assessments verify continued conformity, evaluate management system performance, and confirm ongoing governance effectiveness.

RSI

Ready to Take the Next Step?

RSI Security provides independent certification and assessment services for ISO-aligned AI Management Systems. Our assessments evaluate governance processes, risk management practices, and lifecycle controls to determine conformity with ISO/IEC 42001 requirements.

858.999.3030 | info@rsisecurity.com | rsisecurity.com