AI & Partners

Amsterdam - London - Singapore

EU AI Act

ISO/IEC FDIS 42005 – Impact Assessments of AI Systems

A Guide to Implementation

May 2025

AI & Partners

Sean Musch, AI & Partners

Michael Borrelli, AI & Partners

Charles Kerrigan, CMS UK

Martin Ebers, Robotics & AI Law Society

Nadir Ali, Global AI & FinTech Advisor

ISO 42005

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 robust frameworks to ensure AI systems are trustworthy, effective, and aligned with human values. ISO 42005 provides a systematic approach to AI management systems, offering guidance for the governance, oversight, and continual improvement of AI capabilities across their lifecycle.

This report examines the core principles, implementation strategies, and organizational impacts of ISO 42005, delivering practical insights for entities aiming to operationalize trustworthy AI. From transparency and accountability to ongoing performance evaluation, the standard lays the groundwork for structured AI management aligned with internationally recognized best practices.

With rising global attention to AI governance—such as the EU AI Act and other emerging regulations—organizations are under increasing pressure to establish clear accountability and demonstrable control over their AI systems. By implementing ISO 42005, businesses can build confidence with stakeholders, strengthen operational integrity, and align with evolving regulatory and ethical expectations.

Whether you are designing AI systems, overseeing digital transformation, or shaping policy, this report is a strategic resource for interpreting and applying ISO 42005. At AI & Partners, we are committed to guiding organizations in deploying AI that is responsible, resilient, and in harmony with global standards for AI management.

Best regards,

Sean Musch

Founder/CEO

AI & Partners

Key questions being asked about ISO/IEC FDIS 42005

What is the main purpose of ISO 42005?

ISO 42005 aims to provide a standardized framework for managing data quality within complex systems, particularly those incorporating smart technologies and precision-based approaches. It outlines principles and guidelines to ensure that data collected, processed, and shared across value chains is reliable, traceable, and fit for purpose. By doing so, it enhances decision-making, promotes interoperability among systems, and supports sustainability and innovation across industries. It's essential for stakeholders involved in data-driven practices.

Who are the primary stakeholders of ISO 42005?

The primary stakeholders include system operators, domain experts, equipment manufacturers, data service providers, regulatory bodies, and researchers. Each plays a unique role in generating, managing, or using data. ISO 42005 provides guidance tailored to these diverse needs, encouraging collaboration across the data lifecycle. It emphasizes transparency, accountability, and trust, enabling stakeholders to benefit from improved data quality and interoperability while maintaining appropriate control and understanding of the data they generate or use.

How does ISO 42005 define data quality?

ISO 42005 defines data quality as the degree to which data is suitable for its intended use, focusing on aspects like accuracy, completeness, consistency, timeliness, and traceability. It recognizes that poor data quality can lead to misinformed decisions, inefficiencies, and loss of trust. The standard emphasizes context-specific assessment, where data quality must be evaluated based on how well it supports a particular task or decision. High-quality data must be both technically correct and operationally useful.

Why is traceability emphasized in ISO 42005?

Traceability in ISO 42005 ensures that the origin, history, and modifications of data can be tracked and verified. This is especially critical when data is shared across systems and stakeholders. It helps identify sources of errors, ensures compliance with regulations, and builds trust among data users. Traceability supports transparency, accountability, and informed decision-making. It also helps in attributing value or responsibility correctly, particularly in collaborative or multi-party environments.

How does ISO 42005 address data sharing challenges?

ISO 42005 tackles data sharing by recommending clear protocols, metadata standards, and mutual agreements that define access rights, ownership, and responsibilities. It highlights the importance of understanding data provenance and context to avoid misinterpretation. The standard also encourages trust frameworks and transparency between parties. By promoting interoperability and consistent data practices, ISO 42005 reduces technical and organizational barriers, enabling secure and effective data exchange in complex networks.

What role do metadata and documentation play in ISO 42005?

Metadata and documentation are central to ISO 42005, as they provide the context necessary to interpret and reuse data accurately. The standard requires comprehensive metadata to accompany data, detailing its source, collection methods, processing history, and applicable conditions. This enables users to assess data relevance and reliability for their specific use cases. Proper documentation ensures consistency, supports traceability, and facilitates integration across platforms. It also helps future-proof data assets by preserving contextual knowledge over time.

How does ISO 42005 support smart technologies?

ISO 42005 supports smart systems by offering a framework to manage complex data flows from sensors, machinery, and digital platforms. It ensures that data generated by IoT devices and automated systems is of high quality and usable for decision-making. By promoting standards for data formats, quality assessment, and traceability, it enhances interoperability among tools and systems. This leads to more efficient resource use, better performance insights, and improved outcomes in data-driven operations.

How is data lifecycle management addressed in ISO 42005?

ISO 42005 treats data lifecycle management as a structured process encompassing data creation, collection, storage, processing, sharing, and archiving or disposal. It emphasizes maintaining data quality throughout each stage and ensuring alignment with intended purposes. The standard promotes best practices like routine validation, secure storage, controlled access, and proper decommissioning of outdated data. Lifecycle thinking helps avoid data degradation, ensures relevance, and supports long-term usability—key for managing large volumes of data over time.

How can ISO 42005 help build trust in data systems?

By providing clear guidelines on data quality, transparency, traceability, and stakeholder responsibilities, ISO 42005 fosters trust among data producers and users. It encourages open communication about how data is collected and used, enabling stakeholders to make informed decisions with confidence. Trust is especially important in collaborative networks where data crosses organizational boundaries. By standardizing expectations and practices, ISO 42005 reduces uncertainty, mitigates risks, and builds a reliable foundation for data sharing and cooperation.

What are the benefits of implementing ISO 42005 in operations?

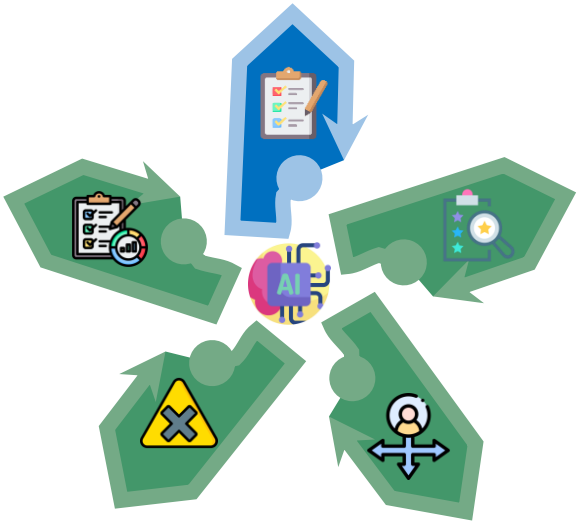
Implementing ISO 42005 brings numerous benefits, including improved data-driven decision-making, greater efficiency, enhanced traceability, and better compliance with regulatory or market requirements. It supports sustainable practices by enabling precise resource use and monitoring impacts. Standardized practices also reduce data silos and foster innovation through interoperability. For enterprises and policymakers, it provides a trustworthy framework for managing digital transformation. Ultimately, it empowers organizations to leverage data as a strategic asset responsibly and effectively.

How does ISO 42005 relate to the EU AI Act and potential European harmonized standards?

ISO 42005 provides a globally oriented framework for data quality management, but its relationship with the EU AI Act remains indirect and currently undefined. While the standard supports foundational principles relevant to trustworthy AI — such as data traceability, transparency, and accountability — it is not formally harmonized with the EU AI Act. Based on developments within European standardization bodies like CEN/CENELEC JTC 21, it is expected that dedicated harmonized standards will be developed to support compliance with the AI Act. These may reference ISO/IEC standards like ISO 42005 but could diverge significantly, especially in areas such as AI impact assessments. As of now, the European Commission has not issued a formal standardization request specific to this area, leaving the alignment between ISO 42005 and EU AI governance frameworks an open and evolving issue.

Understanding ISO/IEC FDIS 42005

Implementing an AI Impact Assessment Process



What is involved?

Implementing an AI Impact Assessment (AIIA) process involves identifying potential ethical, legal, social, and technical impacts of an AI system throughout its lifecycle. This includes data governance, fairness, accountability, transparency, safety, and human rights considerations. The process typically integrates stakeholder consultation, risk assessment tools, documentation, and alignment with existing regulatory frameworks. It ensures that AI systems are developed responsibly, that potential harms are mitigated, and that the outcomes align with organizational values and societal expectations.

How does it happen?

The AIIA process begins with scoping the AI system's purpose, context, and stakeholders. Then, a multidisciplinary team evaluates the AI's potential impacts using structured frameworks and tools. This includes assessing data sources, algorithms, deployment environments, and decision-making risks. Key activities include stakeholder engagement, scenario analysis, and reviewing for bias or discrimination. The findings are documented, and mitigation strategies are developed. The process is iterative—revisited during development, deployment, and post-implementation—to ensure continued alignment with legal standards.

Why is it needed?

An AI Impact Assessment is essential to ensure AI systems are developed and used responsibly. It helps identify and address risks such as bias, privacy breaches, or unintended harms before they escalate. The process builds trust among users, regulators, and the public by demonstrating transparency and accountability. It also supports compliance with emerging AI regulations and international standards. Ultimately, it guides the ethical design and use of AI, safeguarding human rights and promoting beneficial, inclusive outcomes for society.

Documenting an AI Impact Assessment Process

What is involved?

Documenting an AI Impact Assessment involves creating a detailed, structured record of the assessment process, findings, and decisions made throughout the AI system's development and use. This includes the system's purpose, potential risks and impacts, stakeholder input, mitigation strategies, and compliance steps. The documentation should be clear, comprehensive, and accessible to both internal teams and external auditors or regulators. It forms the basis for accountability, continuous improvement, and transparency, supporting trust in the responsible use of AI.

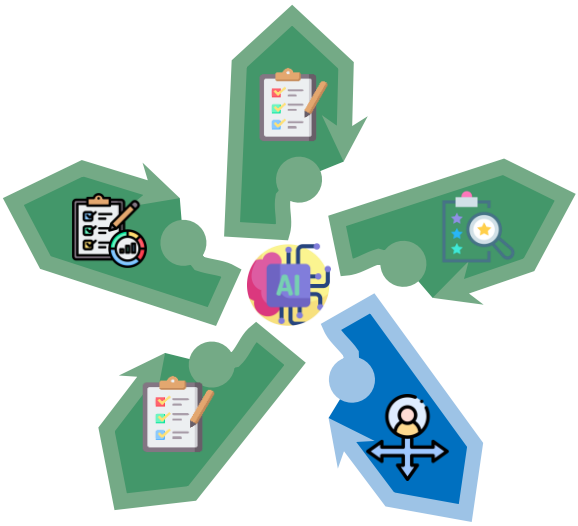
How does it happen?

Documentation begins alongside the assessment process and continues throughout the AI system's lifecycle. Teams compile structured reports that include impact analyses, risk mitigation plans, stakeholder consultations, and changes over time. Tools such as standardized templates, checklists, and audit trails help ensure consistency and completeness. This documentation is version-controlled and regularly updated as the system evolves. Ideally, it's maintained by a dedicated governance or ethics team and shared across relevant departments to ensure alignment and informed decision-making.

Why is it needed?

Documenting the AI Impact Assessment process is essential for demonstrating transparency, accountability, and due diligence. It provides traceability for decisions, supports internal governance, and enables external compliance with regulations such as the EU AI Act or ISO standards. Proper documentation also helps identify gaps, supports audits, and informs future assessments. It reassures stakeholders—users, partners, and regulators—that risks are being actively managed. Ultimately, it enhances trust in AI systems and helps prevent reputational, legal, or ethical failures.

Guidance for Use with ISO/IEC 42001



What is involved?

Guidance for use with ISO/IEC 42001 involves providing practical instructions, recommendations, and examples to help organizations implement an AI Management System (AIMS) in alignment with the standard. This includes interpreting the standard's requirements, integrating AI-specific risks and opportunities into management practices, and establishing governance structures. It also supports the implementation of policies, objectives, and continuous improvement processes tailored to AI. The guidance ensures organizations apply ISO/IEC 42001 effectively, regardless of industry, size, or AI maturity level.

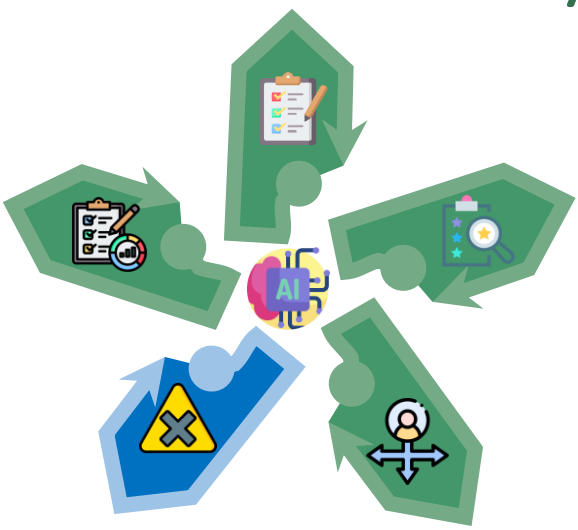
How does it happen?

The guidance is applied during the planning and implementation of an AI Management System, offering step-by-step support for fulfilling ISO/IEC 42001 clauses. It typically includes use cases, illustrative procedures, and templates for documentation. Organizations use it to align internal processes with the standard's requirements—such as leadership commitment, risk management, and operational controls—while addressing AI-specific concerns. Training sessions, workshops, and gap assessments often accompany the guidance, helping teams translate abstract requirements into practical, actionable steps.

Why is it needed?

Guidance for use with ISO/IEC 42001 is needed to bridge the gap between the standard's high-level requirements and real-world implementation. It helps organizations interpret complex concepts, such as AI governance or ethical risk management, and apply them consistently. This ensures a smoother, more effective adoption of the AI Management System, reducing compliance risks and enhancing operational integrity. The guidance also supports scalability and repeatability, enabling diverse organizations to align with best practices and build trustworthy, transparent AI systems.

Harms and Benefits Taxonomy



What is involved?

A Harms and Benefits Taxonomy involves classifying the potential positive and negative impacts of AI systems across ethical, social, legal, economic, and environmental dimensions. It provides a structured way to identify, categorize, and assess possible outcomes such as discrimination, privacy violations, job displacement, innovation, or efficiency gains. The taxonomy serves as a tool for organizations to systematically evaluate AI impacts and align them with their risk management and value creation strategies within an AI Management System.

How does it happen?

The taxonomy is developed through interdisciplinary collaboration, drawing on ethical frameworks, stakeholder input, and regulatory guidelines. Organizations use it during AI design, development, and deployment phases to map risks and benefits across domains—individual, societal, economic, and ecological. It often includes indicators or criteria for impact severity, likelihood, and affected populations. This structured approach enables transparent trade-off analysis, prioritization of mitigation efforts, and documentation within impact assessments, helping to ensure AI systems serve the public good responsibly.

Why is it needed?

A Harms and Benefits Taxonomy is crucial for embedding ethical foresight and accountability into AI development. It helps organizations move beyond technical performance metrics to consider broader implications of their systems. By identifying potential harms and benefits early, teams can proactively mitigate risks, maximize positive outcomes, and comply with legal and societal expectations. It also enhances stakeholder trust by demonstrating a thoughtful, systematic approach to ethical impact evaluation—critical for responsible AI under standards like ISO/IEC 42001.

Aligning AI System Impact Assessment with other Assessments

What is involved?

Aligning AI System Impact Assessments with other assessments means integrating AI-specific evaluations—such as ethical, societal, or technical risks—into broader organizational frameworks like privacy impact assessments (PIAs), data protection impact assessments (DPIAs), cybersecurity audits, or environmental assessments. This approach ensures consistency, reduces duplication, and embeds AI considerations into enterprise-wide governance. It involves mapping overlapping areas, identifying shared controls, and streamlining documentation to create a cohesive risk and impact management structure that supports both compliance and organizational goals.

How does it happen?

This alignment occurs by cross-referencing AI impact assessment elements with existing organizational risk frameworks. For example, privacy risks identified in a DPIA can inform the AI assessment process, while cybersecurity controls can be extended to AI-specific vulnerabilities. Cross-functional teams collaborate to harmonize templates, workflows, and review cycles. Tools and checklists are adapted to address shared concerns, and documentation is centralized to enhance traceability. Ultimately, the process becomes more efficient and integrated into broader compliance, safety, and ethics practices.

Why is it needed?

Alignment is essential to avoid fragmented governance, conflicting controls, or redundant assessments. As AI systems intersect with multiple domains—privacy, security, human rights—unified assessments ensure all relevant risks are addressed holistically. This improves regulatory readiness, supports informed decision-making, and reduces administrative burden. It also fosters a culture of integrated responsibility across departments. In the context of ISO/IEC 42001, alignment enhances the effectiveness of an AI Management System by embedding AI oversight within the organization's existing governance and assurance ecosystem.

Implementing ISO/IEC FDIS 42005

Phase 1

Establishing the AI Governance Framework

This phase focuses on creating a solid foundation for ISO 42005 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

Operationalizing AI Management Processes

This phase focuses on translating governance policies into actionable processes and integrating them into day-to-day operations. It ensures that AI systems are managed consistently, transparently, and in line with ISO 42005 requirements.

☐ Develop AI Lifecycle Controls

Implement controls for each phase of the AI system lifecycle:

- Define checkpoints for data sourcing, model development, validation, and deployment.
- Establish protocols for human oversight and fallback mechanisms.
- Integrate version control and change management for AI systems.

☐ Embed Risk and Impact Assessments

Operationalize AI risk and impact evaluation procedures.

- Incorporate AI risk assessments into product and project workflows.
- Apply impact assessments for ethical, legal, and social dimensions.
- Prioritize high-risk use cases and define mitigation strategies.

☐ Establish Monitoring and Reporting Mechanisms

Set up processes for continuous monitoring and performance evaluation.

- Implement tools to track AI behaviour, data drift, and model performance.
- Define KPIs for fairness, accuracy, and compliance.
- Automate reporting to support internal reviews and external audits.

Phase 3

Training, Awareness, and Cultural Integration

This phase ensures that AI governance is embraced organization-wide through education, communication, and cultural alignment. It builds competence and accountability across all teams interacting with AI.

☐ Deliver Role-Based Training

Equip staff with knowledge aligned to their roles.

- Provide foundational AI ethics and governance training to all employees.
- Offer specialized modules for developers, data scientists, and compliance officers.
- Include case studies, legal context, and real-world applications.

☐ Foster a Responsible AI Culture

Promote ethical awareness and shared accountability.

- Communicate the organization's AI values and governance commitments.
- Encourage open dialogue on AI risks, concerns, and improvements.
- Recognize and reward responsible innovation practices.

☐ Establish Communication and Engagement Channels

Facilitate ongoing stakeholder engagement.

- Create internal forums or steering groups for AI governance updates.
- Share progress toward ISO 42005 goals with employees and partners.
- Encourage reporting of AI-related issues via anonymous channels.

Phase 4

Continuous Improvement & Certification

This phase prepares the organization for ISO 42005 certification and drives long-term excellence in AI governance through regular reviews, audits, and iterative enhancements.

☐ Conduct Internal Audits and Readiness Reviews

Evaluate preparedness for third-party certification.

- Audit adherence to AI governance policies and lifecycle controls.
- Identify process gaps, non-conformities, and areas for improvement.
- Run mock audits to test documentation, monitoring, and incident response.

☐ Refine and Optimize Governance Processes

Incorporate feedback and adapt to evolving needs.

- Use audit results, stakeholder input, and performance data to refine policies.
- Stay informed on updates to ISO 42005 and related AI regulations.
- Implement process automation and scalability improvements.

☐ Engage Certification Body and Finalize Audit

Complete final steps toward ISO 42005 certification.

- Submit documentation and self-assessment to the chosen certifier.
- Participate in the certification audit and address corrective actions.
- Plan for recertification and ongoing compliance monitoring.

Mapping ISO/IEC FDIS 42005 to EU AI Act

ISO/IEC FDIS 42005	EU AI Act
Implementing an AI Impact Assessment Process (Identifying Stakeholders)	
Implementing an AI Impact Assessment Process (Defining the Scope of the Assessment)	
Implementing an AI Impact Assessment Process (Analysing Risks and Benefits)	
Implementing an AI Impact Assessment Process (Integrating Results into Decision-Making)	
Documenting an Ai Impact Assessment Process (Internal Governance and External Audits)	Art.27
Aligning AI System Impact Assessment with Other Assessments (Data Protection Impact Assessments (DPIAs))	
Aligning AI System Impact Assessment with Other Assessments (Human Rights Impact Assessments)	
Aligning AI System Impact Assessment with Other Assessments (Environmental Assessments)	
Aligning AI System Impact Assessment with Other Assessments (Integrated Risk and Compliance Strategies)	
Documenting an Ai Impact Assessment Process (Objectives and Methodologies)	Art.11
Documenting an Ai Impact Assessment Process (Findings and Decisions)	Annex IV
Documenting an Ai Impact Assessment Process (Transparency and Accountability)	R.71
Documenting an Ai Impact Assessment Process (Traceability)	
Guidance for Use with ISO/IEC 42001 (Alignment with Organisational Roles)	Art.17
Guidance for Use with ISO/IEC 42001 (Lifecycle Stages)	
Guidance for Use with ISO/IEC 42001 (Risk Management Practices)	Art.9
Harms and Benefits Taxonomy (Evaluating Trade-Offs)	
Guidance for Use with ISO/IEC 42001 (Cohesive AI Governance Structure)	Annex VII
Harms and Benefits Taxonomy (Classification of Harms)	Art.6
	Art.10
Harms and Benefits Taxonomy (Classification of Benefits)	Art.1
Harms and Benefits Taxonomy (Prioritising Mitigation Efforts)	Art.14

Disclaimer:

While ISO 42005 offers valuable guidance on data quality management and aligns with principles relevant to trustworthy and responsible data use, it is important to note that ISO standards do **not** confer a *presumption of conformity* under the EU AI Act. Only **European harmonized standards**, as defined in Article 40 of the AI Act, have that legal effect. Nevertheless, ISO 42005 may still serve as a useful reference for organizations aiming to align with the AI Act — particularly in areas where harmonized standards are not yet available — by demonstrating adherence to recognized best practices and risk mitigation approaches.

ISO/IEC FDIS 42005		EU AI Act		
Section	Description	Focus	Article	Explanation
Implementing an AI Impact Assessment Process	This section outlines how organizations can systematically evaluate the potential impacts of AI systems. It involves identifying stakeholders, defining the scope of the assessment, analysing risks and benefits, and integrating results into decision-making. The goal is to ensure that AI deployments are aligned with ethical, legal, and societal expectations.	Identifying Stakeholders	**Article 27** (Fundamental Rights Impact Assessment for High-Risk AI Systems)	Article 27 of the EU AI Act mandates a fundamental rights impact assessment for high-risk AI systems. This assessment requires identifying the categories of natural persons and groups likely to be affected by the AI system. This aligns with the ISO requirement to identify stakeholders.
		Defining the Scope of the Assessment	**Article 27** (Fundamental Rights Impact Assessment for High-Risk AI Systems)	The EU AI Act requires a detailed description of the deployer's processes in which the high-risk AI system will be used, including its intended purpose and the frequency of use. This corresponds to defining the scope of the assessment in ISO 42005.
		Analysing Risks and Benefits	**Article 27** (Fundamental Rights Impact Assessment for High-Risk AI Systems)	The EU AI Act necessitates an assessment of specific risks of harm likely to impact the identified categories of persons, taking into account information provided by the AI system provider. This is similar to analysing risks and benefits as outlined in ISO 42005.
		Integrating Results into Decision-Making	**Article 27** (Fundamental Rights Impact Assessment for High-Risk AI Systems)	The EU AI Act requires deployers to notify the market surveillance authority of the results of the fundamental rights impact assessment and to take necessary measures if risks materialize. This step ensures that the assessment results are integrated into decision-making processes, aligning with the ISO requirement.
Documenting an Ai Impact Assessment Process	Focuses on the importance of clearly recording all aspects of the AI impact assessment—such as objectives, methodologies, findings, and decisions. Proper documentation	Objectives and Methodologies	**Article 11** (Technical documentation)	Article 11 of the EU AI Act requires the technical documentation of high-risk AI systems to be comprehensive and demonstrate compliance with the requirements set

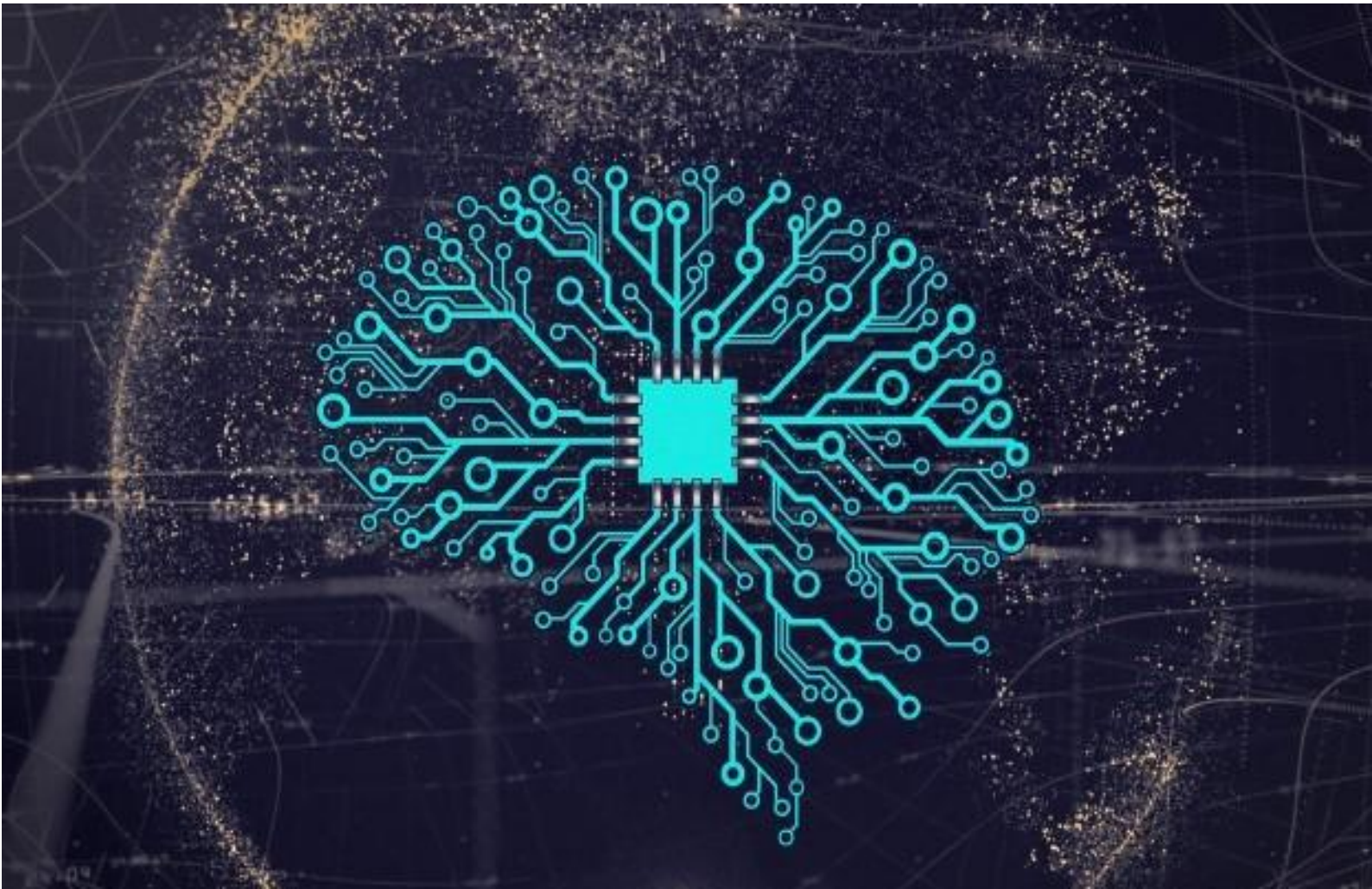
	ensures transparency, accountability, and traceability, supporting both internal governance and external audits.			out in the Act. This includes a detailed description of the AI system's development process, design specifications, and methodologies used. This aligns with the ISO 42005 emphasis on documenting objectives and methodologies.
		Findings and Decisions	**Annex IV** (Technical documenta on referred to in Article 11(1))	Annex IV specifies that the technical documentation must include validation and testing procedures, metrics used to measure accuracy and robustness, and potentially discriminatory impacts. This requirement ensures that findings and decisions are well-documented, supporting transparency and accountability.
		Transparenc y and Accountabili ty	**Recital 71**	Recital 71 highlights the importance of having comprehensible information on how high-risk AI systems are developed and perform throughout their lifecycle, which is essential for traceability and compliance verification. This reflects the ISO 42005 focus on transparency and accountability.
		Internal Governance and External Audits	**Article 27** (Fundamental Rights Impact Assessment for High-Risk AI Systems)	Article 27 mandates a fundamental rights impact assessment for high-risk AI systems, which includes documenting the deployer's processes and the specific risks of harm. This documentation supports internal governance and can be used in external audits, aligning with ISO 42005's objectives.
		Traceability	**Recital 71**	The requirement for technical documentation to be kept up to date and to include information necessary for post-market

				monitoring ensures traceability of high-risk AI systems. This is consistent with the ISO 42005 emphasis on traceability.
Guidance for Use with ISO/IEC 42001	Provides recommendations on how the AI impact assessment process can be integrated within the broader AI management system defined by ISO/IEC 42001. This includes aligning assessments with organizational roles, lifecycle stages, and risk management practices to create a cohesive and effective AI governance structure.	Alignment with Organisational Roles	**Article 17** (Quality management system)	Article 17 of the EU AI Act requires providers of high-risk AI systems to implement a quality management system that ensures compliance with the regulation. This system must include roles and responsibilities for management and staff, aligning with the ISO guidance to integrate AI impact assessments with organizational roles.
		Lifecycle Stages	**Article 9** (Risk management system)	Article 9 outlines a risk management system that must be maintained throughout the entire lifecycle of a high-risk AI system. This continuous process involves regular reviews and updates, which aligns with the ISO guidance to integrate AI impact assessments across different lifecycle stages.
		Risk Management Practices	**Article 9** (Risk management system)	The risk management system described in Article 9 requires the identification, analysis, and mitigation of risks associated with high-risk AI systems. This is consistent with the ISO guidance to align AI impact assessments with risk management practices, ensuring a cohesive governance structure.
		Cohesive AI Governance Structure	**Annex VII** (Conformity based on an assessment of the quality management system and an assessment of the technical documentation)	The EU AI Act emphasizes the need for a structured approach to AI governance, as seen in the requirements for technical documentation and conformity assessments (Annex VII). This structured approach supports the ISO guidance

				to create an effective AI governance structure by integrating impact assessments within the broader management system.
Harms and Benefits Taxonomy	Introduces a structured classification of potential harms (e.g., privacy violations, bias, safety risks) and benefits (e.g., efficiency, accessibility, innovation) associated with AI systems. This taxonomy supports consistent, comprehensive evaluations and helps stakeholders understand trade-offs and prioritize mitigation efforts.	Classification of Harms	**Article 6** (Classification rules for high-risk AI systems)	Article 6 and Annex III classify AI systems as high-risk based on their potential to cause significant harm to health, safety, or fundamental rights. This aligns with the ISO taxonomy's focus on identifying potential harms such as privacy violations, bias, and safety risks.
			Article 10 (Data and data governance)	Article 10 emphasizes the need for data governance to prevent biases that could negatively impact fundamental rights or lead to discrimination. This supports the ISO taxonomy's classification of bias as a potential harm.
		Classification of Benefits	**Article 1** (Subject matter)	Article 1 outlines the regulation's purpose to promote human-centric and trustworthy AI, ensuring benefits such as innovation and efficiency while protecting fundamental rights. This aligns with the ISO taxonomy's focus on benefits like efficiency, accessibility, and innovation.
		Evaluating Trade-Offs	**Article 9** (Risk management system)	Article 9 requires a risk management system that evaluates and mitigates risks throughout the AI system's lifecycle, balancing potential harms and benefits. This supports the ISO taxonomy's role in helping stakeholders understand trade-offs and prioritize mitigation efforts.
		Prioritising Mitigation Efforts	**Article 14** (Human oversight)	Article 14 mandates human oversight to minimize risks to health,

				safety, or fundamental rights, ensuring that potential harms are effectively mitigated. This aligns with the ISO taxonomy's goal of prioritizing mitigation efforts.
Aligning AI System Impact Assessment with Other Assessments	Discusses how AI impact assessments can be aligned with existing processes such as data protection impact assessments (DPIAs), human rights impact assessments, and environmental assessments. This ensures efficiency, avoids duplication, and promotes integrated risk and compliance strategies.	Data Protection Impact Assessments (DPIAs)	**Article 27** (Fundamental Rights Impact Assessment for High-Risk AI Systems)	Article 27 of the EU AI Act allows for the fundamental rights impact assessment to complement existing data protection impact assessments conducted under Article 35 of Regulation (EU) 2016/679 (GDPR) or Article 27 of Directive (EU) 2016/680. This provision supports the ISO 42005 guidance to align AI impact assessments with DPIAs, ensuring efficiency and avoiding duplication.
		Human Rights Impact Assessments	**Article 27** (Fundamental Rights Impact Assessment for High-Risk AI Systems)	Article 27 mandates a fundamental rights impact assessment for high-risk AI systems, which inherently includes considerations of human rights. This aligns with the ISO 42005 recommendation to integrate AI impact assessments with human rights impact assessments, promoting a comprehensive approach to risk and compliance.
		Environmental Assessments	**Article 27** (Fundamental Rights Impact Assessment for High-Risk AI Systems)	While the EU AI Act does not explicitly mandate environmental assessments, the overarching goal of the regulation is to ensure AI systems are safe and aligned with societal values, which can include environmental considerations. The ISO 42005 guidance to align AI impact assessments with environmental assessments can be seen as a proactive measure to

	Integrated Risk and Compliance Strategies	**Article 27** (Fundamental Rights Impact Assessment for High-Risk AI Systems)	ensure comprehensive risk management. The EU AI Act emphasizes the importance of a structured approach to AI governance, as seen in the requirements for technical documentation and conformity assessments (Annex VII). This structured approach supports the ISO 42005 guidance to promote integrated risk and compliance strategies by aligning various impact assessments.



Calls to action

1. Align AI Practices with ISO 42005 Through Certified Audit Support

Elevate your AI governance by aligning your AI Impact Assessments with ISO 42005. Work with ISO/IEC 42006-accredited auditors to verify that your AIMS meets both ethical and regulatory expectations, including those outlined in ISO 42001 and global AI legislation.

2. Kickstart Responsible AI with a Structured ISO 42005 Readiness Review

Initiate your compliance journey by conducting a readiness review guided by ISO 42005 principles and assessed through ISO 42006-auditor methodologies. This approach helps you identify gaps in your impact assessment processes, ensuring a smoother transition toward full ISO 42001 certification.

3. Demonstrate Ethical AI Deployment Through Verified Impact Assessments

Showcase your commitment to responsible AI by embedding ISO 42005-based impact assessments into your AIMS. Independent verification by ISO/IEC 42006-compliant bodies builds stakeholder trust and confirms your system's fairness, transparency, and social alignment.

4. Ensure Lifecycle Accountability with ISO 42005-Backed Audits

Implement ongoing risk and impact monitoring processes aligned with ISO 42005, validated through recurring ISO 42006 surveillance audits. These help you maintain up-to-date safeguards as your AI systems evolve, reinforcing your posture on ethical AI use.

5. Accelerate AI Compliance Through Expert-Led ISO 42005 Integration

Collaborate with ISO/IEC 42006-certified professionals to operationalize ISO 42005 impact assessments within your AI lifecycle. Their expertise in cross-standard alignment (with ISO 42001 and the EU AI Act) ensures audit-readiness and effective, risk-aware AI deployment.

Conclusion

ISO 42005:2024 represents a major step forward in the structured governance of artificial intelligence, offering a standardized framework for developing, operating, and maintaining trustworthy AI systems. As organizations worldwide embrace AI to drive innovation, ISO 42005 provides essential guidance for establishing management systems that ensure ethical, transparent, and effective AI deployment across the entire system lifecycle. By embedding principles of accountability, traceability, and continual improvement, the standard is helping to shape industry practices and reinforce international commitments to responsible AI.

Yet, the true impact of ISO 42005 will lie in its implementation. Organizations face varied challenges—integrating AI-specific controls into existing management systems, maintaining governance structures that ensure oversight, and aligning operational practices with emerging regulatory expectations. For small and medium-sized enterprises (SMEs), in particular, translating ISO 42005 into actionable policies may require tailored support and scalable solutions that uphold compliance without hindering innovation.

Despite these challenges, early adopters of ISO 42005 are already showcasing its value. Pioneering organizations across tech, finance, and healthcare are leveraging the standard to embed AI governance into their operational core—enhancing transparency, aligning with stakeholder expectations, and strengthening resilience in the face of complex AI use cases. By formalizing responsibilities, system monitoring, and improvement processes, these organizations demonstrate how structured AI management contributes to both compliance and competitive advantage.

For business leaders and policymakers alike, ISO 42005 offers a unique opportunity to lead the next wave of AI governance. Success will depend on the development of robust policies, investment in management capabilities, and collaboration across sectors and disciplines. As AI continues to shape critical decisions in society, ISO 42005 provides a critical foundation to ensure systems are not only technically sound, but also aligned with ethical and societal values.

Looking ahead, the longevity and impact of ISO 42005 will depend on widespread adoption, continuous learning, and harmonization with upcoming regulations such as the EU AI Act. Organizations that proactively implement ISO 42005 position themselves at the forefront of trustworthy AI, setting a global benchmark for responsible and sustainable AI management.

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), 'Information technology — Artificial intelligence — AI system impact assessment', accessible at: https://www.iso.org/standard/44545.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