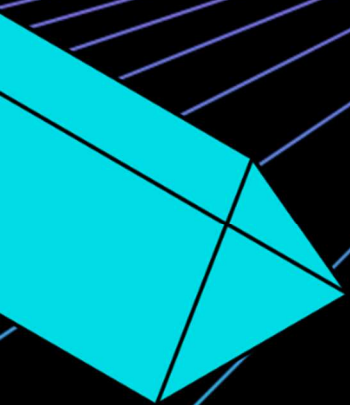
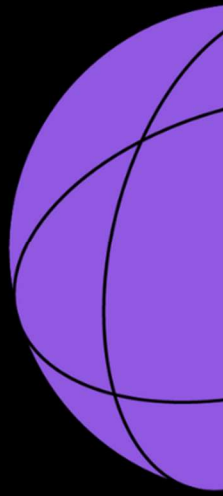


Whitepaper | November 2025

Mind the Gap - ISO 14971 meets the EU AI Act



Executive Summary

Risk management is a central pillar of medical device regulation, ensuring patient safety and compliance throughout the product lifecycle. With the introduction of the EU Artificial Intelligence Act (AIA), its importance has grown further, raising the question of how far ISO 14971 already meets the risk management requirements of Article 9 and where additional measures may be needed. The paper demonstrates that ISO 14971 already provides a strong structural backbone for meeting the risk management requirements of Art. 9 AIA. Both frameworks share an emphasis on a documented, continuous and lifecycle-based process for identifying, evaluating and mitigating risks. This means that manufacturers of AI-based medical devices do not need to entirely reinvent their risk management systems to achieve compliance.

ISO 14971 falls short in addressing AI-specific dimensions that the AI Act makes explicit. These include risks to fundamental rights, impacts on vulnerable groups, data governance challenges, and testing obligations linked to defined performance metrics or, where applicable, real-world testing under Art. 60 AIA. To achieve full compliance, manufacturers must therefore extend their existing ISO 14971 processes with targeted enhancements that reflect the cross-sectoral and fundamental rights-oriented perspective of the AI Act.

Taken together, AI Act and ISO 14971 are not competing but complementary. ISO 14971 secures the device-focused safety paradigm, while the AI Act broadens the scope to societal and data-driven risks. Manufacturers that align their risk management processes accordingly can ensure regulatory conformity and strengthen trust in the safe use of AI in healthcare.

Introduction

Introducing medical devices to the European market rests on two essential pillars: A relevant level of clinical performance as well as an acceptable level of risk to patient safety. The latter is achieved through a systematic risk management process, an integral part of any medical device introduced under the Medical Device Regulation (MDR).

A widely used process to demonstrate that the risk to patient safety has been limited to an acceptable minimum is laid out in ISO 14971¹. Following this harmonised standard, manufacturers have to follow a structured process comprised of risk identification, risk evaluation and risk mitigation to determine the acceptability of residual risks. A combination of the residual risk and the recognised state of the art then determines the suitability of placing the medical device on the market. Furthermore, the risk management process is intended as a continuous process, which does not end with the introduction of the device to the market but must be repeated at pre-determined intervals to ensure risks are managed in a continuous manner.

At first sight, this covers many of the requirements laid out in Art. 9 of the EU AI Act (AIA)², which calls for the establishment of a risk management system (RMS) to be maintained as a continuous iterative process throughout the entire lifecycle of a high-risk AI system (Art. 9 (1)–(2) AIA). At a deeper look, however, Art. 9 includes AI-specific requirements that are not yet covered by a process established following ISO 14971.

This paper explores these gaps by first examining the requirements laid out in Art. 9 before evaluating how ISO 14971 aligns with these requirements and where gaps remain. The analysis shows that ISO 14971 covers many of the requirements laid out in Art. 9 AIA. Where ISO 14971 falls short, however, are AI-specific aspects specifically mentioned in the AIA such as fundamental-rights impacts, data governance risks or AI system testing.

¹ Reference is made to the German edition of EN ISO 14971:2019 + A11:2021, Medical devices – Application of risk management to medical devices.

² Reference is made to regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024.

Requirements for Risk Management under the EU AI Act

A key requirement for high-risk AI systems under the AIA is the introduction of a comprehensive risk management system (Art. 9(1) AIA). Such a system must be established, documented and maintained throughout the lifecycle of an AI system as a continuous and iterative process (Art. 9(2) AIA). Central elements include the systematic identification and analysis of known and reasonably foreseeable risks, their estimation and evaluation as they relate to the intended use and foreseeable misuse, as well as the adoption of targeted mitigation measures (Art. 9(2)(a)-(d) AIA). The remaining residual risks, which may be reasonably mitigated or eliminated through the design or development of the high-risk AI system must be judged acceptable, giving due consideration to state of the art, the interaction of different requirements, and the expected level of knowledge and training of users (Art. 9(3)-(5) AIA). Testing plays a key role in ensuring that systems perform consistently for their intended purpose including, where appropriate, in real-world conditions in accordance with Art. 60 AIA (Art. 9(6)-(8) AIA). In addition, providers must consider the specific risks to vulnerable groups, particularly minors, and may integrate risk management procedures with other sectoral Union law where applicable (Art. 9(9)-(10) AIA). A detailed overview of the requirements under Art. 9 AIA can be found in the Annex of this paper.

Article 9 AI Act in comparison to ISO 14971

The comparison of the requirements set out in Art. 9 AIA with those of ISO 14971 shows that the standard covers most of the obligations established under the AI Act. Nonetheless, targeted extensions are needed to address the AI-specific aspects that otherwise remain insufficiently covered. The detailed analysis shows the following:

Table 1: Comparison of Risk Management System Requirements between Article 9 AIA and ISO 14971

AI Act Reference	ISO 14971 Clause	Coverage Ratio ³	Brief Justification
9(1) Establishment, implementation, documentation, maintenance of an RMS	4.1-4.5: Requirements for Risk Management Systems	Full	ISO 14971 requires an ongoing, documented risk management process with management responsibilities, planning and a risk-management file, matching Art. 9(1) AIA.
9(2) Risk Management along the lifecycle, iterative process	4.1: Risk Management Process 9: Risk Management Review 10.1 -10.4: Post-Market Activities	Full	ISO 14971 frames risk management as a continuous process across the lifecycle and requires active post-production information and periodic review in line with Art. 9(2) AIA.
9(2)(a) Identify and analyse known/foreseeable risks to health, safety and fundamental rights	5.2-5.6: Risk Analysis	Partial	ISO 14971 covers the identification, analysis and evaluation of hazards specific to patient health and safety. However, fundamental rights impacts are not covered.
9(2)(b) Estimate and evaluate risks (intended use and foreseeable misuse)	5.2: Intended Use and reasonably foreseeable Misuse 5.5: Risk Estimation 6: Risk Evaluation	Full	Based on the intended purpose of the medical device, ISO 14971 requires estimating and evaluating risks, including reasonably foreseeable misuse and is thus in accordance with Art. 9(2)(b) AIA.
9(2)(c) Evaluate other risks from post-market monitoring according to Art. 72 AIA	4.4: Post-Market Plan 10: Post-Market Activities	Full	ISO 14971 requires a comprehensive range of post-market activities and is thus aligned with Art. 9(2)(c) AIA.

³ Coverage Ratio: Full - ISO 14971 fully aligns with the requirements of the AI Act. Partial - A process exists, but it does not fully meet the requirements. Gap - ISO 14971 does not address the topic or covers it only marginally.

9(2)(d) Adopt targeted risk management measures	7.1-7.6: Risk Mitigation	Full	ISO 14971 requires the manufacturer to implement a range of mitigation measures to reduce the risks of a device to an acceptable level. This is fully aligned with Art. 9(2)(d) AIA.
9(3) Risks reasonably mitigated or eliminated by design, development or technical information	4.1: Risk Management Process 7.1: Hierarchy of Risk Controls	Full	ISO 14971 requires risk controls to minimise existing risks to an acceptable level, either through inherently safe design, further mitigation measures or additional information and, thus, covers Art. 9(3) AIA.
9(4) Consider interplay of all Chapter III Section 2 requirements when defining measures		Gap	Although ISO 14971 ensures holistic residual risk judgement, it does not account for risks stemming from the interplay of risk mitigation measures addressing requirements laid out in Chapter III Section 2 AIA.
9(5) Residual risk per hazard and overall residual risk must be acceptable	7.3: Residual Risk 8: Overall Residual Risk	Full	ISO 14971 requires explicit acceptability criteria for single and overall residual risk as well as documentation of the method in the plan and is thus in alignment with Art. 9(5) AIA.
9(5)(a) Eliminate/reduce risks through design as far as technically feasible	7.1(a): Inherently Safe Design	Full	ISO 14971 suggests three options to control reasonably foreseeable risks. Eliminating them through technical design has highest priority and is thus in line with Art. 9(5)(a) AIA.
9(5)(b) Apply mitigation control where elimination not possible	7.1(b): Protective Measures	Full	Additional to technical measures mentioned in Clause 7.1 (a) in ISO 14971, the standard also includes further non-technical mitigation measures and is thus in line with Art. 9(5)(b) AIA.
9(5)(c) Provide information under Article 13 and, where appropriate, training to deployers	7.1(c): Information for Safety; Training 4.2: Competence	Partially	ISO 14971 requires certain information for safety and training to be provided but does not cover all the information mentioned in Article 13.

<p>9(5) sentence 3 Consider deployer knowledge, experience, education, expected training, and use context</p>	<p>5.2: Intended user and Deployment Environment</p>	<p>Full</p>	<p>ISO 14971 requires capturing user profiles, competence and environments, consistent with Art. 9(5) AIA sentence 3.</p>
<p>9(6) Testing to identify appropriate measures; ensure consistent performance and compliance</p>	<p>7.2: Verify Implementation and Effectiveness</p>	<p>Partial</p>	<p>ISO 14971 mandates validation of risk controls, but AI-specific testing for high-risk requirements outlined in Section 2 AIA such as accuracy or robustness, however, are not specifically covered.</p>
<p>9(7) Testing may include real-world testing as per Article 60</p>	<p>-</p>	<p>Gap</p>	<p>If real-world testing is involved, this needs to be conducted in line with Art. 60 AIA. ISO 14971, however, does not address real-world testing nor does it define the regulatory governance requirements of Art. 60 AIA. Yet, it is important to note that real-world testing is not mandatory under the AIA.</p>
<p>9(8) Testing throughout development and before placing on the market; against pre-defined metrics and probabilistic thresholds</p>	<p>4.4.7: Verification 7.2: Effectiveness Verification</p>	<p>Partial</p>	<p>ISO 14971 requires pre-market validation of risk controls. Even though testing is one option, ISO 14971 does not prescribe AI performance metrics or thresholds and thus only partially covers Art. 9(8).</p>
<p>9(9) Consider impacts on minors (<18) and other vulnerable groups</p>	<p>5.2 Intended User and Deployment Environment</p>	<p>Partial</p>	<p>ISO 14971 requires capturing user profiles, competence and environments. Checking for vulnerable groups such as minors is not considered by default but is only covered if included in the intended purpose or the employment environment of the AI medical device.</p>

The way forward: AI-specific extensions

To address the identified gaps, organizations may adopt a range of measures. With respect to fundamental rights risks, including the protection of vulnerable groups, appropriate approaches may involve integrating a dedicated fundamental rights impact assessment during the identification phase or maintaining a separate register of fundamental rights risks, such as informed consent, protection of personal data, and freedom of occupation.

In relation to data governance risks, options range from product-specific data-lifecycle controls during collection, labeling, curation, versioning or retention to establishing a central data-governance process. Such a process may serve as a general process or employ documented checklists to systematically identify dataset hazards and corresponding controls.

For AI performance metrics and thresholds, organizations may consider defining both clinical and model-centric metrics, setting explicit acceptance limits and monitoring thresholds in planning documents, or establishing release gates with predefined change and monitoring criteria that reflect the requirements set out in Chapter III Section 2 AIA. Annex E of ISO 24971 can be helpful for identifying suitable supporting standards in this regard.

Finally, to address cybersecurity threats, relevant measures may include extending threat modeling across all data and model phases of the AI lifecycle, introducing provenance and access controls, and conducting adversarial or red-team exercises.

Conclusion

The analysis shows that manufacturers do not need to reinvent their risk management process to meet the requirements laid out in Art. 9 AIA. ISO 14971 already provides a structurally compatible backbone for Art. 9 AIA and delivers most lifecycle, documentation, and verification expectations - especially when embedded into an ISO 13485 QMS.

Similar to the relation between ISO 13485 and Art. 17 covered in an earlier whitepaper⁴, however, the analysis shows that AI-specific enhancements are needed. For ISO 14971 this includes a consideration of fundamental rights impacts and vulnerable groups, taking risks from data governance for training, validation, and monitoring into account as well as explicit performance metrics and thresholds throughout development. Optionally, governance for real-world testing under Art. 60 AIA may be set up.

While ISO 14971 covers all essential requirements for medical device manufacturers, it leaves gaps with respect to the AI-specific components. These observations are consistent with the technology-specific, sector-agnostic orientation of the AI Act, which complements the device-focused MDR framework paradigm.

⁴ Whitepaper: Better Safe Than Sorry? ISO 13485 and the EU AI Act, available at: https://www.tuev-lab.ai/fileadmin/user_upload/TUEV_AI_Lab_Whitepaper_QMS_ISO13485-EUAIAct_EN.pdf

Annex: The requirements of Article 9 AIA

Art. 9 AIA	Requirement
9(1)	A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems
9(2)	The risk management system shall be understood as a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating. It shall comprise the following steps:
9(2)(a)	the identification and analysis of the known and the reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights when the high-risk AI system is used in accordance with its intended purpose
9(2)(b)	the estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose, and under conditions of reasonably foreseeable misuse
9(2)(c)	the evaluation of other risks possibly arising, based on the analysis of data gathered from the post-market monitoring system referred to in Article 72;
9(2)(d)	the adoption of appropriate and targeted risk management measures designed to address the risks identified pursuant to point (a)
9(3)	The risks referred to in this Article shall concern only those which may be reasonably mitigated or eliminated through the development or design of the high-risk AI system, or the provision of adequate technical information
9(4)	The risk management measures referred to in paragraph 2, point (d), shall give due consideration to the effects and possible interaction resulting from the combined application of the requirements set out in this Section, with a view to minimising risks more effectively while achieving an appropriate balance in implementing the measures to fulfil those requirements.
9(5)	The risk management measures referred to in paragraph 2, point (d), shall be such that the relevant residual risk associated with each hazard, as well as the overall residual risk of the high-risk AI systems is judged to be acceptable.

9(5)(a) elimination or reduction of risks identified and evaluated pursuant to paragraph 2 in as far as technically feasible through adequate design and development of the high-risk AI system

9(5)(b) where appropriate, implementation of adequate mitigation and control measures addressing risks that cannot be eliminated;

9(5)(c) provision of information required pursuant to Article 13 and, where appropriate, training to deployers.

9(5) Sentence 3 With a view to eliminating or reducing risks related to the use of the high-risk AI system, due consideration shall be given to the technical knowledge, experience, education, the training to be expected by the deployer, and the presumable context in which the system is intended to be used.

9(6) High-risk AI systems shall be tested for the purpose of identifying the most appropriate and targeted risk management measures. Testing shall ensure that high-risk AI systems perform consistently for their intended purpose and that they are in compliance with the requirements set out in this Section

9(7) Testing procedures may include testing in real-world conditions in accordance with Article 60.

9(8) The testing of high-risk AI systems shall be performed, as appropriate, at any time throughout the development process, and, in any event, prior to their being placed on the market or put into service. Testing shall be carried out against prior defined metrics and probabilistic thresholds that are appropriate to the intended purpose of the high-risk AI system.

9(9) When implementing the risk management system as provided for in paragraphs 1 to 7, providers shall give consideration to whether in view of its intended purpose the high-risk AI system is likely to have an adverse impact on persons under the age of 18 and, as appropriate, other vulnerable groups

9(10) For providers of high-risk AI systems that are subject to requirements regarding internal risk management processes under other relevant provisions of Union law, the aspects provided in paragraphs 1 to 9 may be part of, or combined with, the risk management procedures established pursuant to that law.



TÜV AI.Lab GmbH

Max-Urich-Str. 3

13355 Berlin

Deutschland

www.tuev-lab.ai

[www.tuev-risk-](http://www.tuev-risk-navigator.ai)

[navigator.ai](http://www.tuev-risk-navigator.ai)

The TÜV AI.Lab was founded in 2023 as an independent joint venture by the TÜV companies TÜV SÜD, TÜV Rheinland, TÜV NORD, TÜV Hessen and TÜV Thüringen. The TÜV AI.Lab aims to translate the regulatory requirements for AI into practice and make Europe a hotspot for safe and trustworthy AI. To this end, it develops quantifiable conformity criteria and suitable test methods for AI. The AI.Lab also actively supports the development of standards and norms for AI systems.