KPMG

ISO/IEC 42001 Certification: The Global Standard for AI Management Systems (AIMS)

How to establish trust, transparency and control in artificial intelligence governance

May 2025

KPMG. Make the Difference.

Executive Summary

In response to growing concerns about ethics, bias, privacy, and transparency, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have introduced.

ISO/IEC 42001

the first international standard for Artificial Intelligence Management Systems (AIMS).

This paper provides a structured overview of the standard:

- Its core components.
- Benefits.
- Associated regulatory framework.
- Guidance on implementation and certification.

It serves as a practical resource for quality management professionals and organizations seeking to **integrate and manage AI responsibly.**

KPMG Switzerland certification body is one of the world's **leading Conformity Assessment Bodies (CABs)** providing certifications for AI management systems (AIMS) based on ISO/IEC 42001.

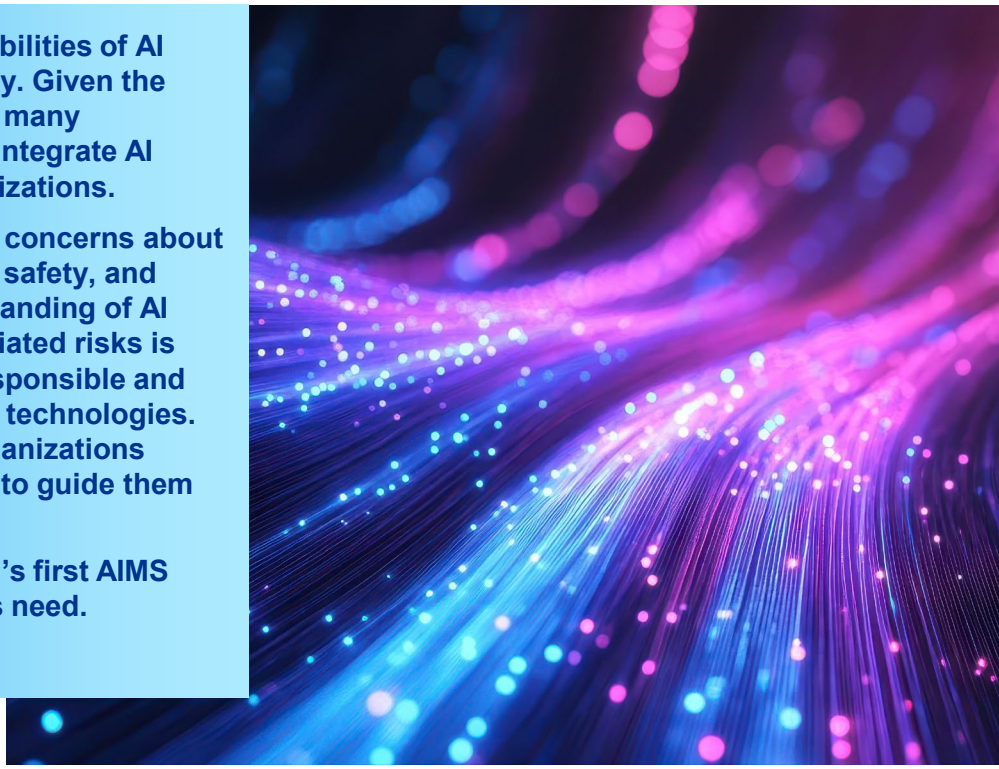
Contents

ISO/IEC 42001 – The world's first AIMS standard

In recent years, the capabilities of AI have grown exponentially. Given the immense potential of AI, many companies are eager to integrate AI systems into their organizations.

However, there are deep concerns about privacy, bias, inequality, safety, and security. A deep understanding of AI systems and their associated risks is needed to ensure the responsible and sustainable use of these technologies. Now more than ever, organizations today need a framework to guide them on their AI journey.

ISO/IEC 42001, the world's first AIMS standard, addresses this need.



About ISO/IEC 42001

ISO/IEC 42001:2023-12 is a **globally recognized standard** that provides guidelines for the governance and management of AI technologies. It provides a systematic approach to address the challenges associated with AI implementation in a recognized management system framework that covers areas such as ethics, accountability, transparency and data privacy. Designed to oversee the various aspects of AI, it provides an integrated approach to managing AI projects, from risk assessment to effective management of those risks.

By establishing clear guidelines for AI governance, ISO/IEC 42001 promotes an environment conducive to innovation.

It provides a framework for organizations to navigate the complex landscape of AI development and encourages the adoption of best practices that enhance the reliability and security of AI systems. This, in turn, fosters trust among stakeholders and facilitates the responsible use of AI technologies.

ISO/IEC 42001 – The world's first AIMS standard (cont.)

Core components of the ISO/IEC 42001 standard

The ISO/IEC 42001 standard is structured around several core components that are essential for the effective management of AI systems:

- **AI Management Systems (AIMS):** Integration with organizational processes to ensure continuous improvement and alignment with other ISO standards.
- **AI Risk Assessment:** A systematic approach to identifying and mitigating risks throughout the AI lifecycle.
- **AI Impact Assessment:** Evaluation of the impact of AI on individuals and society.
- **Data Protection and AI Security:** Focus on complying with privacy laws and securing AI systems against threats.

An **AI Management System (AIMS)** is a structured framework designed to oversee and manage the implementation, operation and risks associated with AI technologies within an organization.

AIMS integrates governance, compliance, risk management, and ethical oversight to ensure that AI initiatives are aligned with organizational goals and regulatory standards, such as those outlined in frameworks such as **NIST, ISO/IEC 42001**, and the European Union's **EU AI Act.**

Benefits of certification to ISO/IEC 42001

The ISO/IEC 42001 standard sets a global benchmark for AIMS and defines a structured framework to help organizations integrate AI into their operations in an ethical and secure manner. The standard ensures compliance with regulatory requirements and best practices while mitigating AI-related risks.

The certification process establishes, implements, maintains, and enhances AIMS within organizations. It also ensures the **ongoing monitoring** and governance of AI operations.

ISO/IEC 42001 certification helps organizations:

- Build transparent, trustworthy and ethical AI systems.
- Meet compliance obligations such as the EU AI Act.
- Improve risk management and accountability.
- Increase customer and stakeholder confidence.
- Align AI governance with strategic business goals.

ISO/IEC 42001 is designed to help organizations and society as a whole derive maximum benefit from the use of AI in a secure and efficient manner.

Organizational benefits include:

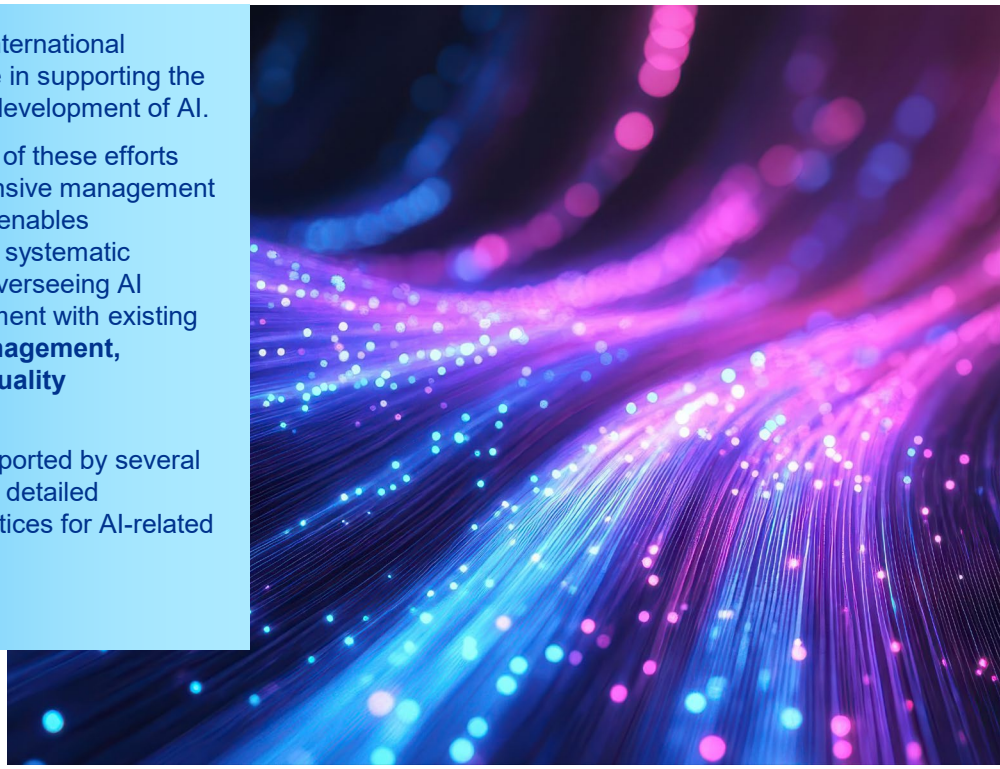
- Improved quality and reliability of AI systems.
- Improved operational efficiency.
- Reduced development and compliance costs.
- Strengthened governance and ethical oversight.

Overview of certification standards and international regulations

Certification standards and international regulations play a pivotal role in supporting the ethical, reliable, and secure development of AI.

ISO/IEC 42001 is at the core of these efforts and establishes a comprehensive management system for AI. This standard enables organizations to implement a systematic approach to governing and overseeing AI technologies, ensuring alignment with existing ISO frameworks for **risk management, information security,** and **quality management.**

ISO/IEC 42001 is further supported by several technical reports that provide detailed methodologies and best practices for AI-related challenges.



ISO/IEC Technical Reports supporting AIMS:

ISO/IEC TR 24027:

Methods for assessing bias and fairness in AI systems, along with potential mitigation strategies.

ISO/IEC TR 24028:

Overview of AI trustworthiness and suggestions for improving it.

ISO/IEC TR 24029:

Statistical, formal and empirical approaches to evaluating the robustness of neural networks, with a focus on resilience in AI models.

In addition, several other standards provide essential context and support for organizations seeking AIMS certification.

Overview of certification standards and international regulations (cont.)

Other key standards for AI certification:

ISO/IEC 23894:

Guidance for managing AI risks through both a framework and risk management processes.

ISO/IEC 22989:

Standardized vocabulary and basic AI concepts to provide a common understanding among stakeholders.

ISO/IEC 5259:

A comprehensive framework for assessing data quality in machine learning, which is critical to the performance and fairness of AI systems.

ISO/IEC 31000:

A general risk management framework that can be used to design and implement appropriate control measures for AIMS.

In addition to ISO standards, organizations must also align with rapidly evolving regulatory frameworks:

- The EU AI Act (effective from 1 February 2025) is the world's first binding legal framework for AI. It introduces a risk-based classification of AI systems and mandates compliance with ethical and security requirements.
- In the Unites States, the NIST AI Risk Management Framework continues to guide federal and private-sector AI governance through robust technical and procedural standards.

Together, ISO/IEC 42001 and these regulatory frameworks provide a **global foundation for responsible AI**, ensuring organizations are not only technically compliant but also ethically and societally aligned.

Supporting norms and standards for AI certification

ISO Guide 73
Implementation of risk manage-ment for organization developing, providing or using AI products, systems and services

ISO Guide 73
Risk and opportunities within the AI management systems

ISO Guide 73
Risk and control measurement which modifies risks

ISO Guide 73
Risk and effect of uncertainty

Adressing Operational Risk Management, ISO/IEC 42001: **chapt. 6 & chapt. 8**

ISO/IEC 38500
Governing body

Understanding the organization and scope, ISO/IEC 42001: **chapt. 4**

ISO/IEC 27001
Information Security in terms of the preservation of confidentiality, integrity and availability of information

Leadership, Policies and responsibilities, ISO/IEC 42001: **chapt. 5**

ISO/IEC 38507
Alignment with other organizations policies

ISO/IEC 19944-1
Categories of data

ISO/IEC 5259-1
Data Quality

Implementation guidance for AI controls and continual improvement, ISO/IEC 42001: **chapt. 10 & Annex B (normative)**

ISO/IEC 23053
Tooling resources

ISO/IEC TR 24368
Ethical & social concerns

Addressing societal impacts of AI systems and resources for AI systems, ISO/IEC 42001: **Annex B (normative)**

ISO/IEC 22989
AI Life cycle stage and model

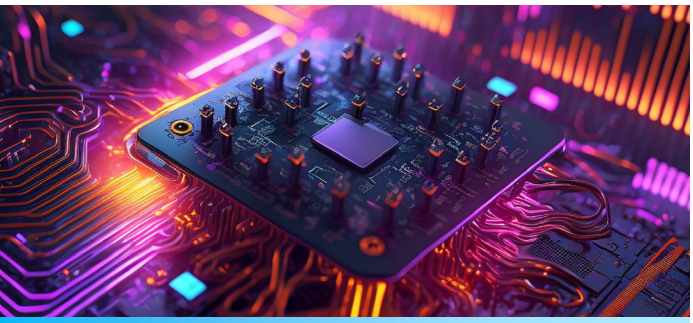
Objectives for responsible development of AI system, ISO/IEC 42001: **Annex B (normative)**

ISO/IEC TR 24029-1
Assessment of the robustness of neural networks

ISO/IEC TR 24028
Trustworthiness in artificial intelligence

ISO/IEC TR 24027
Bias in AI systems and AI aided decision making

Technical software norms for the trust of AI systems, referred to ISO/IEC 42001



While ISO/IEC 42001 provides the core framework for managing AI responsibly, several complementary ISO and IEC standards support the design, implementation, and continuous improvement of a certifiable AI Management System (AIMS).

These supporting standards are not mandatory for certification but provide practical tools and structured guidance for specific focus areas such as risk, security, data, and ethics.

Risk management and uncertainty

Risk in AI is often defined in terms of **potential events and their consequences**. To manage this effectively, organizations need a consistent framework for identifying, assessing and controlling risks – especially those unique to AI technologies:

ISO Guide 73:

Establishes consistent risk terminology and concepts to understand and manage uncertainty – making it a helpful reference when building an AIMS.

ISO/IEC 31000:

Provides a broad, adaptable framework for enterprise risk management that can be tailored to AI contexts and incorporated into an AIMS.

ISO/IEC 42001 requires all identified AI risks to be formally documented and linked to specific **control objectives**. These should be included in a **Statement of Applicability (SoA)** – a critical component of certification.

AI-Specific risk and organizational policy alignment

AI adds a new layer of complexity to governance, requiring organizations to define their risk appetite and align AI development with overarching business strategies and ethical commitments.

Two key standards support this alignment:

ISO/IEC 23894:

Provides specific guidance on managing risks related to AI products, systems and services throughout their lifecycle.

ISO/IEC 38507:

Supports governing bodies and senior leadership in incorporating AI oversight into corporate governance frameworks.

These standards help ensure that technical risk decisions reflect broader organizational priorities, including compliance, accountability and long-term trustworthiness.

Security & information protection

AI systems are deeply intertwined with sensitive data and critical infrastructure. Ensuring confidentiality, integrity and availability — as well as authenticity, non-repudiation and accountability – is essential.

ISO/IEC 27001:

Establishes a best-practice framework for **Information Security Management Systems (ISMS),** which can be integrated with AIMS to strengthen security controls.

ISO/IEC 42001:

The security-related control objectives in ISO/IEC 42001 are designed to work in harmony with existing ISMS programs, especially in high-risk or regulated industries.

By incorporating proven information security principles, organizations can reduce vulnerabilities and maintain operational resilience.

Data Quality and Classification

Because most AI systems are data-driven, data quality and governance of training and operational data directly affect results. To ensure transparency, fairness and reliability, organizations should adopt structured approaches to data management.

ISO/IEC 5259-1:

Defines methods for assessing and maintaining data quality in machine learning environments.

ISO/IEC 19944-1:

Provides guidance on categorizing and managing shared data, particularly in cloud and cross-border contexts.

Clear data definitions and transparent categorization are essential not only for system performance but also for meeting accountability and auditability requirements under ISO/IEC 42001.

Lifecycle governance and machine learning tools

AI projects often span multiple phases – from design and prototyping to deployment and retirement. Standards that guide end-to-end lifecycle management and development practices ensure that AI systems remain safe, ethical and effective over time.

ISO/IEC 22989:

Supports the development of an adapted AI system lifecycle model, complete with control objectives for each phase.

ISO/IEC 23053:

Provides guidance on tools and workflows in machine learning development, helping operational teams structure their AI processes.

ISO/IEC TR 24368:

Addresses ethical and societal considerations, including human impact, inclusion and fairness.

These standards allow organizations to implement AIMS in a way that is technically rigorous and socially aligned, building trust among stakeholders and end-users alike.

Together, these supporting standards provide the practical backbone for translating ISO/IEC 42001 into an effective, certifiable and future-ready AI governance system.

International risk management frameworks for AI (OECD & NIST)

While ISO/IEC 42001 provides the foundation for AI governance within organizations, a broader perspective is necessary to fully address the ethical, societal and operational risks of AI. Two influential frameworks – from the **Organization for Economic Co-operation and Development (OECD)** and the **U.S. National Institute of Standards and Technology (NIST)** – complement ISO standards by providing **internationally recognized principles** and **risk management models.**

OECD Framework – Socio-technical dimensions of AI risk

The OECD developed a conceptual framework for managing the risks and impacts of AI through a multi-stakeholder, lifecycle-oriented lens. These stakeholders include not only developers and deployers of AI systems, but also policymakers, end-users and society at large.

This framework is intended for use by all AI actors, defined as “those who play an active role in the life cycle of AI systems, including organizations and individuals that deploy or operate AI”.

The OECD classifies AI activities into **five socio-technical dimensions** that affect governance and policy development [OECD (2022) OECD Framework for the Classification of AI systems | OECD Digital Economy Papers:

1. Human and institutional involvement.
2. Data and input characteristics.
3. AI model design and functionality.
4. Deployment context.
5. Expected impacts on society and the environment.

Each dimension supports a holistic approach to understanding where and how AI risk arises — from privacy and bias, to transparency, accountability, and unintended societal consequences.

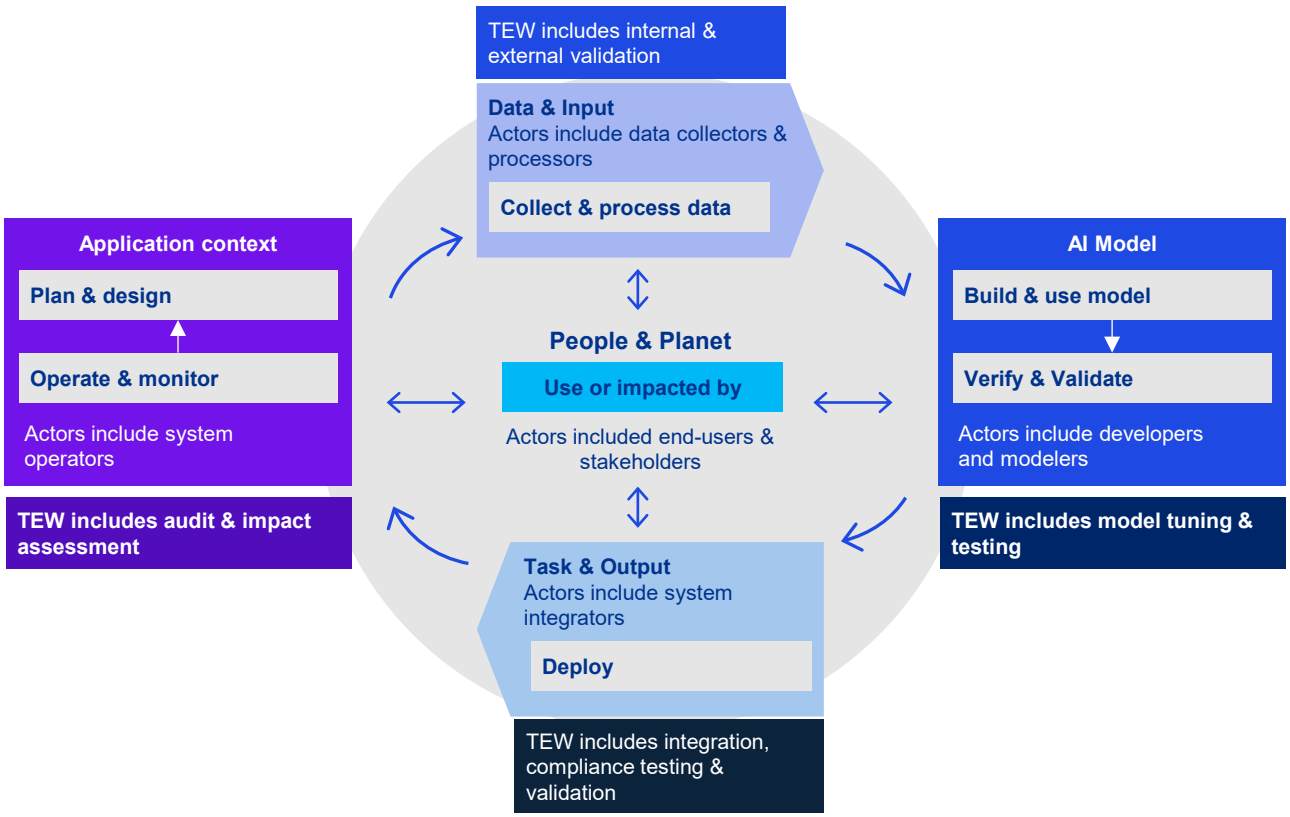
NIST AI Risk Management Framework (RMF)

The NIST AI RMF, developed by the U.S. National Institute of Standards and Technology, provides a structured and technical model for building trustworthy and secure AI systems. It emphasizes that managing AI risk is a shared responsibility across the AI lifecycle and aligns well with ISO/IEC 42001 and other governance standards. A central feature of the NIST framework is TEVV – Test, Evaluation, Verification, and Validation – which helps organizations ensure that AI systems behave as expected, safely and reliably.

Key lifecycle stages emphasized by NIST include:

- **Collect & process data:** Collect and prepare data for training, ensuring accuracy, representativeness and regulatory compliance.
- **Build & use model:** Develop the AI model, train it on data sets and deploy it in real-world environments.
- **Verify & validate:** Test and evaluate the model to ensure it performs as intended and does not exhibit bias, security vulnerabilities or unpredictable behavior.

International risk management frameworks for AI (OECD & NIST) (cont.)



Source: Lifecycle and Key dimensions of an AI System based on the Framework of OECD.

Why these frameworks matter

Both the OECD and NIST frameworks promote a multi-dimensional, risk-aware approach to AI governance. They are particularly valuable for:

- Identifying risks early in the AI lifecycle.
- Engaging diverse stakeholders in AI design and deployment decisions.
- Supporting alignment with legal, ethical and organizational values.
- Enhancing transparency and enabling better auditability of AI systems.

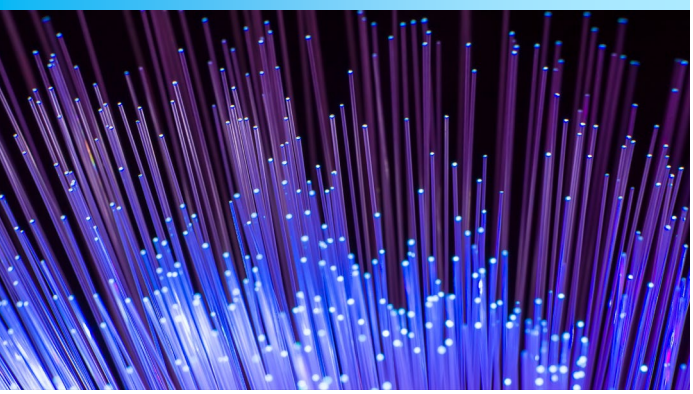
These international perspectives provide **essential context** for organizations seeking to implement ISO/IEC 42001 and demonstrate a commitment to **global best practices in responsible AI.**

Together with ISO/IEC standards, these frameworks help bridge the gap between technical performance and ethical responsibility – a key factor in building trust in AI.

Model validation and Trusted AI

As AI models become more complex and dynamic, understanding how they behave – and whether they can be trusted – becomes increasingly difficult. Organizations face the challenge of not only evaluating performance, but also ensuring that models operate in ways that are **reliable, explainable, secure and fair.**

This is where **model validation** comes in. It is the process of confirming that AI systems work as intended, meeting both **technical requirements** and **ethical expectations.**



KPMG's approach to model validation

KPMG takes a systematic approach to model validation, combining in-house expertise with the support of trusted external partners, such as **LatticeFlow**. This partnership brings in-depth technical expertise and leverages industry-leading validation methodologies – including:

- **White-box testing:** Examining model internals to understand logic and detect bias or blind spots.
- **Grey-box testing:** Combining partial model knowledge with scenario-based validation.
- **Black-box testing:** Testing outputs based on inputs, without access to the model's inner workings.

These methods are tailored to evaluate critical model properties and behaviors across a variety of contexts and use cases.

Key model validation objectives

Robust model validation is essential for ensuring responsible AI. It assesses whether models are:

- **Robust** to adversarial conditions.
- **Predictable** in performance under varying operational environments.
- **Fair** across demographic or contextual variations.
- **Free from bias,** or capable of mitigating unintentional discrimination.
- **Transparent,** with results that can be interpreted and explained.
- **Safe and secure,** especially in high-risk or regulated settings.

Model validation also ensures compliance with both **regulatory obligations** and **internal risk tolerances** – particularly in light of evolving regulatory landscapes such as the **EU AI Act** and **ISO/IEC 42001** requirements.

KPMG's Trusted AI Framework

Test results and model fare not evaluated in isolation. At KPMG, they are interpreted in the broader context of the **Trusted AI Framework** – a proprietary, multi-dimensional governance model developed through global experience and applied in numerous client engagements.

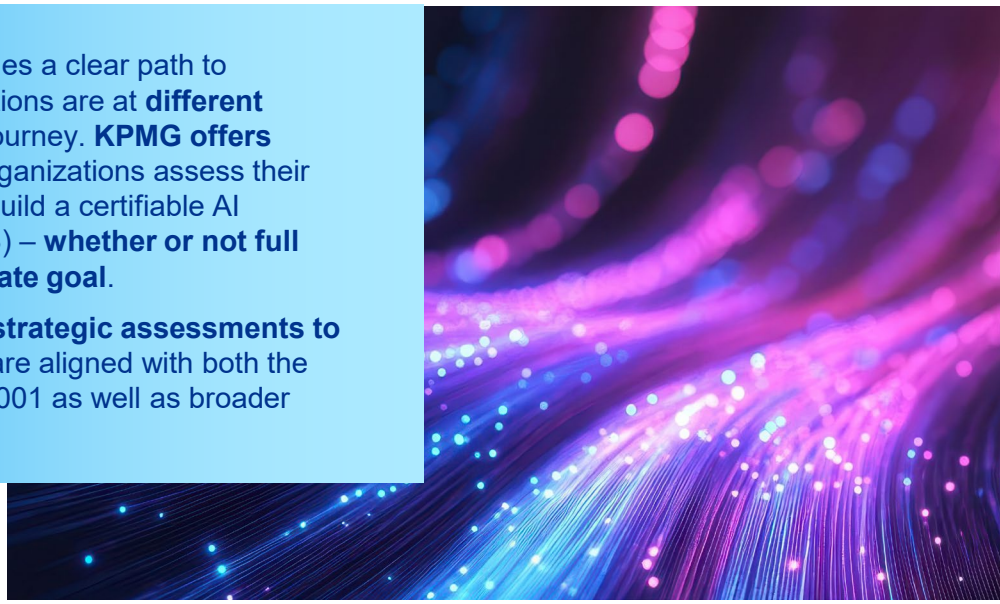
- Ethical alignment.
- Technical robustness.
- Privacy and data protection.
- Human oversight.
- Transparency.
- Accountability.
- Inclusiveness.
- Sustainability.
- Security.
- Explainability.

By applying this holistic lens, organizations can build AI systems that not only perform well but also align with their core values and stakeholder expectations.

Tailored service approach

While ISO/IEC 42001 provides a clear path to certification, many organizations are at **different stages** of their AI maturity journey. **KPMG offers tailored services** to help organizations assess their readiness, close gaps and build a certifiable AI Management System (AIMS) – **whether or not full certification is the immediate goal**.

These services range from **strategic assessments to technical validations** and are aligned with both the requirements of ISO/IEC 42001 as well as broader industry best practices.



ISO/IEC 42001: A Management System (MS) standard

Like other ISO management system standards (e.g. ISO 9001, ISO/IEC 27001), ISO/IEC 42001 is designed to help organizations establish, implement, maintain, and continually improve their internal AI governance systems.

An AIMS is defined as a set of **interrelated, interacting elements** that define:

- AI-specific policies and objectives.
- Risk and impact assessment processes.
- Governance, monitoring, and continuous improvement mechanisms.
- Alignment with legal, ethical, and business requirements.

KPMG supports clients throughout this lifecycle — whether the goal is certification, compliance with emerging regulations (such as the EU AI Act), or building stakeholder trust.

ISO/IEC 42001 was intentionally written as a standard for management systems (MS), intended for organizations wishing to implement an MS and pursue accredited certification for it. Accredited certification to ISO/IEC 42001 means an independent third-party MS certification body has verified that a company's internal MS meets internationally recognized standards (e.g., ISO/IEC 42001).

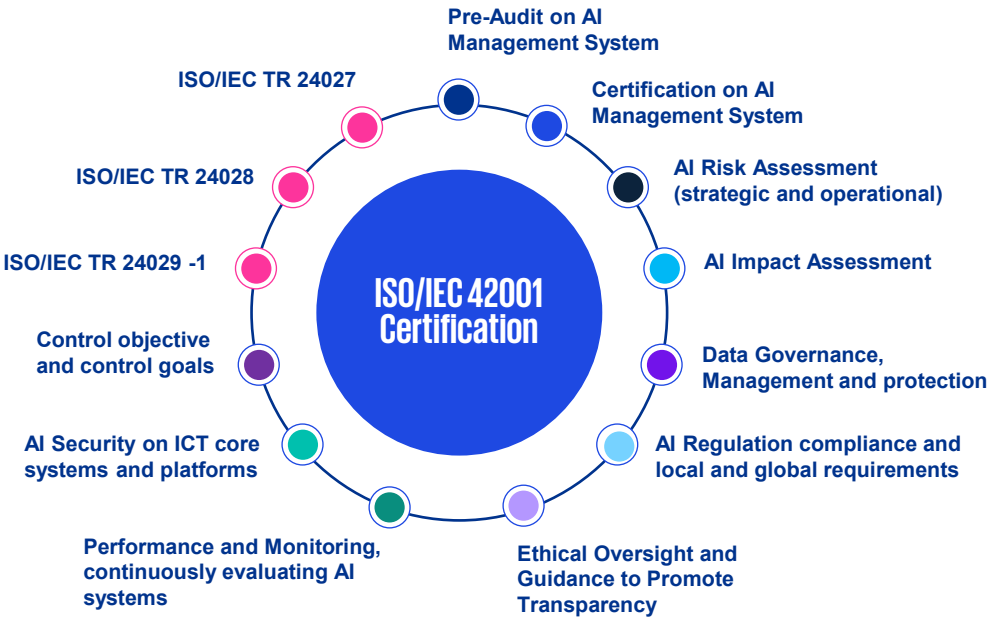
The leading AI standard, ISO/IEC 42001, provides the framework and requirements for organizations to build a responsible, ethical and trustworthy management system, and when coupled with accredited certification, the organization should be able to assure its customers of consistency and effectiveness.

Tailored service approach (cont.)

KPMG's AIMS services

KPMG offers a comprehensive portfolio of services that support organizations in managing and governing their AI systems effectively.

These services encompass various stages of AI management, including pre-audits, full audits, single assessments, and technical model validation. Each service is carefully tailored to meet the specific needs of the organization.



Pre-Audit on AI Management System

A preliminary review to assess the organization's AI management processes, identify gaps, and ensure alignment with certification standards prior to the formal audit.

AI Risk Assessment (strategic and operational)

The process of identifying, assessing, and mitigating risks associated with AI systems, such as bias, security vulnerabilities, or unintended outcomes, to ensure safe and reliable operations.

AI Impact Assessment

Evaluating the potential societal, environmental, and organizational impacts of AI systems to ensure they are aligned with ethical, safety and business objectives.

Data Governance, Management and protection

Implementing policies and processes to ensure data integrity, quality, privacy, and security throughout the AI lifecycle.

AI Regulation compliance and local and global requirements

Ensuring the AI systems adhere to applicable laws, regulations, and standards at both local and international levels to avoid legal risks.

Ethical Oversight and Guidance to Promote Transparency

Establishing ethical frameworks to guide AI development, ensuring fairness, accountability, and transparency while promoting trust in AI systems.

Performance and Monitoring, continuously evaluating AI systems

Continuously evaluating AI systems to ensure they meet performance goals, detect issues and maintain optimal functionality over time.

AI Security on ICT core systems and platforms

Protecting the underlying ICT infrastructure and platforms against cyber threats to ensure the secure operation of AI systems.

Control objective and control goals

Defining clear objectives and measurable targets for AI system governance to ensure compliance, performance, and accountability.

Tailored service approach (cont.)

Strategic & operational focus areas

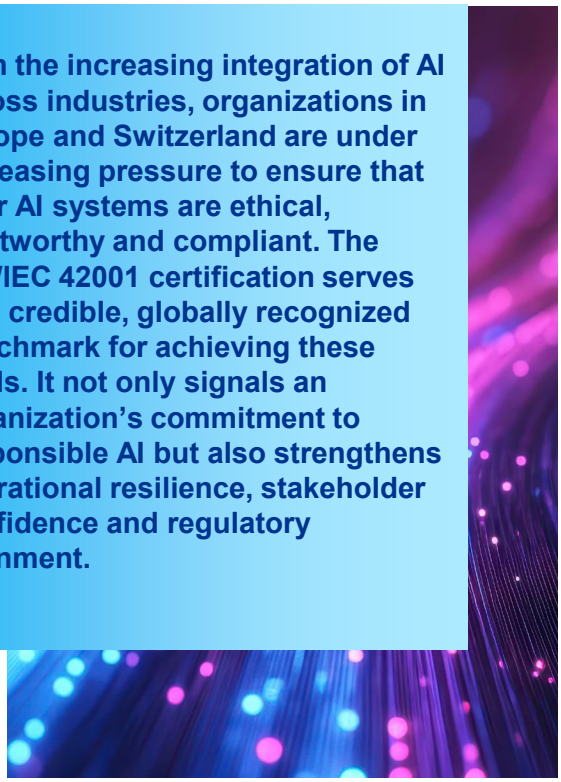
KPMG's services also cover deeper, organization-wide areas of AI governance, including:

- **Strategic risk management:** Identifying and mitigating high-level risks associated with AI, such as data breaches, algorithmic bias, and unethical use. This includes proactive planning to protect sensitive information, ensure fairness in AI decision-making and maintain ethical use of AI.
- **Regulatory compliance:** Ensuring that AI systems comply with industry-specific regulations and global standards. This includes staying abreast of evolving legal requirements, implementing compliance frameworks and conducting regular audits to avoid legal and reputational risks.
- **Operational risk management:** Addressing day-to-day risks in AI implementation to maintain system integrity, reliability, and security. This includes streamlining operational processes, identifying vulnerabilities, and reducing potential disruptions.
- **Ethical Oversight:** Establishing robust guidelines to ensure AI systems operate with transparency, fairness and accountability. This includes defining ethical principles, conducting bias audits and promoting responsible AI governance.
- **Performance monitoring:** Continuously assessing AI models to ensure they remain accurate, efficient and aligned with business objectives. This involves regular evaluations, model retraining and performance benchmarks to enhance AI reliability.
- **Addressing algorithmic bias:** Implementing strategies to detect, prevent and correct biases in AI models. This includes using diverse datasets, fairness-aware algorithms and bias-mitigation techniques to promote equitable outcomes.

Whether your organization is preparing for certification, complying with the EU AI Act or building an internal AI governance model, KPMG's tailored approach provides practical, scalable support at every step of your AI journey.

ISO/IEC 42001:2023 certification in Europe and Switzerland

With the increasing integration of AI across industries, organizations in Europe and Switzerland are under increasing pressure to ensure that their AI systems are ethical, trustworthy and compliant. The ISO/IEC 42001 certification serves as a credible, globally recognized benchmark for achieving these goals. It not only signals an organization's commitment to responsible AI but also strengthens operational resilience, stakeholder confidence and regulatory alignment.



Strategic value of certification

ISO/IEC 42001 provides a management system framework for the governance, deployment and oversight of AI systems. Certification demonstrates that an organization has implemented formalized processes to:

- Identify and mitigate AI-related risks.
- Ensure transparency, security and ethical accountability.
- Comply with legal and regulatory standards, including the upcoming EU AI Act.
- Build stakeholder and customer trust.
- Foster innovation in a controlled and auditable environment.

For organizations operating in or trading with the EU, ISO/IEC 42001 certification can also serve as a **practical basis for demonstrating compliance** with the EU AI Act, which enters into force in February 2025.

Certification landscape in Europe and Switzerland

Interest in ISO/IEC 42001 is growing rapidly across Europe and Switzerland, especially in sectors where AI impacts **critical infrastructure, financial systems, health, public administration or consumer safety.**

Key drivers in the region include:

- Anticipation of **strict regulatory enforcement** under the EU AI Act.
- Increasing focus on **digital trust and AI ethics** by both public institutions and private stakeholders.
- The need for **standardized internal controls** to effectively manage the AI lifecycle effectively.
- Pressure to demonstrate compliance across **multiple jurisdictions** using a unified framework.

With a ISO/IEC 42001 certification, Swiss and European organizations gain a **competitive edge**, signaling operational maturity and regulatory readiness in an evolving AI ecosystem.

Cost and Scope Considerations

The cost of ISO/IEC 42001 certification depends on **several factors**:

- Organization size and complexity.
- Number of sites and AI use cases.
- Maturity of existing governance systems.
- Integration with other ISO management systems (e.g. ISO/IEC 27001, ISO 9001).

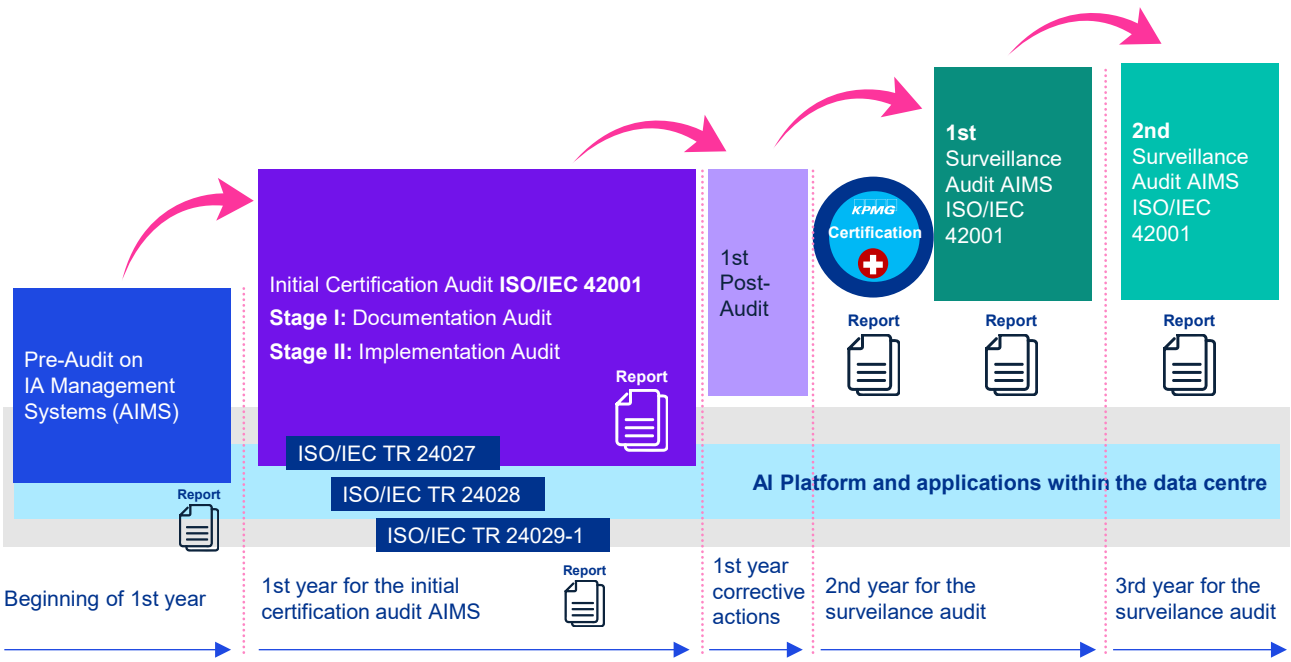
Costs may include:

- Initial **gap assessments** and **pre-audits.**
- Technical consulting/coaching to build or adjust the AIMS framework.
- Fees for external auditors and certification bodies.
- Potential **IT upgrades**, especially around data governance, risk management, and monitoring systems.

While large organizations with multiple AI applications and platforms may incur higher costs, small and mid-sized enterprises can implement a **scalable version of the AIMS**, focusing on high-risk areas and expanding over time. Certification is not only about compliance — it's about building AI governance as a strategic capability. In Europe and Switzerland, this is becoming a critical differentiator in both public trust and market leadership.

Certification Audit approach to attain the ISO/IEC 42001:2023 certification

Achieving certification to ISO/IEC 42001 requires organizations to undergo a **structured, multi-phase audit process,** designed to assess the design, implementation, and continuous improvement of the AI Management System (AIMS). This process ensures that all AI governance elements meet the standard's requirements and are applied effectively in practice. KPMG, as an accredited certification body, follows a clearly defined methodology in line with international auditing practices and ISO certification principles.



Audit phase 1:
Scope definition

The first step is to define the scope of the AIMS, including:

- AI systems, services and processes covered
- Geographic locations or organizational units involved
- Relevant legal and regulatory contexts (e.g. EU AI Act).

This scope provides the basis for audit planning and ensures alignment with organizational objectives. **Senior management responsibility** is critical at this stage to ensure strategic alignment and cross-functional coordination.

Audit phase 2:
Risk assessment

A comprehensive **AI risk assessment** helps to:

- Identify potential risks to individuals, society and the organization
- Evaluate the ethical, legal, operational and technical implications
- Define mitigation measures and controls aligned with ISO/IEC 42001.

This includes an AI impact assessment that evaluates broader implications such as fairness, transparency and unintended consequences.

Audit phase 3:
Proper documentation

During the **Audit Stage I**, the KPMG certification body will assess the organization's documentation and internal controls to ensure:

- Availability and suitability of information
- The AIMS aligns with ISO/IEC 42001 requirements
- Regulatory and legal compliance measures are appropriately addressed
- Confidentiality, integrity, and accountability controls are defined.

This stage identifies any **gaps or weaknesses** that must be addressed prior to full certification.

Audit phase 4:
Implementation and operational audit

The **Audit Stage II** focuses on evaluating the **practical implementation** of the AIMS, including:

- Interviews with stakeholders and system owners.
- Validation of AI control execution and implementation through technical environments.
- Verification of performance monitoring, data governance and ethical oversight.
- Internal audit results and management review processes.

Auditors assess whether the organization not only has the right processes in place but is also **actively operating and improving them.**

Audit phase 5:
Post-Audit for the countermeasures and improvements

Following the Post-Audit on Stage II, any **non-conformities or improvement areas** are documented. The organization is required to:

- Improve corrective actions within a defined timeframe.
- Re-validate the corrective measures and ensure correct implementation.
- Provide evidence of remediation.
- Engage in follow-up validation, if needed.

Once all requirements are met, KPMG finalizes the certification decision.

Audit phase 6:
Notification of the decision and certification

Upon successful completion of all audit phases, KPMG issues the globally recognized **ISO/IEC 42001 certificate**. The certification is valid for **three years**, with **annual surveillance audits** to verify ongoing compliance, followed by a **re-certification audit** in the third year.

Surveillance audits ensure that:

- Continuous improvement is being applied.
- Pre-selected control objectives on mission critical processes and core-applications are implemented securely and effectively.
- AI risks are being reassessed and controlled.
- The AIMS remains effective, relevant, and aligned with evolving expectations.

ISO/IEC 42001 certification is not a one-time event – it's an ongoing commitment to responsible, trustworthy AI governance .

Contact at KPMG

Reto P. Grubenmann

Director, Head of Certification Bodies
KPMG AG
E: retogrubenmann@kpmg.com
T: +41 58 249 42 46

Badenerstrasse 172
PO Box CH-8036 Zurich
Switzerland

kpmg.ch/certification

Document Classification: KPMG Confidential

CREATE: CRT161287A | May 2025