AI & Partners

Amsterdam - London - Singapore

EU AI Act

ISO/IEC 42001: 2023

A Guide to Implementation

March 2025

AI & Partners

Sean Musch, AI & Partners

Michael Borrelli, AI & Partners

Charles Kerrigan, CMS UK

Jeff Bennison, Wriben Consultancy Services

AI & Partners

Amsterdam - London - Singapore

AI & Partners defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots professional services, regulatory interventions, and participating in industry groups such as AI Commons, we fight for fundamental rights in the artificial intelligence age.

This report was prepared by Sean Donald John Musch and Michael Charles Borrelli. For more information visit https://www.ai-and-partners.com/.

Contact: Michael Charles Borrelli | Director | m.borrelli@ai-and-partners.com.

This report is an AI & Partners publication.

Contents

Introduction

As artificial intelligence continues to transform industries, organizations must adopt structured governance frameworks to ensure ethical, transparent, and accountable AI deployment. ISO/IEC 42001:2023 introduces the world's first AI Management System (AIMS) standard, providing a systematic approach to AI risk management, compliance, and continuous improvement.

This report explores the key principles, implementation strategies, and industry implications of ISO 42001, offering practical guidance for organizations seeking to align their AI systems with global best practices. From leadership commitments to AI risk assessments, the standard establishes a comprehensive foundation for responsible AI development and use.

With growing regulatory scrutiny—including the EU AI Act—organizations face increasing pressure to demonstrate AI governance maturity. In adopting ISO 42001, businesses can enhance trust, mitigate risks, and streamline compliance efforts in an evolving regulatory landscape.

Whether you are an AI provider, enterprise leader, or policymaker, this report serves as a strategic resource for navigating ISO 42001's implementation. At AI & Partners, we remain committed to supporting organizations in building AI that is ethical, accountable, and aligned with international standards.

Best regards,

Sean Musch

Founder/CEO

AI & Partners

Key questions being asked about ISO/IEC 42001: 2023

1. What is ISO/IEC 42001?

ISO/IEC 42001 is an international standard that provides requirements for establishing, implementing, maintaining, and continually improving an AI management system (AIMS). It is designed to help organizations responsibly develop, use, and govern AI systems while ensuring compliance with ethical, legal, and regulatory requirements. The standard outlines best practices for AI risk management, transparency, accountability, and performance evaluation. By following ISO 42001, organizations can enhance trust in their AI systems, mitigate potential risks, and align AI governance with business objectives. It applies to all types of organizations, including technology firms, government agencies, and financial institutions.

2. Why is ISO/IEC 42001 important for AI governance?

ISO/IEC 42001 is important for AI governance because it establishes a structured framework for managing AI risks, ensuring ethical AI deployment, and maintaining regulatory compliance. AI technologies pose unique challenges such as bias, lack of transparency, and security risks. This standard helps organizations address these issues by implementing policies, risk assessments, and monitoring mechanisms. It also fosters responsible AI development by promoting fairness, accountability, and human oversight. By adopting ISO 42001, organizations can improve AI system reliability, protect user rights, and demonstrate commitment to ethical AI practices, gaining stakeholder trust and regulatory approval.

3. Who should implement ISO/IEC 42001?

ISO/IEC 42001 is applicable to any organization that develops, provides, or uses AI systems. This includes AI technology companies, financial institutions, healthcare providers, government agencies, and educational institutions. Organizations that rely on AI for decision-making, automation, or analytics can benefit from implementing the standard to ensure compliance with ethical and legal requirements. It is also relevant for organizations seeking to mitigate AI-related risks, improve AI governance, and enhance public trust. ISO 42001 provides a framework that can be tailored to an organization's size, industry, and specific AI use cases, making it widely applicable.

4. What are the key clauses of ISO/IEC 42001?

ISO/IEC 42001 consists of nine clauses which are mandatory for formal certification (i.e. to establish an AI management system). These include **context of the organization**, which identifies external and internal AI-related factors; **leadership**, which ensures commitment from top management; **planning**, which defines AI objectives and risk management strategies; **support**, which covers resources, training, and documentation; **operation**, which includes AI risk assessments and impact evaluations; **performance evaluation**, which involves monitoring and audits; and **improvement**, which ensures continuous enhancement of AI governance. These components work together to create a structured approach for responsible AI development and deployment.

5. How does ISO/IEC 42001 help manage AI risks?

ISO/IEC 42001 helps organizations manage AI risks through structured risk assessment and mitigation strategies. It requires organizations to identify potential AI risks, such as bias, data security issues, and unintended consequences, and implement controls to address them. The standard promotes continuous monitoring of AI systems to detect anomalies and ensure compliance with ethical and legal standards. It also emphasizes AI impact assessments, which evaluate potential effects on individuals and society. By integrating risk management into AI governance, ISO 42001 helps organizations minimize harm, improve system reliability, and enhance accountability in AI decision-making. ISO 42001 draws on risk management practices similar to ISO/IEC 23894:2023.

6. How does ISO/IEC 42001 support regulatory compliance?

ISO/IEC 42001 aligns with global AI regulations and ethical guidelines, helping organizations meet compliance requirements. Many countries are developing AI regulations focusing on transparency, fairness, and accountability. This standard provides a structured framework to ensure AI systems adhere to these principles. By implementing ISO 42001, organizations can demonstrate responsible AI governance to regulators, auditors, and stakeholders. It also facilitates compliance with data protection laws, such as the GDPR, by ensuring proper AI risk assessments and documentation. This proactive approach reduces legal risks, prevents fines, and enhances the credibility of AI-driven organizations.

7. How does ISO/IEC 42001 address AI ethics and fairness?

ISO/IEC 42001 incorporates ethical principles into AI governance by promoting fairness, transparency, and accountability. It requires organizations to implement policies that prevent discrimination and bias in AI decision-making. The standard emphasizes human oversight, ensuring that AI systems do not operate without ethical considerations. AI impact assessments help evaluate potential societal and individual consequences, reducing unintended harm. Additionally, ISO 42001 encourages organizations to establish grievance mechanisms, allowing affected parties to report concerns. By embedding ethical considerations into AI governance, this standard helps organizations align AI systems with human rights and fairness principles.

8. What are the benefits of ISO/IEC 42001 certification?

Achieving ISO/IEC 42001 certification provides several benefits, including improved AI governance, risk mitigation, and regulatory compliance. Certification demonstrates an organization's commitment to ethical AI practices, enhancing trust among stakeholders, customers, and regulators. It also provides a competitive advantage by showcasing responsible AI management, which can attract business partnerships and investment. Additionally, certification helps organizations streamline AI risk management processes, ensuring long-term sustainability.

9. How does ISO/IEC 42001 differ from other AI standards?

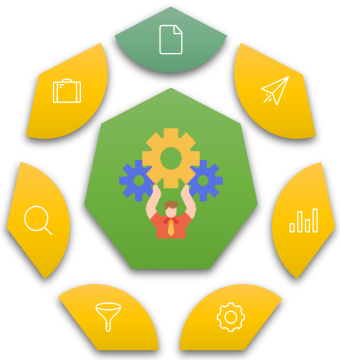
ISO/IEC 42001 differs from other AI standards by focusing specifically on AI management systems. While standards like ISO/IEC 27001 address information security and ISO/IEC 38507 focuses on AI governance for corporate boards, ISO 42001 provides a comprehensive framework for AI risk management, ethical considerations, and performance evaluation. It integrates AI-specific challenges, such as bias, explainability, and continuous learning, into a structured governance model. While ISO27001 addresses information security, organisations that have implemented ISO27001 will already be part of the way to ISO42001 compliance due to various areas of synergy between them. Unlike guidelines from the OECD, which offers high-level recommendations, ISO 42001 provides actionable requirements for organizations to establish and maintain an AI management system.

10. How can organizations implement ISO/IEC 42001?

Organizations can implement ISO/IEC 42001 by first conducting a gap analysis to assess their current AI governance practices against the standard's requirements. The next step involves defining AI objectives, establishing leadership commitment, and integrating AI risk management into business processes. Organizations must document AI policies, conduct impact assessments, and implement monitoring mechanisms. Regular audits and performance evaluations help ensure compliance and continual improvement. Training employees on AI governance and aligning AI strategies with regulatory requirements are also critical. Seeking external certification can further validate compliance and enhance trust in AI-driven services.

Understanding ISO/IEC 42001:2023

Context of the Organisation



Sub-Clauses:

- Understanding the organisation and its context
- Understanding the needs and expectations of interested parties
- Determining the scope of the AI management system
- AI management system

Why?

Understanding the context of an organization is essential for ensuring that its AI management system aligns with its objectives, regulatory requirements, and external influences. This understanding helps identify internal and external factors that can impact AI-related processes, risks, and compliance obligations. It ensures that organizations develop, deploy, and use AI systems responsibly, while considering legal, ethical, and societal expectations. In analysing its context, an organization can proactively address challenges, optimize its AI governance, and establish a clear framework for decision-making, risk management, and continuous improvement.

What?

The context of the organization refers to the external and internal factors that affect its ability to achieve the intended results of its AI management system. This includes legal, ethical, cultural, and economic influences, as well as governance structures, policies, and AI system objectives. Organizations must identify relevant stakeholders, such as AI providers, customers, regulators, and data subjects, to understand their roles and responsibilities. It also involves defining the organization's relationship with AI technologies and ensuring alignment with its strategic direction.

Where?

The concept of organizational context is applied across all aspects of AI management, from system development and deployment to regulatory compliance and risk management. It affects AI governance frameworks, ethical AI considerations, and operational decision-making. Industries such as healthcare, finance, transportation, and government rely on understanding their context to ensure AI systems are used safely and effectively. The context also informs AI policies, data management strategies, and accountability mechanisms, ensuring that AI applications align with industry best practices and legal requirements.

Who?

The requirement to understand organizational context applies to all entities involved in AI development, deployment, and governance. This includes AI providers, designers, developers, operators, evaluators, users, regulators, and other stakeholders. It is relevant for organizations of all sizes, from startups to multinational corporations, as well as public institutions that use AI systems. Additionally, policymakers and oversight bodies rely on contextual understanding to ensure AI technologies comply with societal values and legal frameworks.

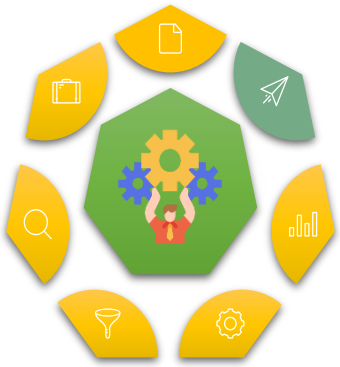
When?

The analysis of an organization's context applies at all stages of the AI management system lifecycle. It is crucial during the initial planning and implementation of AI systems, but also needs to be reviewed continuously as technologies, regulations, and business environments evolve. Context assessment should be revisited periodically to address emerging risks, new compliance requirements, and evolving stakeholder expectations. Organizations should integrate this process into their regular AI risk assessments and governance reviews.

How?

Organizations apply contextual analysis by identifying and documenting relevant external and internal factors that influence their AI management system. This involves assessing legal requirements, ethical considerations, competitive landscapes, and organizational policies. AI governance teams must engage with stakeholders, conduct risk assessments, and establish policies that reflect their operational realities. Additionally, organizations should integrate contextual considerations into AI impact assessments, system design processes, and compliance frameworks to ensure responsible AI deployment and management.

Leadership



Sub-Clauses:

- Leadership and commitment
- AI policy
- Roles, responsibilities and authorities

Why?

Leadership is essential for the successful implementation and ongoing effectiveness of an AI management system. Strong leadership ensures that AI policies, ethical guidelines, and regulatory requirements are integrated into the organization's core business processes. It fosters a culture of responsibility, compliance, and continual improvement in AI governance. Without leadership, organizations risk misalignment between AI strategies and business objectives, ineffective resource allocation, and increased legal or ethical risks. Leadership provides direction and accountability, ensuring that AI systems are used safely, ethically, and in a manner that aligns with organizational goals.

What?

Leadership in the context of AI management refers to the role of top management in setting policies, defining responsibilities, and ensuring the effective implementation of AI governance frameworks. It includes establishing AI objectives, integrating AI management system requirements into business processes, and allocating resources for compliance and continual improvement. Leadership also involves promoting awareness of AI-related responsibilities and ensuring that employees and stakeholders understand the importance of adhering to ethical and regulatory standards.

Where?

Leadership applies across all areas of an organization that interact with AI, including system development, deployment, compliance, risk management, and decision-making. It is crucial in sectors such as finance, healthcare, manufacturing, and public administration, where AI systems influence critical outcomes. Leadership is also applied in governance structures, corporate strategy, regulatory adherence, and AI ethics oversight. By embedding leadership in all AI-related processes, organizations ensure responsible AI use and alignment with legal, ethical, and societal expectations.

Who?

Leadership responsibilities apply primarily to top management, including executives, directors, and senior AI governance personnel. However, leadership extends to all levels of the organization, as various roles contribute to AI system oversight and compliance. AI project managers, ethics committees, compliance officers, and legal teams also play critical roles in enforcing AI policies. Additionally, leadership applies to external stakeholders, such as regulators and industry bodies, who influence AI governance frameworks and compliance requirements.

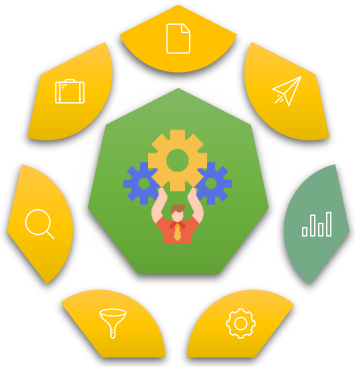
When?

Leadership in AI management applies throughout the entire lifecycle of an AI system, from initial development to deployment, monitoring, and decommissioning. It is especially critical during strategic planning, risk assessment, and compliance evaluations. Leadership must also be exercised when responding to AI-related incidents, ethical concerns, and regulatory changes. Organizations should demonstrate leadership on an ongoing basis by reviewing and updating AI policies to keep pace with technological advancements and emerging risks.

How?

Leadership is applied through the establishment of AI policies, commitment to regulatory compliance, and fostering an ethical AI culture. Top management ensures the integration of AI governance into business processes by defining clear roles and responsibilities, allocating necessary resources, and promoting continuous improvement. Organizations implement leadership through AI risk assessments, stakeholder engagement, and transparent decision-making. Leadership is also demonstrated through regular training, AI ethics reviews, and internal audits to ensure compliance and accountability.

Planning



Sub-Clauses:

- Actions to address risks and opportunities
  - General
  - AI risk assessment
  - AI risk treatment
  - AI system impact assessment
- AI objectives and planning to achieve them
- Planning of changes

Why?

Planning is essential for ensuring the effectiveness of an AI management system by addressing risks, setting objectives, and aligning AI strategies with organizational goals. It enables organizations to anticipate potential challenges, allocate resources efficiently, and comply with legal and ethical requirements. Proper planning helps in mitigating AI-related risks such as bias, security threats, and regulatory non-compliance. It also ensures continuous improvement in AI governance, fostering trust and reliability in AI-driven processes.

What?

Planning in the context of AI management involves defining actions to address risks and opportunities, setting AI-related objectives, and ensuring compliance with policies and standards. It includes AI risk assessment, impact evaluation, and establishing measurable goals for responsible AI development. Organizations must determine acceptable risk levels, assess AI system impacts, and document strategies for integrating AI into business operations. Planning also involves defining governance structures, assigning responsibilities, and implementing necessary controls for AI risk treatment.

Where?

Planning is applied across all functions and levels of an organization that interact with AI systems. It is particularly relevant in AI governance, risk management, compliance, and operational decision-making. Industries such as healthcare, finance, manufacturing, and government apply AI planning to ensure ethical AI deployment and adherence to regulations. Planning is also crucial in AI system design, development, and monitoring to prevent unintended consequences and enhance transparency in AI decision-making.

Who?

AI planning applies to top management, AI governance teams, compliance officers, data scientists, developers, and risk management professionals. It also involves external stakeholders such as regulators, customers, and industry bodies who influence AI governance. Organizations of all sizes, from startups to multinational corporations, must engage in structured AI planning to ensure responsible AI use. Additionally, policymakers and oversight entities rely on AI planning frameworks to regulate AI technologies effectively.

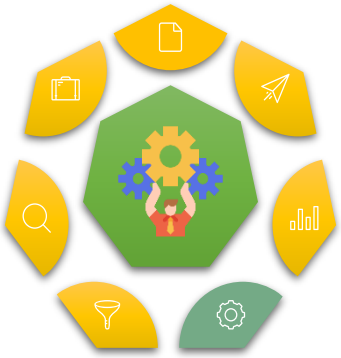
When?

Planning is an ongoing process that applies throughout the AI system lifecycle, from initial strategy development to implementation, monitoring, and continuous improvement. It is especially critical during AI risk assessments, system impact evaluations, and regulatory compliance reviews. AI planning must also adapt to changes in technology, legislation, and societal expectations. Organizations should conduct periodic reviews to update AI objectives and risk treatment strategies as new challenges and opportunities emerge.

How?

AI planning is applied through structured processes that include risk assessment, impact analysis, and objective setting. Organizations must document AI risk criteria, evaluate AI system consequences, and establish controls for AI risk treatment. Planning also involves stakeholder engagement, resource allocation, and compliance integration into AI governance frameworks. AI policies and objectives should be aligned with business goals and regulatory standards, ensuring AI management systems remain effective and adaptable.

Support



Sub-Clauses:

- Resources
- Competence
- Awareness
- Communication
- Documented information
  - General
  - Creating and updated documented information
  - Control of documented information

Why?

Support is necessary to ensure the effective operation and continuous improvement of an AI management system. It provides the essential resources, competence, awareness, communication, and documented information needed to maintain AI governance and compliance. Without adequate support, organizations risk inefficiencies, security vulnerabilities, and non-compliance with regulatory requirements. Proper support mechanisms also enhance transparency, accountability, and trust in AI systems by ensuring that all personnel are properly trained and informed.

What?

Support in AI management refers to the framework of resources, skills, awareness, and documentation required to implement and maintain AI governance effectively. It includes personnel training, information management, communication strategies, and technical infrastructure to sustain AI systems. The organization must ensure that employees understand their roles and responsibilities, have the necessary expertise, and follow documented procedures to manage AI-related risks and compliance requirements.

Where?

Support is applied across all areas of AI management, including development, deployment, monitoring, and risk assessment. It ensures that AI-related policies, ethical considerations, and compliance requirements are met in sectors such as healthcare, finance, government, and technology. Organizations apply support mechanisms in AI training programs, risk management strategies, internal audits, and documentation processes to ensure the effective governance and operational integrity of AI systems.

Who?

Support applies to all individuals involved in AI management, including executives, AI governance teams, developers, compliance officers, risk managers, and end users. It also extends to external stakeholders such as regulators, auditors, and customers who interact with AI systems. Organizations must ensure that all personnel handling AI systems are properly trained and that stakeholders receive relevant information and communication to maintain trust and compliance.

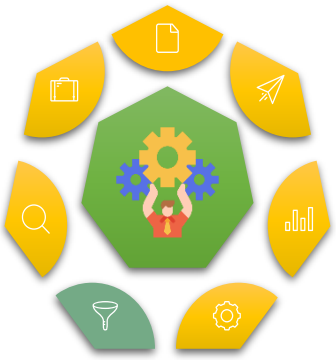
When?

Support is a continuous requirement throughout the lifecycle of an AI system, from its initial development to its deployment, monitoring, and eventual decommissioning. It is crucial during training sessions, risk assessments, and compliance reviews. Organizations must also provide ongoing support to adapt to regulatory updates, technological advancements, and evolving ethical considerations in AI governance.

How?

Support is applied through structured processes that include resource allocation, competence development, awareness programs, communication protocols, and documentation management. Organizations ensure support by providing training, defining clear roles and responsibilities, and implementing AI policies that align with regulatory and ethical standards. Documented procedures, regular audits, and stakeholder engagement also contribute to the effective application of support in AI management.

Operation



Sub-Clauses:

- Operational planning and control
- AI risk assessment
- AI risk treatment
- AI system impact assessment

Why?

Operation is essential for ensuring the effective implementation, monitoring, and control of AI systems throughout their lifecycle. It establishes structured processes to maintain AI performance, security, and compliance while mitigating risks. Proper operational planning ensures AI systems function as intended, prevent failures, and align with legal and ethical requirements. Without well-defined operations, AI systems may exhibit unintended biases, security vulnerabilities, or failures that can lead to regulatory penalties, reputational damage, or user harm.

What?

Operation in AI management refers to the processes and controls required for the deployment, monitoring, and continuous improvement of AI systems. It involves defining operational procedures, ensuring system performance, and implementing corrective measures in response to failures. This includes AI risk assessment, system updates, security protocols, and event logging to maintain system reliability and traceability. Organizations must document operational procedures and allocate responsibilities to personnel managing AI operations.

Where?

Operation is applied across all AI-related processes, including system design, development, deployment, monitoring, and maintenance. It is particularly critical in sectors such as healthcare, finance, manufacturing, and public administration, where AI systems influence decision-making and regulatory compliance. AI operation is also relevant in cybersecurity, fraud detection, and automated decision-making, ensuring that AI models function safely and effectively in real-world applications.

Who?

Operation applies to AI developers, system administrators, compliance officers, risk managers, and governance teams responsible for AI deployment and monitoring. It also involves external stakeholders such as regulators, auditors, and customers who rely on AI-generated outputs. Organizations using AI in critical sectors must ensure that operational responsibilities are clearly defined, with accountability assigned to personnel overseeing AI performance, maintenance, and risk management.

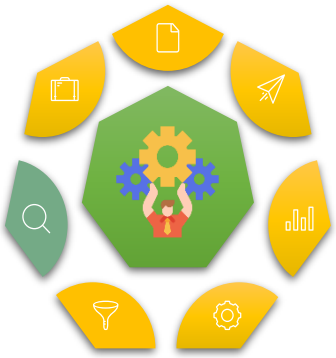
When?

Operation applies continuously throughout the AI system lifecycle, from initial deployment to decommissioning. It is particularly crucial during system rollouts, updates, and risk assessments. AI operations must be regularly reviewed and updated to address evolving risks, regulatory changes, and advancements in AI technology. Organizations should integrate operational processes into their AI governance frameworks, ensuring that monitoring and risk mitigation strategies are consistently applied.

How?

Operation is applied through structured processes such as AI risk assessment, impact evaluation, system performance monitoring, and incident response. Organizations must document AI system operations, define roles and responsibilities, and implement real-time monitoring mechanisms. Automated logging of AI activities helps track system behaviour, identify anomalies, and support regulatory compliance. Additionally, organizations should establish rollback plans, update procedures, and user notification mechanisms for AI system changes.

Performance Evaluation



Sub-Clauses:

- Monitoring, measurement, analysis, and evaluation
- Internal audit
  - General
  - Internal audit programme
- Management review
  - General
  - Management review inputs
  - Management review results

Why?

Performance evaluation is essential for assessing the effectiveness, reliability, and compliance of AI systems with organizational objectives and regulatory requirements. It ensures that AI models function as intended, meet ethical standards, and remain free from bias or degradation over time. Regular performance assessments help organizations detect risks, address inefficiencies, and maintain transparency in AI-driven decision-making. Without performance evaluation, AI systems may drift from their intended functionality, leading to inaccurate outputs, security vulnerabilities, or legal non-compliance.

What?

Performance evaluation in AI management involves the systematic monitoring, measurement, analysis, and review of AI system performance. It includes defining key performance indicators (KPIs), establishing evaluation methodologies, and conducting audits to ensure AI systems align with organizational goals. The process assesses AI effectiveness, compliance with ethical principles, and overall system integrity. It also includes internal audits and management reviews to identify areas for improvement and maintain AI system accountability.

Where?

Performance evaluation is applied across all AI-related processes, including model development, deployment, risk management, and compliance assessment. It is particularly relevant in industries such as healthcare, finance, transportation, and public administration, where AI systems impact critical decisions. Organizations apply performance evaluation in AI governance frameworks, auditing procedures, and impact assessments to ensure continuous compliance with ethical and regulatory standards.

Who?

Performance evaluation applies to AI developers, system operators, compliance officers, auditors, and risk management teams. It also involves top management, who must review AI system performance to ensure alignment with business objectives. Additionally, external stakeholders such as regulators, customers, and ethical review boards play a role in evaluating AI system impacts and ensuring adherence to industry standards.

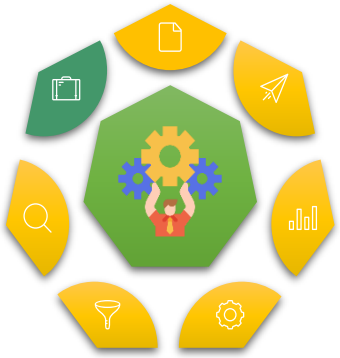
When?

Performance evaluation is an ongoing process applied at various stages of the AI system lifecycle, from initial development to deployment, monitoring, and decommissioning. It should be conducted at planned intervals and whenever significant changes occur in AI system functionality, data inputs, or regulatory landscapes. Organizations must also perform evaluations in response to AI-related incidents, ensuring corrective actions are taken to maintain system integrity and compliance.

How?

Organizations apply performance evaluation through structured methodologies, including continuous monitoring, periodic audits, and management reviews. This involves setting measurable performance criteria, collecting relevant data, and analysing AI system outputs to detect deviations from expected behaviour. AI risk assessments, compliance checks, and ethical impact evaluations are integrated into the process. Documentation of performance results is required to demonstrate accountability and inform future improvements.

Improvement



Sub-Clauses:

- Continual improvement
- Non-conformity and corrective action

Why?

Improvement is essential for ensuring that an AI management system remains effective, adaptable, and compliant with evolving standards and regulations. AI technologies and risks are constantly changing, requiring organizations to continuously refine their processes, address nonconformities, and enhance system performance. Without a structured improvement process, AI systems may become outdated, inefficient, or non-compliant, leading to security vulnerabilities, operational failures, and reputational damage.

What?

Improvement in AI management refers to the ongoing efforts to enhance the suitability, adequacy, and effectiveness of AI-related processes. It includes continual improvement initiatives, corrective actions for nonconformities, and preventive measures to mitigate future risks. Organizations must systematically review AI system performance, identify gaps, and implement necessary changes to ensure compliance with internal policies and external regulations.

Where?

Improvement applies across all AI management processes, from system development and deployment to monitoring, risk management, and compliance. It is particularly relevant in industries such as healthcare, finance, and government, where AI systems must be regularly updated to align with ethical and regulatory requirements. Organizations apply improvement mechanisms within AI governance frameworks, incident response strategies, and performance evaluations.

Who?

Improvement applies to all personnel involved in AI system management, including executives, compliance officers, risk managers, developers, and data scientists. It also involves external stakeholders such as regulators, auditors, and users who provide feedback on AI system performance. Ensuring a culture of continual improvement requires commitment from top management and collaboration across different teams.

When?

Improvement is a continuous process that applies throughout the lifecycle of an AI system. It is especially critical when nonconformities are identified, during periodic audits, after major regulatory updates, or in response to AI-related incidents. Organizations should establish a structured approach to reviewing and improving their AI management system at regular intervals and whenever new risks or opportunities arise.

How?

Improvement is applied through systematic evaluation, corrective actions, and innovation in AI management practices. Organizations must document and review AI-related nonconformities, assess root causes, and implement corrective measures. Continuous learning, stakeholder feedback, and technological advancements drive improvements. AI system audits, risk assessments, and governance reviews ensure that enhancements are effectively integrated into business processes.

Implementing ISO/IEC 42001:2023

Phase 1

Building Strong Pillars for ISO 42001

This phase lays the groundwork for ISO 42001 by assessing your current AI governance structure, identifying gaps, and defining AI management policies. It ensures that your organization is well-prepared for compliance.

☐ Conduct a Readiness Assessment

Perform a gap analysis to evaluate current AI governance against ISO 42001.

- Identify AI-related risks, compliance obligations, and organizational objectives.
- Map existing AI processes, policies, and documentation.
- Engage stakeholders (executives, compliance teams, AI developers) in the assessment.
- Select a certification body and schedule the audit.

☐ Define AI Management Policies & Objectives

Develop a clear AI policy aligned with ISO 42001 and business goals.

- Establish AI governance roles, leadership commitment, and accountability structures.
- Define ethical AI principles, risk management strategies, and compliance measures.
- Document AI system lifecycle processes, from development to decommissioning.

☐ Develop & Execute Implementation Roadmap

Ensure the right expertise, tools, and technology are in place.

- Assign roles and responsibilities for AI governance, compliance, and risk management.
- Allocate budget and resources for AI audits, employee training, and system monitoring.
- Create a timeline with milestones, ensuring phased implementation and progress tracking.

Phase 2

Executing Your ISO 42001 Compliance Plan

This phase focuses on implementing ISO 42001 controls, integrating compliance measures into business operations, and training employees to maintain AI system integrity.

☐ Implement AI Risk Mangement Controls

Establish risk assessment and mitigation strategies for AI systems.

- Conduct AI risk and impact assessments (bias, fairness, transparency, security).
- Define controls for data governance, privacy, and ethical AI usage.
- Implement monitoring tools to track AI performance and mitigate risks in real-time.

☐ Train Employees and Enhance Awareness

Ensure all employees understand AI compliance, ethics, and risk management.

- Conduct AI governance training for developers, compliance teams, and decision-makers.
- Provide ongoing education on regulatory updates and evolving AI risks.
- Implement internal reporting mechanisms for AI-related issues or concerns.

☐ Establish Continuous AI System Monitoring

Track AI system performance, compliance, and nonconformities.

- Develop an AI performance evaluation framework with key performance indicators (KPIs).
- Maintain records of AI decisions, risk assessments, and system updates.
- Implement corrective and preventive actions (CAPA) to address AI governance gaps.

Phase 3

Conducting an ISO 42001 Pre-Audit

This phase ensures your organization is fully prepared for certification by conducting pre-audits, reviewing AI governance structures, and resolving compliance gaps.

☐ Perform a Pre-Audit & Identify Gaps

Assess AI system readiness through an ISO 42001 pre-audit.

- Review AI governance policies, risk management practices, and operational controls.
- Identify weaknesses in AI compliance and implement necessary improvements.
- Conduct AI ethics and security assessments to ensure regulatory alignment.

☐ Review & Update AI Governance Documentation

Ensure policies, procedures, and records meet ISO 42001 standards.

- Update AI policies and risk management frameworks based on audit findings.
- Ensure all documented processes align with ISO 42001 compliance requirements.
- Verify that AI lifecycle documentation includes details (e.g. development, testing).

☐ Conduct a Management Review & Final Check

Ensure leadership oversight and commitment before the certification audit.

- Conduct a management review meeting to finalize compliance status.
- Validate that AI risk assessments, employee training, and system monitoring are in place.
- Obtain leadership approval to proceed with the formal ISO 42001 certification audit.

Phase 4

Obtaining ISO 42001 Certification

This final phase involves engaging an accredited certification body to conduct the formal audit, addressing any nonconformities, and achieving certification.

☐ Contact Certification Body & Execute the Audit

Follow-up with chosen recognized certifying body to assess ISO 42001 compliance.

- Contact the accredited organization chosen for the certification process.
- Execute a certification audit, such as document review and on-site assessments.
- Ensure all stakeholders are prepared for audit interviews and system evaluations.

☐ Undergo the Certification ISO 42001 Audit

Demonstrate AI governance compliance and risk management effectiveness.

- Provide documents for the review of policies, risk assessments, and compliance records.
- Permit on-site audit assessment of AI system operations, risk controls, and governance.
- Discuss findings with assessors upon assessment completion.

☐ Achieve Certification & Maintain Ongoing Compliance

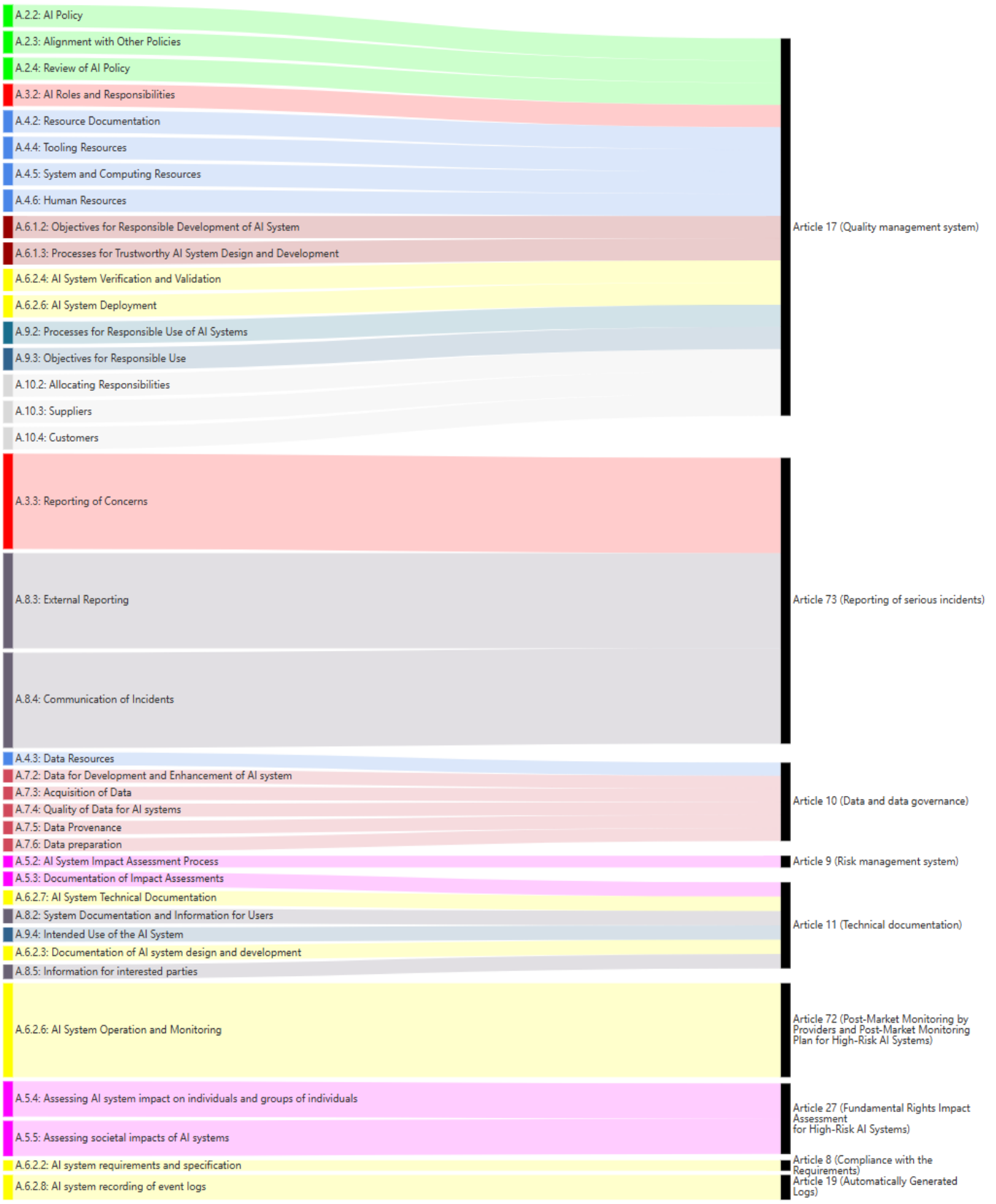
Receive ISO 42001 certification and establish continuous improvement measures.

- Implement an AI management review cycle to update policies and risk frameworks.
- Conduct regular internal audits to ensure ongoing compliance..
- Maintain certification by preparing for surveillance audits and regulatory updates.

Mapping ISO/IEC 42001:2023 to EU AI Act

ISO/IEC 42001:2023

EU AI Act



ISO/IEC 42001:2023			EU AI Act	
Reference	**Topic**	**Control**	**Article**	**Explanation**
A.2.2	AI policy	The organization shall document a policy for the development or use of AI systems.	17	Article 17 of the EU AI Act requires providers of high-risk AI systems to establish a quality management system, which includes documenting policies and procedures.
A.2.3	Alignment with other organizational policies	The organization shall determine where other policies can be affected by or apply to, the organization's objectives with respect to AI systems.	17	Article 17 also emphasizes the integration of AI system management with other organizational policies.
A.2.4	Review of the AI policy	The AI policy shall be reviewed at planned intervals or additionally as needed to ensure its continuing suitability, adequacy and effectiveness.	17	Article 17 mandates regular reviews of the quality management system to ensure its effectiveness.
A.3.2	AI roles and responsibilities	Roles and responsibilities for AI shall be defined and allocated according to the needs of the organization.	17	Article 17 requires defining roles and responsibilities within the quality management system.
A.3.3	Reporting of concerns	The organization shall define and put in place a process for employees of the organization to report concerns about the organization's role with respect to an AI system throughout its life cycle.	73	Article 73 outlines procedures for reporting serious incidents related to AI systems
A.4.2	Resource documentation	The organization shall identify and document relevant resources required for the activities at given AI system life cycle stages and other AI-related activities relevant for the organization.	17	Article 17 includes resource management as part of the quality management system.
A.4.3	Data resources	As part of resource identification, the organization shall document information about the data resources utilized for the AI system.	10	Article 10 focuses on data governance, including data management practices.
A.4.4	Tooling resources	As part of resource identification, the organization shall document information about the tooling resources utilized for the AI system.	17	Article 17 includes technical specifications and standards as part of the quality management system.

ISO/IEC 42001:2023			EU AI Act	
Reference	**Topic**	**Control**	**Article**	**Explanation**
A.4.5	System and computing resources	As part of resource identification, the organization shall document information about the system and computing resources utilized for the AI system.	17	Article 17 covers resource management, including system resources.
A.4.6	Human resources	As part of resource identification, the organization shall document information about the human resources and their competences utilized for the development, deployment, operation, change management, maintenance, transfer and decommissioning, as well as verification and integration of the AI system.	17	Article 17 also addresses the allocation of human resources within the quality management system.
A.5.2	AI system impact assessment process	The organization shall establish a process to assess the potential consequences for individuals and societies that can result from the AI system throughout its life cycle.	9	Article 9 requires a risk management system to assess potential impacts.
A.5.3	Documentation of AI system impact assessments	The organization shall document the results of AI system impact assessments and retain results for a defined period.	11	Article 11 requires maintaining technical documentation, which includes impact assessments.
A.5.4	Assessing AI system impact on individuals and groups of individuals	The organization shall assess and document the potential impacts of AI systems to individuals or groups of individuals throughout the system's life cycle.	27	Article 27 of the EU AI Act requires a fundamental rights impact assessment for high-risk AI systems, which includes assessing the impact on individuals and groups.
A.5.5	Assessing societal impacts of AI systems	The organization shall assess and document the potential societal impacts of their AI systems throughout their life cycle.	27	Article 27 also covers the broader societal impacts as part of the fundamental rights impact assessment, ensuring that the potential societal consequences are documented and addressed.

ISO/IEC 42001:2023			EU AI Act	
Reference	**Topic**	**Control**	**Article**	**Explanation**
A.6.1.2	Objectives for responsible development of AI system	The organization shall identify and document objectives to guide the development of trustworthy AI systems, and take those objectives into account and integrate measures to achieve them in the development life cycle.	17	Article 17 includes setting objectives for compliance and responsible development.
A.6.1.3	Processes for trustworthy AI system design and development	The organization shall define and document the specific processes for the responsible design and development of the AI system.	17	Article 17 requires defining processes for AI system design and development.
A.6.2.2	AI system requirements and specification	The organization shall specify and document requirements for new AI systems or material enhancements to existing systems.	8	Article 8 of the EU AI Act requires high-risk AI systems to comply with the requirements laid down in Section 2, taking into account their intended purpose and the state of the art in AI technologies. This includes specifying and documenting requirements for new AI systems or enhancements.
A.6.2.3	Documentation of AI system design and development	The organization shall document the AI system design and development based on organizational objectives, documented requirements and specification criteria.	11	Article 11 mandates the creation of technical documentation for high-risk AI systems. This documentation must demonstrate compliance with the requirements and provide necessary information for assessment by competent authorities. It includes elements such as design specifications, development processes, and system architecture.
A.6.2.4	AI system verification and validation	The organization shall define and document verification and validation measures for the AI system and specify criteria for their use.	17	Article 17 includes examination, test, and validation procedures.
A.6.2.5	AI system deployment	The organization shall document a deployment plan and ensure that appropriate requirements are met prior to deployment.	17	Article 17 requires a deployment plan as part of the quality management system.

ISO/IEC 42001:2023		EU AI Act		
Reference	**Topic**	**Control**	**Article**	**Explanation**
A.6.2.6	AI system operation and monitoring	The organization shall define and document the necessary elements for the ongoing operation of the AI system. At the minimum, this should include system and performance monitoring, repairs, updates and support.	72	Article 72 outlines post-market monitoring requirements.
A.6.2.7	AI system technical documentation	The organization shall determine what AI system technical documentation is needed for each relevant category of interested parties, such as users, partners, supervisory authorities, and provide the technical documentation to them in the appropriate form.	11	Article 11 requires comprehensive technical documentation.
A.6.2.8	AI system recording of event logs	The organization shall determine at which phases of the AI system life cycle, record keeping of event logs should be enabled, but at the minimum when the AI system is in use.	19	Article 19 requires providers to keep logs automatically generated by high-risk AI systems, which aligns with the need to determine phases for event log recording.
A.7.2	Data for development and enhancement of AI system	The organization shall define, document and implement data management processes related to the development of AI systems.	10	Article 10 covers data management processes.
A.7.3	Acquisition of data	The organization shall determine and document details about the acquisition and selection of the data used in AI systems.	10	Article 10 includes data collection processes.
A.7.4	Quality of data for AI systems	The organization shall define and document requirements for data quality and ensure that data used to develop and operate the AI system meet those requirements.	10	Article 10 emphasizes data quality requirements.
A.7.5	Data provenance	The organization shall define and document a process for recording the provenance of data used in its AI systems over the life cycles of the data and the AI system.	10	Article 10 requires documentation of data provenance.

ISO/IEC 42001:2023			EU AI Act	
Reference	**Topic**	**Control**	**Article**	**Explanation**
A.7.6	Data preparation	The organization shall define and document their needs for and approaches to data preparation.	10	Article 10 focuses on data governance, including data management processes that encompass data preparation.
A.8.2	System documentation and information for users	The organization shall determine and provide the necessary information to users of the system.	11	Article 11 requires providing necessary information to users.
A.8.3	External reporting	The organization shall provide capabilities for interested parties to report adverse impacts of the system.	73	Article 73 outlines reporting obligations for incidents.
A.8.4	Communication of incidents	The organization shall determine and document a plan for communicating incidents to users of the system.	73	Article 73 requires communication plans for incidents.
A.8.5	Information for interested parties	The organization shall determine and document their obligations to reporting information about the AI system to interested parties.	11	Article 11 requires the provision of technical documentation to interested parties, ensuring transparency and accountability in reporting information about AI systems.
A.9.2	Processes for responsible use of AI systems	The organization shall define and document the processes for the responsible use of AI systems.	17	Article 17 includes defining processes for responsible use.
A.9.3	Objectives for responsible use of AI system	The organization shall identify and document objectives to guide the responsible use of AI systems.	17	Article 17 requires setting objectives for responsible use.
A.9.4	Intended use of the AI system	The organization shall ensure that the AI system is used according to the intended uses of the AI system and its accompanying documentation.	17	Article 11 requires documentation of the intended use.
A.10.2	Allocating responsibilities	The organization shall ensure that responsibilities within their AI system life cycle are allocated between the organization, its partners, suppliers, customers and third parties.	17	Article 17 includes an accountability framework.

ISO/IEC 42001:2023			EU AI Act	
Reference	**Topic**	**Control**	**Article**	**Explanation**
A.10.3	Suppliers	The organization shall establish a process to ensure that its usage of services, products or materials provided by suppliers aligns with the organization's approach to the responsible development and use of AI systems.	17	Article 17 requires ensuring supplier alignment with AI system objectives.
A.10.4	Customers	The organization shall ensure that its responsible approach to the development and use of AI systems considers their customer expectations and needs.	17	Article 17 includes customer communication as part of the quality management system.

Calls to action

1. Adopt ISO 42001 for AI Governance

Ensure your organization is aligned with global AI best practices by implementing ISO 42001. Strengthen AI governance, manage risks effectively, and enhance compliance with international regulations like the EU AI Act.

2. Conduct and ISO 42001 Pre-Audit

Assess your current AI systems against ISO 42001 and the EU AI Act. Identify gaps, mitigate risks, and build a roadmap for compliance to ensure responsible AI deployment.

3. Transparency and Accountability

Implement policies that improve AI system explainability, fairness, and ethical decision-making. Strengthen public and stakeholder trust by embedding transparency and accountability in AI operations.

4. Invest in AI Risk Management and Monitoring

Proactively monitor AI performance, assess impact risks, and integrate continuous improvement processes. Stay ahead of regulatory changes by establishing robust AI risk management frameworks.

5. Partner with AI Governance Experts

Work with AI compliance specialists to navigate ISO 42001 certification and regulatory requirements. Leverage expert insights to develop a sustainable, ethical, and compliant AI strategy.

Conclusion

ISO/IEC 42001:2023 marks a pivotal milestone in the development of structured, ethical, and accountable AI governance. As organizations worldwide seek to manage AI risks while fostering innovation, this new standard provides a comprehensive framework for implementing AI Management Systems (AIMS). By establishing clear requirements for transparency, accountability, and risk mitigation, ISO 42001 is already reshaping industry best practices and reinforcing global efforts toward responsible AI adoption.

However, effective implementation will determine the standard's impact. Organizations face varying levels of readiness, with challenges such as aligning existing governance structures, ensuring adequate oversight, and balancing compliance with operational flexibility. Small and medium enterprises (SMEs), in particular, may require additional support to integrate ISO 42001 into their AI strategies while maintaining competitiveness in an evolving regulatory environment.

Despite these challenges, early adopters are demonstrating the benefits of structured AI governance. Technology firms, financial institutions, and healthcare organizations are leveraging ISO 42001 to strengthen compliance, mitigate AI-related risks, and build public trust. By embedding risk assessments, ethical safeguards, and continuous monitoring into their AI ecosystems, these organizations illustrate how a proactive approach can enhance both regulatory alignment and operational efficiency.

For businesses and policymakers alike, ISO 42001 presents a unique opportunity to establish AI governance leadership. Implementing clear policies, investing in AI risk management, and fostering cross-sector collaboration will be crucial in driving widespread adoption. As industries increasingly rely on AI-driven decision-making, the standard provides a vital foundation for ensuring AI remains transparent, reliable, and aligned with societal expectations.

Looking ahead, the long-term success of ISO 42001 will depend on industry-wide engagement, ongoing refinement of best practices, and integration with emerging AI regulations, such as the EU AI Act. For those organisations that embrace the standard, they can position themselves at the forefront of responsible AI development, setting a global benchmark for ethical, effective, and sustainable AI governance.

About AI & Partners

AI & Partners

Amsterdam - London - Singapore

AI & Partners – 'AI That You Can Trust'

At AI & Partners, we're here to help you navigate the complexities of the EU AI Act, so you can focus on what matters—using AI to grow your business. We specialize in guiding companies through compliance with tailored solutions that fit your needs. Why us? Because we combine deep AI expertise with practical, actionable strategies to ensure you stay compliant and responsible, without losing sight of your goals. With our support, you get AI you can trust—safe, accountable, and aligned with the law.

To find out how we can help you, email contact@ai-and-partners.com or visit https://www.ai-and-partners.com.

Contacts

Sean Donald John Musch, CEO/Founder, s.musch@ai-and-partners.com

Michael Charles Borrelli, Director, m.borrelli@ai-and-partners.com

Authors

Sean Donald John Musch, CEO/Founder

Michael Charles Borrelli, Director

References

European Parliament and The Council of the European Union, (2024), 2024/1689 Regulation (EU) 2024/1689 of the European Parliament and of The Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), accessible at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689 (last accessed 2nd March 2025)

International Organization for Standardization, (2023), 'ISO/IEC 23894:2023: Information technology — Artificial intelligence — Guidance on risk management', accessible at: https://www.iso.org/standard/77304.html (last accessed 3rd March 2025)

International Organization for Standardization, (2023), 'ISO/IEC 42001:2023: Information technology — Artificial intelligence — Management system', accessible at: https://www.iso.org/standard/81230.html (last accessed 2nd March 2025)

Important notice

This document has been prepared by AI & Partners B.V. for the sole purpose of enabling the parties to whom it is addressed to evaluate the capabilities of AI & Partners B.V. to supply the proposed services.

Other than as stated below, this document and its contents are confidential and prepared solely for your information, and may not be reproduced, redistributed or passed on to any other person in whole or in part. If this document contains details of an arrangement that could result in a tax or National Insurance saving, no such conditions of confidentiality apply to the details of that arrangement (for example, for the purpose of discussion with tax authorities). No other party is entitled to rely on this document for any purpose whatsoever and we accept no liability to any other party who is shown or obtains access to this document.

This document is not an offer and is not intended to be contractually binding. Should this proposal be acceptable to you, and following the conclusion of our internal acceptance procedures, we would be pleased to discuss terms and conditions with you prior to our appointment. Images used throughout the document have either been produced in-house or sourced from publicly available sources (see **References** for details).

AI & Partners B.V. is the Dutch headquarters of AI & Partners, a global professional services firm. Please see https://www.ai-and-partners.com/ to learn more about us.

Designed and produced by AI & Partners B.V