e

AI & Partners

Amsterdam - London - Singapore

EU AI Act

ISO/IEC DIS 42006

A Guide to Implementation

April 2025

AI & Partners

Sean Musch, AI & Partners

Michael Borrelli, AI & Partners

Charles Kerrigan, CMS UK

Filiz Demerci, Technoserve IT Consulting

Vibhav Mithal, Anand and Anand

Leonardo Freixas, The Signal Newsletter

Xiaochen Zhang, AI 2030

Helen Yu, Tigon Advisory Corp

ISO

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 reshapes industries, organizations require rigorously audited governance frameworks to ensure ethical, transparent, and accountable AI deployment. ISO/IEC 42001:2023 establishes the world's first AI Management System (AIMS) standard, while ISO/IEC 42006:2023 provides the critical requirements for bodies certifying these systems—ensuring audits are conducted with AI-specific expertise and impartiality.

This report examines how ISO 42001 implementation, verified through ISO 42006-certified audits, enables organizations to:

1. Systematically manage AI risks (e.g., bias, security) through standardized controls.
2. Align with regulations like the EU AI Act via mapped requirements (e.g., risk management, transparency).
3. Demonstrate governance maturity to stakeholders through credible third-party certification.

With regulators intensifying scrutiny, ISO 42006-compliant certification bodies offer a trusted pathway to validate AIMS effectiveness. Their adherence to strict competence criteria (e.g., AI experience, sector knowledge) and audit methodologies (e.g., two-stage assessments, Annex A's risk-based sampling) ensures:

1. Consistency: Comparable evaluations across industries.
2. Transparency: Clear documentation (e.g., Statement of Applicability) for compliance.
3. Accountability: Annual surveillance audits (Section 9.6) for continuous improvement.

Whether you're an AI provider seeking certification, an enterprise scaling responsible AI, or a policymaker shaping standards, this report provides actionable insights into:

1. Implementing ISO 42001 with controls for data quality, ethics, and lifecycle management.
2. Selecting ISO 42006-accredited auditors to ensure rigorous, unbiased assessments.
3. Leveraging certification to streamline compliance with the EU AI Act and other frameworks.

At AI & Partners, we specialize in bridging ISO 42001 implementation with ISO 42006-certified audits, helping organizations build AI systems that are trusted, compliant, and future-proof.

Best regards,

Sean Musch

Founder/CEO

AI & Partners

Key questions being asked about ISO/IEC DIS 42006

What is the purpose of ISO/IEC DIS 42006?

ISO/IEC DIS 42006 provides requirements for certification bodies auditing and certifying Artificial Intelligence Management Systems (AIMS) according to ISO/IEC 42001. It ensures competence, consistency, and reliability in certification processes, addressing AI-specific risks like data protection, ethics, and algorithm validation. The standard also supports accreditation bodies in evaluating certification bodies' compliance and harmonizing practices globally.

ISO/IEC DIS 42006 specifies additional requirements (beyond ISO/IEC 17021-1) for third-party certification bodies auditing and certifying Artificial Intelligence Management Systems (AIMS) per ISO/IEC 42001:2023. It ensures impartiality, competence, consistency and reliability in certification processes, addressing AI-specific risks (e.g. data protection, ethics, algorithm validation). It also guides accreditation bodies in harmonising and assessing certification-body practices worldwide.

What are the key principles for AIMS certification outlined in the standard?

ISO 42006 inherits the six management-system principles from ISO/IEC 17021-1: impartiality, competence, responsibility, openness, confidentiality and responsiveness to complaints. Certification bodies must avoid conflicts of interest (e.g., no consulting on AI management systems) and ensure auditors have expertise in AI governance, risk management, and sector-specific regulations. These underpin every audit and certification decision to guarantee credible, unbiased, transparent and accountable AIMS assessments.

How does ISO/IEC DIS 42006 address conflicts of interest for certification bodies?

Certification bodies must not engage in consulting for AI-related management systems (e.g., risk or data protection). Permissible activities include generic training or pre-audit scope assessments, provided they avoid company-specific advice. Internal audits for clients are prohibited to prevent self-assessment biases. These rules maintain impartiality and trust in certification outcomes.

What competence criteria are required for AIMS auditors?

Auditors need expertise in AI governance, ISO/IEC 42001, and sector-specific standards. They must have four years of IT/data protection experience (at least two in AI), three days of AIMS training, and 30 audit days within five years. Lead auditors require leadership skills and experience in three ISO/IEC 42001 audits. Technical experts must have three years of sector-specific experience and understood AI audit principles (Application reviewers need documented experience in assessing management-system scopes and audit-time estimation.)

How is audit time calculated under Annex A of the standard?

Audit time under Annex A is determined first by consulting the baseline tables, which assign auditor-days according to the number of staff involved in AI lifecycle activities and their roles (for example, a producer with ten personnel requires five auditor-days, while a user organisation with twenty-five staff requires seven). This baseline is then adjusted to reflect factors such as AI system complexity (data volumes, algorithmic sophistication, regulatory overlays), multi-site or combined audit scopes, and any sector-specific extensions. Remote audit activities are allowed, provided that at least seventy per cent of the total audit time remains on-site (whether physically or via secure virtual presence).

(For surveillance audits, the baseline is reduced—typically to around half the original duration—then adjusted for any changes since the previous cycle, and re-certification audits follow a similar calculation to the initial assessment, accommodating new or expanded AI operations.)

What is the role of the Statement of Applicability (SoA) in AIMS certification?

The SoA documents controls implemented or excluded by an organization to meet ISO/IEC 42001 requirements. It justifies risk management measures and aligns with Annex A controls. Auditors review the SoA to verify compliance and ensure identified risks are addressed. The SoA must be updated for surveillance audits to reflect changes in the AIMS.

The Statement of Applicability (SoA) serves as the cornerstone of AIMS certification by clearly recording every control from Annex A of ISO 42001 that an organisation has chosen to apply or omit, together with the rationale for each decision. Under ISO 42006 (Clause 3.2) and in line with ISO 17021-1's requirements for documented information, the SoA must demonstrate how risk treatment options map to the Annex A controls and explain any exclusions based on risk assessment outcomes or external obligations. During Stage 1 of the certification audit, auditors use the SoA to verify that all significant AI risks have been identified and that the selected controls form a coherent, closed set capable of addressing those risks. Before each surveillance cycle, the organisation is obliged to update the SoA—in some cases obtaining formal top-management approval—so auditors can confirm that changes in processes, scope or external requirements continue to be appropriately reflected. In effect, the SoA provides a transparent, auditable trail from identified AI risks through risk treatment measures to the certification decision itself.

How does the standard handle multi-site or combined audits?

Multi-site audits follow ISO/IEC 17021-1, with sampling based on risk and uniformity. Combined audits (e.g., with ISO 27001) are allowed if AIMS-specific requirements are clearly documented and audit quality is maintained. Certification bodies must ensure integrated documentation distinctly identifies AIMS components and interfaces with other systems.

Multi-site audits under ISO 42006 adhere to the risk-based sampling and uniformity principles of ISO 17021-1 (Clause 9.1.6) and ISO 42006 Clause 9.1.7, using Annex A's guidance to select representative sites while ensuring consistent evaluation of AI lifecycle processes across locations. When combined with other management-system audits (for example ISO 27001), the certification body must preserve the integrity of AIMS requirements by maintaining separate audit scopes, reports and competence criteria as mandated by ISO 17021-1 Clause 9.1.7 and ISO 17021-3, clearly mapping interfaces between systems so that neither the AI-specific controls nor the overarching audit quality are compromised.

What are the stages of initial AIMS certification?

Initial certification under ISO 42006 (Clause 9.3) follows the two-stage model of ISO 17021-1 (Clauses 9.3.1–9.3.2). In **Stage 1**, auditors examine the organisation's AIMS documentation—including its Statement of Applicability, risk assessments and AI policies—to confirm readiness. Only once any minor nonconformities in documentation are resolved do they proceed to **Stage 2**, where control implementation is tested through interviews, system inspections and sample checks to validate compliance with ISO 42001. Major nonconformities discovered at either stage must be closed before the certificate can be issued. Thereafter, annual surveillance audits (ISO 42006 Clause 9.6.2) and full re-certification every three years (Clause 9.6.3) verify that the AIMS remains effective and up to date.

How does ISO/IEC DIS 42006 ensure confidentiality during audits?

Pre-audit agreements must define safeguards for sensitive information (e.g., source code, raw data). Certification bodies use contractual and technical measures to protect intellectual property while ensuring audit access. Confidentiality breaches can lead to assignment termination, reinforcing trust in the certification process.

What is the significance of sector-specific extensions in AIMS certification?

Sector-specific standards extend ISO/IEC 42001 Annex A controls for industries like healthcare or finance. Certification bodies must verify compliance with these extensions, which may add audit time or competence requirements. Although these extensions do not change the fundamental ISO 42001 framework, they provide the necessary depth to certify AIMS in highly regulated or specialised environments.

How does ISO/IEC DIS 42006 address remote audits, and what are the key considerations?

Remote audits are permitted but require a case-by-case risk assessment underpinned by ISO 17021-1 Clause 9.4 to ensure sufficient evidence is gathered. The standard mandates that at least 70% of audit time must be on-site (physical or virtual), with remote methods like web meetings supplementing the process.

Certification bodies must also establish and follow clear protocols for remote access, data security and session control, with audit plans detailing how each remote activity maintains both confidentiality (ISO 17021-1 Clause 8.4) and impartiality (Clause 5.2).

What are the requirements for certification bodies regarding liability and insurance under this standard?

Certification bodies must have liability insurance or an equivalent financial safeguard covering personal injury, property damage, and financial loss related to AI systems. The coverage amount should align with the turnover of their clients' AI-related activities. This ensures financial protection against potential claims arising from certification errors or omissions, reinforcing accountability.

How does the standard ensure the impartiality of certification bodies?

Impartiality is enforced through multiple safeguards in ISO 42006 (Clause 5.2) and ISO 17021-1 Clause 5.2: certification bodies must not offer consulting on AI management, data protection or risk management to the same organisations they audit, and internal audits of clients are expressly forbidden. Personnel assignments are managed to prevent bias—auditors, reviewers and decision-makers are kept independent—and the body must conduct regular impartiality reviews and maintain public records of potential conflicts of interest. These measures collectively guarantee that certification decisions rest solely on objective conformity assessments.

What role do technical experts play in AIMS audits, and what are their qualifications?

Technical experts support auditors by providing sector-specific or AI-related expertise during audits. They must have at least three years of experience in their field, basic AI terminology knowledge, and training in audit principles.

Although their findings inform the audit report, they operate strictly under the auditor's oversight and do not participate in the ultimate certification decision, safeguarding both impartiality and the integrity of conformity assessments.

How are nonconformities handled during AIMS certification audits?

Nonconformities are documented in audit reports, detailing the issue and required corrective actions. Clients must address minor nonconformities before certification, while major ones may delay the process. Surveillance audits verify ongoing compliance, and unresolved nonconformities can lead to certificate suspension or withdrawal. The standard emphasizes risk-based timelines for corrective actions, proportionate to the severity of the issue.

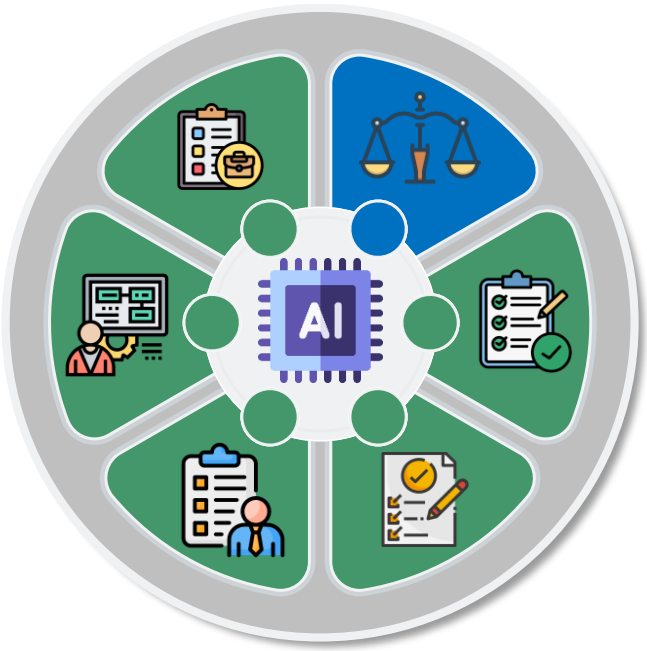
ISO 42006 (Clauses 9.4.3 and 9.6.5), aligned with ISO 17021-1 Clause 9.4, requires that all nonconformities—classified as minor or major—be recorded in the audit report with clear descriptions and prescribed corrective-action deadlines proportionate to their severity. Organisations must rectify minor nonconformities before certification can proceed, while major nonconformities must be closed to the satisfaction of the certification body before a certificate is issued or may otherwise delay or suspend the process. Subsequent surveillance (annual) and re-certification (every three years) audits revisit any outstanding issues to ensure that corrective measures remain effective and the AIMS continuously conforms to ISO 42001.

How is integration with other management-system audits achieved?

(Integration of AIMS audits with other management-system assessments—for example ISO 27001 or ISO 9001—is governed by ISO 42006 Clause 9.1.7 in conjunction with ISO 17021-1 Clause 9.1.7 and ISO 17021-3.) The certification body may conduct a single, combined audit visit provided that the scope, criteria and controls specific to the AI Management System remain clearly identified and are evaluated against ISO 42001's Annex A requirements without dilution. Audit planning must ensure that personnel assigned hold the requisite competences for each standard, that separate audit reports or distinct sections of a unified report document findings for each system, and that impartiality and audit quality are maintained throughout. In this way, organisations benefit from efficiency gains while still receiving a rigorous, standards-compliant evaluation of their AIMS alongside other management systems.

Understanding ISO/IEC DIS 42006

Principles



What are they?

The principles in ISO/IEC DIS 42006 are derived from ISO/IEC 17021-1 and serve as the foundation for auditing and certifying Artificial Intelligence Management Systems (AIMS). They include impartiality, competence, responsibility, openness, confidentiality, and responsiveness to complaints. These principles ensure that certification bodies operate ethically, maintain objectivity, and deliver reliable assessments. Impartiality prevents conflicts of interest, while competence guarantees auditors have the necessary AI and management system expertise.

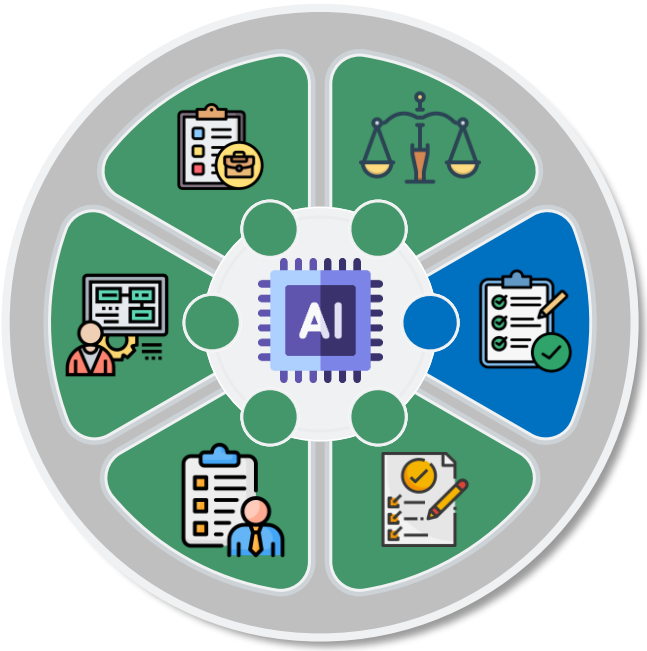
How do they apply?

The principles guide certification bodies in conducting audits and issuing AIMS certifications. Impartiality requires avoiding conflicts (e.g., no consulting for clients). Competence mandates auditors have AI-specific knowledge (e.g., risk management, ISO/IEC 42001). Responsibility ensures proper documentation and decision-making. Openness involves clear communication with clients about audit processes. Confidentiality safeguards proprietary AI data (e.g., algorithms, training data). Responsiveness ensures timely handling of appeals or complaints. These principles are enforced through documented procedures, auditor training, and accreditation body oversight to maintain certification integrity.

Why are they necessary

These principles are critical to ensuring credibility, trust, and consistency in AIMS certifications. AI systems involve high-stakes risks (e.g., bias, security breaches), so impartiality prevents biased assessments. Competence ensures auditors can evaluate AI-specific risks effectively. Responsibility and openness build stakeholder confidence in the process. Confidentiality protects intellectual property, encouraging organizations to seek certification. Responsiveness ensures fairness in resolving disputes. Without these principles, certifications could lack rigor, fail to mitigate AI risks, or lose recognition in the market, undermining the standard's purpose of promoting trustworthy AI management.

General Requirements



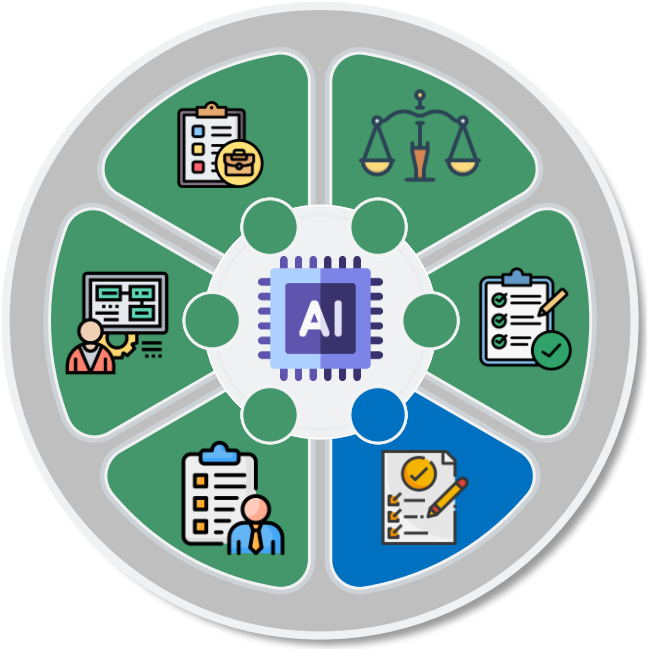
What are they?

The general requirements in ISO/IEC DIS 42006 outline the foundational obligations for certification bodies auditing AIMS. These include legal and contractual compliance, impartiality management, and liability/financial safeguards. Certification bodies must operate lawfully, avoid conflicts of interest (including a strict ban on internal audits and AI-related consulting), and secure insurance to cover potential damages. They must also ensure personnel competence, maintain confidentiality, and establish processes for appeals and complaints. These requirements align with ISO/IEC 17021-1 but include AI-specific adaptations, such as restrictions on consulting services.

Why are they necessary

They ensure credibility and accountability in AIMS certifications. Legal compliance prevents regulatory violations, while impartiality safeguards against biased audits. Liability coverage mitigates financial risks from AI-related incidents. Competence guarantees auditors can assess AI risks (e.g., bias, security), and confidentiality fosters trust by protecting proprietary data. Transparent appeals processes uphold fairness. Without these, certifications could lack rigor, expose stakeholders to unchecked AI risks, or fail to meet international standards—undermining trust in both the certification bodies and the organizations they certify.

Structural Requirements



What are they?

The structural requirements in ISO/IEC DIS 42006 define the organizational framework that certification bodies must establish to conduct AIMS audits effectively. These include governance structures, clearly defined roles and responsibilities, documented procedures for certification processes, and mechanisms for maintaining impartiality and competence. The standard mandates that certification bodies operate as legal entities with sufficient resources, qualified personnel, and management systems to ensure consistent and reliable audits. These requirements align with ISO/IEC 17021-1 but are tailored to address the complexities of AI management systems.

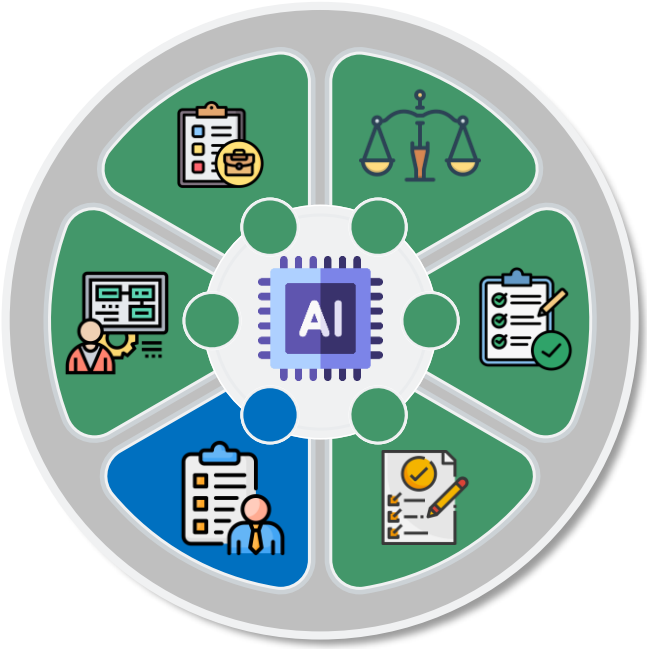
How do they apply?

Certification bodies must implement these structural requirements by establishing formal governance policies, assigning qualified personnel to audit roles, and maintaining documented procedures for all certification activities. They must ensure clear separation between auditing and consulting functions to prevent conflicts of interest. Additionally, they need systems for monitoring auditor competence, managing records, and handling appeals. These structures are applied throughout the certification lifecycle—from initial applications to surveillance audits—to ensure standardized, transparent, and impartial evaluations of an organization's AIMS compliance.

Why are they necessary

The structural requirements are essential for maintaining the integrity and reliability of AIMS certifications. A robust organizational framework ensures audits are conducted consistently and competently, which is critical given the technical and ethical complexities of AI systems. Clear governance prevents conflicts of interest, while documented procedures enhance transparency and accountability. Without these requirements, certification bodies might lack the necessary rigor to properly assess AI risks, leading to inconsistent or unreliable certifications that could undermine trust in both the certifying bodies and the organizations they evaluate.

Resource Requirements



What are they?

AI significantly challenges data protection principles under the GDPR by increasing the likelihood of re-identification of anonymized or pseudonymized data and enabling the inference of new personal data. This enhances risks to privacy, as individuals may be identified or profiled based on seemingly non-personal data. Consequently, GDPR provisions such as legal basis requirements, data subject rights, and safeguards for automated processing become increasingly relevant.

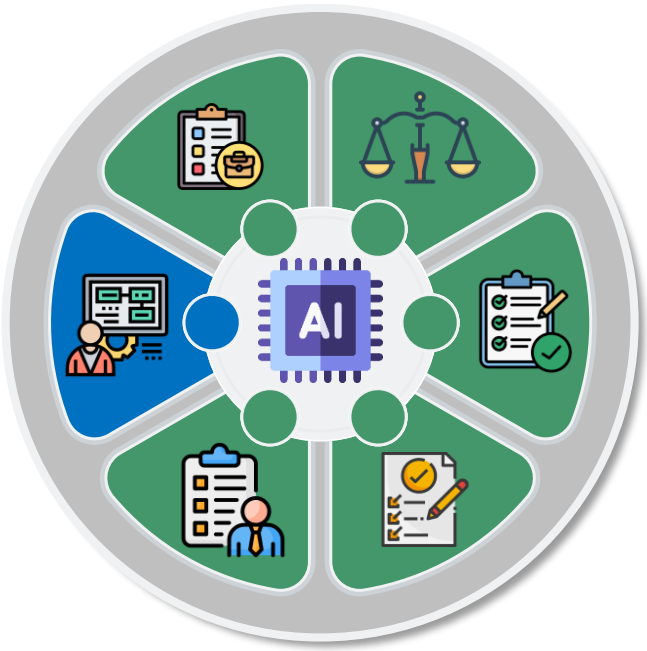
How do they apply?

AI-driven data processing makes personal data more dynamic and context-dependent. The GDPR's definition of personal data extends to identifiable and inferred information, meaning AI techniques can transform previously non-personal data into personal data. This affects compliance, requiring stricter security measures, transparency obligations, and regulatory oversight to prevent unauthorized re-identification and mitigate profiling risks.

Why are they necessary

The issue arises due to AI's capacity to analyze large datasets, detect correlations, and infer information beyond what was originally provided. Advances in machine learning and big data analytics have made it easier to associate disparate data points with individuals, undermining traditional anonymization techniques. As AI becomes more sophisticated, the GDPR's conceptual framework must adapt to ensure robust data protection and prevent misuse of inferred or re-identified data.

Information Requirements



What are they?

The information requirements in ISO/IEC DIS 42006 establish standards for how certification bodies must handle, document, and disclose information related to AIMS certification processes. These include requirements for public information about certification services, standardized certification documents (following Annex B templates), proper use of certification marks, confidentiality protocols for sensitive data, and procedures for information exchange with clients. The requirements ensure transparency in certification activities while protecting proprietary or confidential information related to AI systems and organizational processes.

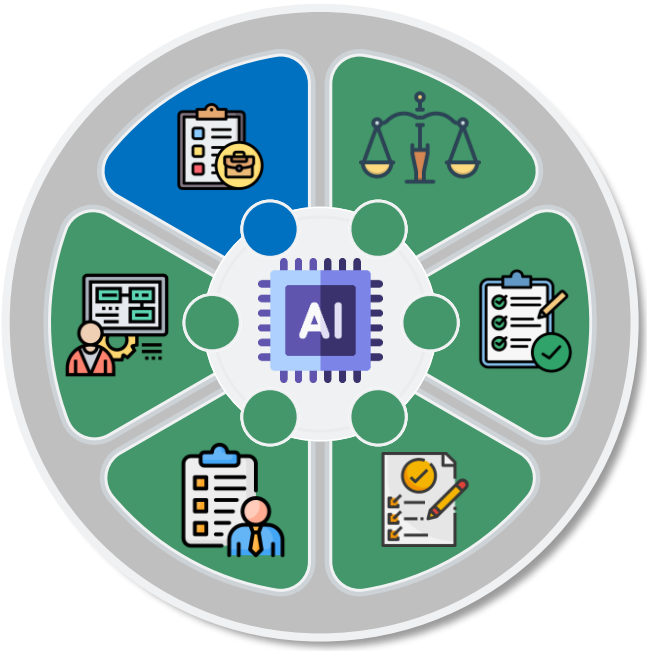
How do they apply?

Certification bodies must implement these requirements by maintaining publicly available information about their certification processes, issuing standardized certificates that comply with Annex B templates, and establishing secure protocols for handling confidential client information. They must define clear rules for using certification marks and maintain documented procedures for information sharing with clients throughout the audit process. These apply from initial application through surveillance audits, ensuring consistent information management while accommodating necessary access to sensitive AI system details during evaluations.

Why are they necessary

These requirements are essential for maintaining both transparency and confidentiality in AIMS certification. Standardized documentation ensures consistent interpretation of certification results across organizations and sectors, while confidentiality protections encourage companies to openly share sensitive AI system details needed for proper evaluation. Clear public information builds market confidence in the certification process, and proper mark usage prevents misrepresentation. Without these requirements, inconsistent information practices could undermine trust in certifications or discourage organizations from participating due to intellectual property concerns.

Process Requirements



What are they?

The process requirements in ISO/IEC DIS 42006 establish a comprehensive framework for conducting AIMS certifications, detailing procedures for pre-certification activities, audit planning, execution, and follow-up. These include a mandatory two-stage audit process (documentation review and on-site assessment), specific methodologies for evaluating AI system controls, protocols for handling non-conformities, and requirements for surveillance and re-certification. The standard also addresses remote audit capabilities, multi-site certification approaches, and integration with other management system audits while maintaining focus on AI-specific risks.

How do they apply?

These process requirements are implemented through structured audit programs where certification bodies must first assess documentation completeness (Stage 1) before verifying implementation effectiveness (Stage 2). Auditors use risk-based sampling to evaluate AI controls, with particular attention to data quality, algorithm validation, and ethical considerations. Findings are documented in standardized reports, and non-conformities trigger corrective action processes. Annual surveillance audits and triennial re-certifications ensure ongoing compliance. The requirements allow adaptation for different organizational sizes and sectors.

Why are they necessary

Process requirements are essential to ensure thorough, consistent, and credible evaluations of AI management systems. The structured approach addresses the unique challenges of AI systems, including their complexity, evolving nature, and potential societal impacts. Standardized methodologies enable comparable assessments across organizations while allowing necessary flexibility for different AI applications. The requirements maintain certification rigor, prevent oversight of critical AI risks, and build stakeholder confidence in certified AIMS. Without them, evaluations might lack consistency, or miss important AI-specific considerations.

Implementing ISO/IEC DIS 42006

Phase 1

Establishing the AI Governance Framework

This phase focuses on creating a solid foundation for ISO/IEC 42001 compliance by evaluating existing AI practices and defining governance structures. It ensures alignment with organizational goals and regulatory requirements.

☐ Conduct Initial Gap Analysis

Assess current AI governance against ISO/IEC 42001 standards:

- Identify gaps in policies, risk management, and compliance.
- Document existing AI workflows, data practices, and ethical guidelines.
- Engage leadership, IT, legal, and AI teams in the review process.
- Select an accredited certification body and plan the audit timeline.

☐ Define AI Governance Policies

Develop a formal AI management policy framework.

- Outline roles, responsibilities, and accountability for AI oversight.
- Establish ethical principles, risk tolerance, and compliance benchmarks.
- Align AI objectives with business strategy and regulatory requirements.
- Document processes for AI development, deployment, and monitoring.

☐ Launch Implementation Plan

Create a structured roadmap for achieving compliance.

- Assign cross-functional teams to lead governance, risk, and compliance efforts.
- Secure budget for training, tools, and certification costs.
- Set measurable milestones (e.g., policy approval, staff training, internal audits).

Phase 2

Implementing AI Controls & Processes

This phase operationalizes the governance framework by integrating ISO/IEC 42001 requirements into daily AI practices.

☐ Deploy Risk Mangement Measures

Establish risk assessment and mitigation strategies for AI systems.

- Implement controls for data quality (e.g., validation checks, bias detection tools).
- Establish security protocols for AI models and training datasets.
- Document risk treatment plans for high-impact scenarios (e.g., algorithmic bias)

☐ Train Teams on Compliance

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

- Conduct role-specific training (developers: technical standards; leadership).
- Simulate audit interviews and evidence collection processes.
- Certify internal auditors on ISO/IEC 42001 requirements.

☐ Document AI Lifecycle Processes

Standardise procedures from development to decommissioning.

- Create templates for model inventories, version control, and change logs.
- Define monitoring KPIs (e.g., accuracy decay, fairness metrics).
- Implement incident response protocols for AI failures.

Phase 3

Pre-Certification Readiness

This phase validates full compliance through internal audits and prepares for the formal certification process.

☐ Conduct Internal Audits

Verify implementation effectiveness before the external audit.

- Perform mock audits covering all ISO/IEC 42001 clauses.
- Prioritize high-risk areas (e.g., third-party AI tools, sensitive data flows).
- Document non-conformities and corrective actions in a tracking system.

☐ Finalise Statement of Applicability (SoA)

Formalise control implementation decisions.

- Justify inclusions/exclusions of Annex A controls with risk assessments.
- Map controls to specific AI systems and processes.
- Obtain executive approval for residual risk acceptance.

☐ Prepare Certification Audit Logistics

Coordinate with the certification body for smooth execution.

- Confirm audit dates, scope, and participant availability.
- Compile evidence bundles (policies, risk registers, training records).
- Designate escorts for auditor site visits (e.g., data labs, cloud environments).

Phase 4

Certification & Continuous Improvement

This phase achieves formal certification and embeds ongoing compliance through surveillance and iterative enhancements.

☐ Undergo Certification Audit

Complete the two-stage external assessment.

- **Stage 1 (Documentation Review)**: Validate SoA, policies, and readiness.
- **Stage 2 (Implementation Audit)**: Test control effectiveness via interviews, system checks, and sampling.

☐ Maintain Compliance

Ensure sustained adherence post-certification.

- quarterly internal reviews of AI systems and controls.
- Schedule annual surveillance audits with the certification body.
- Update the SoA when introducing new AI tools or regulatory changes.

☐ Drive Continuous Improvement

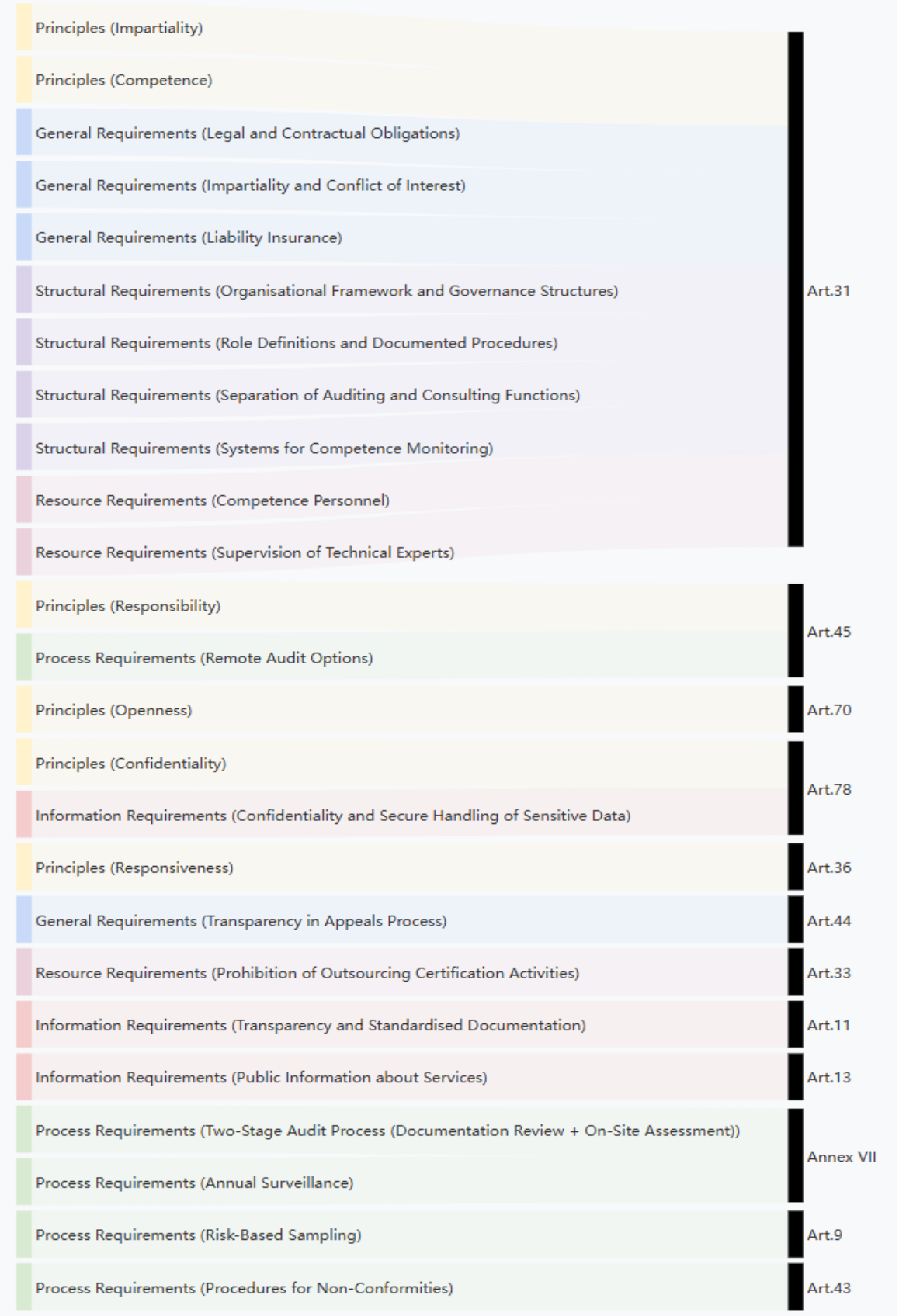
Leverage certification as a dynamic tool.

- Benchmark AI governance against emerging standards (e.g., EU AI Act).
- Incorporate audit learnings into AI development lifecycles.
- Share compliance metrics with stakeholders (e.g., board reports)

Mapping ISO/IEC DIS 42006 to EU AI Act

ISO/IEC DIS 42006

EU AI Act



ISO/IEC DIS 42006		EU AI Act		
Section	**Description**	**Focus**	**Article**	**Explanation**
Principles	The standard adopts core principles from ISO/IEC 17021-1, including **impartiality, competence, responsibility, openness, confidentiality, and responsiveness**. These ensure ethical, unbiased AIMS certifications by prohibiting conflicts of interest (e.g., no consulting for clients), mandating auditor expertise in AI governance, and safeguarding sensitive data.	Impartiality	**Article 31** (Requirements relating to Notified Bodies)	Article 31 of the EU AI Act emphasizes the independence of notified bodies from providers of high-risk AI systems. It mandates that these bodies must not be involved in the design, development, marketing, or use of the AI systems they assess, ensuring impartiality in conformity assessments.
		Competence	**Article 31** (Requirements relating to Notified Bodies)	Article 31 also requires notified bodies to have sufficient internal competences, including administrative, technical, legal, and scientific personnel with experience and knowledge related to AI systems. This aligns with the principle of competence, ensuring that assessments are conducted by qualified individuals.
		Responsibility	**Article 45** (Information obligations of Notified Bodies)	Article 45 outlines the information obligations of notified bodies, which include informing authorities about certificates issued, refused, or withdrawn. This reflects the principle of responsibility, as it ensures accountability in the certification process.
		Openness	**Article 70** (Designation of National Competent Authorities and single point of contact)	While the EU AI Act emphasizes confidentiality, it also requires transparency in certain aspects. For instance, Article 70 mandates that Member States make publicly available

				information on how competent authorities and single points of contact can be contacted 4. This aligns with the principle of openness by ensuring accessibility to relevant information.
		Confidentiality	**Article 78** (Confidentiality)	Article 78 of the EU AI Act explicitly requires the confidentiality of information obtained during conformity assessments, protecting intellectual property rights and trade secrets. This directly corresponds to the principle of confidentiality in ISO 42006.
		Responsiveness	**Article 36** (Changes to notifications)	Article 36 requires notifying authorities to assess the impact of any changes to notifications and to take appropriate steps to ensure the continued conformity of high-risk AI systems. This reflects the principle of responsiveness, as it involves timely actions to address changes and maintain compliance.
General Requirements	Certification bodies must comply with **legal/contractual obligations, manage impartiality, and secure liability insurance** for AI-related risks. They must avoid conflicts (e.g., no internal audits for clients) and ensure transparency in appeals processes.	Legal and Contractual Obligations	**Article 31** (Requirements relating to Notified Bodies)	Article 31 of the EU AI Act requires notified bodies to satisfy organizational, quality management, resources, and process requirements necessary to fulfil their tasks, ensuring they comply with legal and contractual obligations. This aligns with the requirement for certification bodies to comply with legal and contractual obligations under ISO 42006.

		Impartiality and Conflict of Interest	**Article 31** (Requirements relating to Notified Bodies)	Article 31 mandates that notified bodies must be independent of the providers of high-risk AI systems and any other operators with economic interests in those systems. They must not engage in activities that might conflict with their independence or integrity, such as consultancy services. This corresponds to the ISO 42006 requirement to manage impartiality and avoid conflicts of interest, such as conducting internal audits for clients.
		Liability Insurance	**Article 31** (Requirements relating to Notified Bodies)	Article 31 requires notified bodies to take out appropriate liability insurance for their conformity assessment activities unless liability is assumed by the Member State. This is directly related to the ISO 42006 requirement for certification bodies to secure liability insurance for AI-related risks.
		Transparency in Appeals Process	**Article 44** (Certificates)	Article 44 provides for an appeal procedure against decisions of notified bodies, including on conformity certificates issued. This ensures transparency in the appeals process, aligning with the ISO 42006 requirement for transparency in certification activities.
Structural Requirements	Defines the **organizational framework** for certification bodies, including governance structures, role	Organisational Framework and Governance Structures	**Article 31** (Requirements relating to Notified Bodies)	Article 31 of the EU AI Act outlines the requirements for notified bodies, including their

	definitions, and documented procedures. Requires clear separation of auditing/consulting functions and systems for competence monitoring.			establishment under national law and the need for a legal personality. This aligns with the ISO 42006 requirement for a defined organizational framework and governance structures for certification bodies.
		Role Definitions and Documented Procedures	**Article 31** (Requirements relating to Notified Bodies)	Article 31 also specifies that notified bodies must have documented procedures to ensure the confidentiality of information and maintain professional secrecy. This corresponds to the ISO 42006 requirement for documented procedures and role definitions within certification bodies.
		Separation of Auditing and Consulting Functions	**Article 31** (Requirements relating to Notified Bodies)	Article 31 mandates that notified bodies must be independent of the providers of high-risk AI systems and must not engage in activities that could conflict with their independence, such as consultancy services **5**. This directly aligns with the ISO 42006 requirement for a clear separation of auditing and consulting functions to ensure impartiality and integrity in audit processes.
		Systems for Competence Monitoring	**Article 31** (Requirements relating to Notified Bodies)	Article 31 requires notified bodies to have sufficient internal competences and to ensure that their personnel possess the necessary experience and knowledge related to AI systems **7**. This reflects the ISO 42006 requirement for systems to monitor

				and ensure competence within certification bodies.
Resource Requirements	Mandates **competent personnel** (e.g., auditors with 4+ years of IT experience, 2 in AI) and prohibits outsourcing of certification activities. Technical experts may support audits but require supervision.	Competence Personnel	**Article 31** (Requirements relating to Notified Bodies)	Article 31 of the EU AI Act requires notified bodies to have sufficient internal competences, including administrative, technical, legal, and scientific personnel with experience and knowledge related to AI systems. This aligns with the ISO 42006 requirement for auditors with specific IT and AI experience, ensuring that personnel involved in conformity assessments possess the necessary expertise.
		Prohibition of Outsourcing Certification Activities	**Article 33** (Subsidiaries of and Subcontracting by Notified Bodies)	Article 33 allows notified bodies to subcontract specific tasks but mandates that they ensure subcontractors meet the requirements laid down in Article 31 and take full responsibility for the tasks performed. While the EU AI Act permits subcontracting under strict conditions, it emphasizes maintaining control and responsibility, which aligns with the ISO 42006 focus on direct control over audits.
		Supervision of Technical Experts	**Article 31** (Requirements relating to Notified Bodies)	Article 31 requires notified bodies to document and implement structures and procedures to safeguard impartiality and promote competence throughout their organization and

				assessment activities. This includes ensuring that any technical experts involved in audits are adequately supervised, aligning with the ISO 42006 requirement for supervision of technical experts supporting audits.
Information Requirements	Covers **transparency and confidentiality**, requiring standardized certification documents (per Annex B), public information about services, and secure handling of sensitive AI data (e.g., algorithms).	Transparency and Standardised Documentation	**Article 11** (Technical documentation)	Article 11 requires the technical documentation of high-risk AI systems to be comprehensive and up-to-date, demonstrating compliance with the Act's requirements. This aligns with ISO 42006's emphasis on standardized certification documents, ensuring that all necessary information is available for assessment and compliance verification.
		Public Information about Services	**Article 13** (Transparency and provision of information to deployers)	Article 13 mandates that high-risk AI systems be accompanied by clear and accessible instructions for use, including information on the system's characteristics, capabilities, and limitations. This requirement ensures that deployers and the public have access to relevant information, aligning with ISO 42006's focus on public information about services.
		Confidentiality and Secure Handling of Sensitive Data	**Article 78** (Confidentiality)	Article 78 emphasizes the confidentiality of information obtained during conformity assessments, protecting intellectual property rights and

				trade secrets **3**. This directly corresponds to ISO 42006's requirement for secure handling of sensitive AI data, such as algorithms, balancing disclosure with IP protection.
Process Requirements	Outlines a **two-stage audit process** (documentation review + on-site assessment), risk-based sampling, and procedures for nonconformities. Includes remote audit options and annual surveillance.	Two-Stage Audit Process (Documentation Review + On-Site Assessment)	**Annex VII** (Conformity based on an assessment of the quality management system and an assessment of the technical documentation)	Annex VII of the EU AI Act outlines the conformity assessment procedure, which includes an assessment of the quality management system and technical documentation. This aligns with the two-stage audit process in ISO 42006, where documentation review is a critical component of the conformity assessment.
		Risk-Based Sampling	**Article 9** (Risk management system)	Article 9 of the EU AI Act requires a risk management system for high-risk AI systems, which involves identifying and analysing risks throughout the AI system's lifecycle. This risk-based approach is consistent with the risk-based sampling methodology in ISO 42006, ensuring that audits focus on areas of higher risk.
		Procedures for Non-Conformities	**Article 43** (Conformity assessment)	Article 43 outlines the conformity assessment procedures, including the involvement of notified bodies to ensure compliance with the requirements. If nonconformities are identified, the notified body must refuse to issue a certificate and provide detailed reasons, which aligns with ISO 42006's procedures for

			addressing nonconformities.
	Remote Audit Options	**Article 45** (Information obligations of Notified Bodies)	While the EU AI Act does not explicitly mention remote audits, Article 45 allows for information sharing and cooperation between notified bodies and market surveillance authorities, which can facilitate remote assessments. This flexibility supports the remote audit options outlined in ISO 42006.
	Annual Surveillance	**Annex VII** (Conformity based on an assessment of the quality management system and an assessment of the technical documentation)	Annex VII specifies that notified bodies must carry out periodic audits to ensure the provider maintains and applies the quality management system. This requirement for ongoing surveillance aligns with ISO 42006's emphasis on annual surveillance to ensure continuous compliance.

Calls to action

1. Adopt ISO 42001 with ISO 42006-Certified Audits

Ensure your AI Management System (AIMS) meets global standards by working with ISO/IEC 42006-compliant certification bodies. Strengthen governance, mitigate AI risks, and streamline compliance with regulations like the EU AI Act through credible, impartial audits that adhere to ISO 42006's rigorous principles.

2. Conduct a Gap Analysis with ISO 42006-Aligned Auditors

Prepare for certification by engaging auditors trained under ISO/IEC 42006 to assess your AIMS against ISO 42001 and the EU AI Act. Identify gaps, prioritize corrective actions, and build a compliance roadmap backed by standardized audit methodologies.

3. Embed Transparency via ISO 42006 Certification

Leverage ISO 42006-certified audits to validate your AIMS's explainability, fairness, and accountability measures. Certification bodies under this standard follow strict documentation and confidentiality protocols (Section 8.4) to protect IP while demonstrating compliance.

4. Strengthen Risk Monitoring with Certified Surveillance

Proactively monitor your AIMS using ISO 42006's surveillance processes (Section 9.6). Annual audits ensure continuous adherence to risk controls, addressing evolving threats like algorithmic bias or data security breaches.

5. Partner with AI Governance Experts

Collaborate with certification bodies compliant with ISO/IEC 42006 to navigate AIMS certification and regulatory requirements. Their expertise in AI governance, audit planning, and corrective action management ensures a seamless path to compliance.

Conclusion

ISO/IEC 42001:2023 represents a watershed moment in establishing structured, ethical AI governance through its AI Management System (AIMS) framework. As organizations globally navigate the dual imperatives of AI innovation and risk management, this standard provides the blueprint for implementing robust governance systems. However, the true measure of its impact lies in effective implementation - and this is where ISO/IEC 42006 plays a pivotal role.

The certification framework established by ISO 42006 ensures that AIMS audits are conducted by bodies with:

- Demonstrated AI-specific expertise (Table 1 competence requirements)
- Rigorous methodologies (two-stage audit process)
- Strict impartiality safeguards (Section 5.2 conflict-of-interest rules)

For organizations implementing ISO 42001, working with ISO 42006-compliant certification bodies offers:

- **Credible Validation** of their AIMS against both the standard and regulations like the EU AI Act
- **Risk-Based Assessments** through Annex A's audit time calculations
- **Ongoing Compliance** via annual surveillance audits (Section 9.6)

While adoption challenges exist - particularly for SMEs in aligning existing governance structures - early adopters across tech, finance, and healthcare are demonstrating the value of ISO 42001 when paired with ISO 42006-certified audits. These organizations are:

- Streamlining compliance with emerging regulations
- Building stakeholder trust through third-party verified governance
- Implementing continuous improvement processes (Section 9.6.3)

Looking ahead, the synergy between ISO 42001's framework and ISO 42006's certification requirements will be crucial for:

- Maintaining audit consistency as the standard evolves
- Ensuring interoperability with other AI regulations
- Scaling adoption across industries and organization sizes

Organizations that embrace both standards position themselves as leaders in responsible AI, with certification serving as both a compliance tool and competitive differentiator. As AI systems grow more complex, this dual approach - robust AIMS implementation verified through standardized audits - will become the global benchmark for trustworthy 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 5th April 2025)

International Organization for Standardization, (2025), 'ISO/IEC FDIS 42006Information technology — Artificial intelligence — Requirements for bodies providing audit and certification of artificial intelligence management systems', accessible at: https://www.iso.org/standard/44546.html (last accessed 5th April 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