International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Risk Management Framework in the AI Act

Md Fokrul Islam Khan *

Department of Management Information System, International American University, USA.

International Journal of Science and Research Archive, 2025, 14(03), 466-471

Publication history: Received on 27 January 2025; revised on 07 March 2025; accepted on 09 March 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.14.3.0688

Abstract

The Artificial Intelligence Act (AI Act) is a landmark regulatory system proposed by the European Commission to oversee the development and setting out of artificial intelligence across the European Union. The AI Act was officially proposed in April 2021 and aims to put clear regulations on AI applications, especially those falling into high-risk categories, with the purpose of protecting public health, safety, and fundamental rights. The legislation follows a risk-based approach that will enable a balance of harms related to the usage of AI technologies with innovation. This leading-edge framework makes the EU an international leader in the ethical governance of AI and, hence, should serve as a model for similar initiatives across other parts of the world. This article will carry out a doctrinal assessment or analysis of Article 9 under the AI Act through four methods of statutory interpretation: literal, systematic, teleological, and historical. Relying on the existing Drafts and proposed amendments from the European Commission, Council, and European Parliament, this analysis delineates Article 9's purpose and scope and its specific risk management requirements. It will continue to discuss the potential enforcement strategy for the provisions of this article and end with a section on recommendations to amplify the legislative process under the AI Act.

Keywords: Artificial Intelligence; Risk Management; AI Act; European Commission

1. Introduction

The European Union's Artificial Intelligence Act, introduced by the European Commission in April 2021, is the world's first inclusive regulatory framework through which artificial intelligence has ever been governed within a significant jurisdiction. The AI Act is expected to be a global benchmark, likely influencing the frameworks through which AI governance occurs worldwide. This is mainly in countries such as the US and the United Kingdom, in efforts to set guiding principles on safety, ethics, and transparency concerning AI [1].By targeting AI's potential risks to human rights, health, and safety, the AI Act sets requirements for high-risk AI systems, emphasizing robust risk management practices. Such requirements are crucial as AI becomes increasingly embedded in high-stakes applications, such as critical infrastructure, healthcare, and law enforcement, where unmanaged risks could have severe consequences.

One of the keystones of the AI Act is the structured approach it builds out under Article 9 for risk management, where developers and deployers must have a system to identify, assess, and mitigate all risks associated with those systems throughout the life cycle. According to Veale & Zuiderveen [2], such a risk management policy would hold all the risks that can be created around operations, ethics, and misuse in pursuing responsible AI use. In this respect, the emphasis by the European Commission upon binding risk management is indicatively an understanding that AI risks extend considerably beyond just technical malfunction. This includes broad social and economic impacts such as bias, unfair discrimination, and security vulnerabilities, as Vesnic et al. [3] research highlights. Consequently, risk management provisions under the AI Act have been essential to aligning AI innovation with EU values for trust, accountability, and human rights, promoting an environment in which AI systems would be safely and responsibly deployable.

* Corresponding author: Md Fokrul Islam Khan

Over the last years, management of AI risks has been gaining visibility amongst both regulators and operators in the private sector. For example, the NIST AI Risk Management Framework voluntary guidelines in the US have informed better ethics in using AI [4]. However, the AI Act goes a step further in the sheer legal requirement for high-risk AI application operators to maintain the risk under control. This increases the accountability bar for suppliers of AI systems and brings a level playing field in the EU member states. The novelty of this approach in the AI Act will combine the protection of innovation with serving as a model for genuinely global, organized AI governance that minimizes risks without hindering technological development, as Laux et al. [5] state. This controlling emphasis on the management of AI risk underlines a growing consensus that there needs to be a proactive safety-focused AI ecosystem. It places the EU in pole position concerning the development of trustworthy AI.

2. Regulatory Concept

The regulatory concept behind Article 9 of the AI Act focuses on implementing a structured, risk-based approach to artificial intelligence regulation, prioritizing safety and ethical standards. The AI Act labels AI systems according to their levels of risk, which then accordingly bans those AI systems presenting "unacceptable risks," imposes strict demands on "high-risk" AI systems, and allows low-risk AI systems to operate with minimal constraints [6]. Compliance, in this regard, involves the fact that suppliers of high-risk AI systems must adhere to the measures described in Chapter 2 of the Act, with the understanding that even so, some residual risks may still be at large. Article 9 addresses this residual risk, requiring providers to implement a comprehensive risk management system to pinpoint and mitigate these risks to an acceptable level, thus acting as an additional safeguard within the regulatory framework.

Article 9 is structured around a central mandate for high-risk AI providers to create a risk management system, with specific procedural details provided in paragraphs 2–7. This risk management system has two main components: a risk management process, outlined in paragraphs 2–4, and testing procedures in paragraphs 5–7. Additional provisions in Article 9 cater to specific groups, including children and credit institutions, acknowledging the unique needs of these sectors [6]. Standards also play a crucial role in achieving compliance, and providers can demonstrate conformity with the AI Act by adhering to harmonized standards, which are explicitly referenced in Article 9(3) as providing a "presumption of conformity." While harmonized standards for AI risk management are not yet available, European Standards Organizations are in the process of developing them. In the interim, international standards, such as the NIST AI Risk Management Framework or ISO/IEC 23894, offer provisional guidance [6]. Although these international standards do not guarantee conformity under EU law, they can serve as valuable tools for providers aiming to comply with Article 9.

3. Purpose

The primary purposes of the AI Act is to establish a uniform legal system across the EU for the expansion, deployment, and use of AI in alignment with EU values and to facilitate the smooth internal market functioning. The Act classifies AI systems as "unacceptable, "high-risk," and "low risk" and covers harms to individuals and society that AI could cause. This means that high-risk AI systems must be put up with the enhanced need to develop risk management processes and continuous oversight procedures [7]. Such will mitigate their potential threats to human rights and public safety. This kind of legislation also underlines the EU's main aim to become the global leader in ethical and secure AI by fostering "Legally Trustworthy AI" through commitment to basic rights, the rule of law, and democratic principles.

Fundamentally, it is set to avoid fragmentation in the market by creating clarity within the law and an integrated regulatory framework that eliminates most inconsistencies capable of disrupting free movement for AI systems across the EU market [6]. Besides, the AI Act safeguards citizens against intrusive applications like biometric identification in public spaces or systems rooted in models of human manipulative design are protected by prohibition or heavy restriction. It will include transparency requirements, including human oversight, that secures the deployment of AI by democratic values and public interest. The aim of the AI Act, therefore, is regulatory compliance and building public trust in AI by promoting technological innovation with an ethical and legally secure framework.

4. Scope of Application

The scope of application under the AI Act has material, personal, regional, and temporal dimensions of its applicability. Materially, under the AI Act, high-risk AI systems are characterized as those with capabilities and usages that may cause significant harm, such as tools used in the process of screening and assessment in the context of employment or enforcement. Specific applications, including those used in medical science or autonomous vehicle technologies like

Tesla's, are examples of high-stakes use cases that fall under these provisions [8]. AI systems with "unacceptable" risks are prohibited, indicating a strict regulatory boundary against systems likely to harm or exploit users.

In terms of personal scope, Article 9 mandates that suppliers of high-risk AI system establish a risk management system. Providers, as defined by Article 3, include those responsible for placing these AI systems on the EU market, regardless of whether they are based within the EU or in third countries. Public authorities are generally included, though some exceptions apply, specifically for international organizations and certain public bodies excluded from compliance with Article 9. Regionally, the AI Act extends to all providers operating within or whose AI system outputs are used within the EU, ensuring that foreign providers must comply with EU standards if their AI systems impact EU residents. Temporally, compliance deadlines vary. Providers are given twenty-four months to create risk management systems after the Act's enforcement, though extensions are under consideration.

5. Requirements

5.1. Risk management system, Article 9(1)

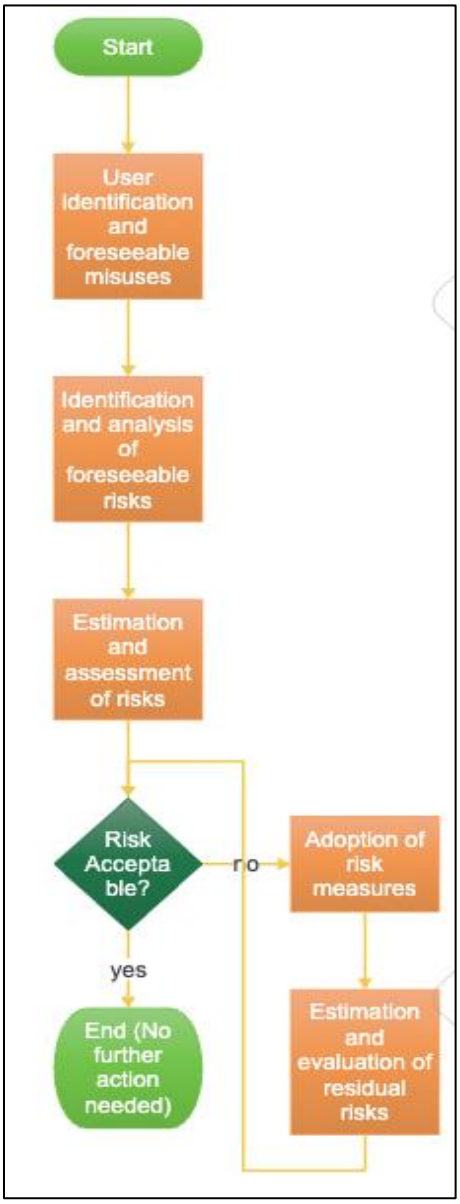

Figure 1 Risk Management Process

Under Article 9(1) of the EU Artificial Intelligence Act, establishing a risk management framework for high-risk AI systems is essential. This system, which must be "established, implemented, documented, and maintained," forms the backbone of the regulatory requirements (EU AI Act, 2024). Establishment entails creating and approving specific policies and procedures, while implementation requires putting these practices into action effectively within the organization [6]. Documentation involves systematically detailing the system's inaccessible records, allowing regulatory bodies to verify compliance. Lastly, maintaining the system demands periodic reviews and updates to keep the system effective throughout the AI framework lifecycle.

The process for risk management, under Article 9 of the EU Artificial Intelligence Act, should be a structured, continuous, and iterative procedure through the whole lifecycle of high-risk AI systems. That would mean it starts with the allocation and analysis of risks to health, safety, and fundamental rights-particularly those foreseeable from the system's intended use or possible misuse. This identification relies on systematic methods, such as risk taxonomies and scenario analysis, to detect potential hazards and anticipate harmful outcomes [6]. The following procedure, after the identification of risk, is the estimation and evaluation for probability and severity, as shown in Figure 1. The evaluation thus provides a way for the AI provider to measure the potential impact due to the realized risk and decide on priorities according to the magnitude of such risks.

Once the risks are assessed, the providers implement measures for risk management in order to deal with and mitigate those risks. These include design modifications, control implementations, or other preventive actions that effectively lower risks to an acceptable level [9].This process is iterative and adaptive, requiring continuous monitoring, review, and updates. Providers must revisit and refine risk management measures, especially as new data becomes available from post-market monitoring systems, ensuring that emerging risks are addressed promptly and thoroughly. If the risk is acceptable, it is documented using now the procedures highlighted in Article 9(1), and then after that, it is completed. Then, if after all residual acceptable risks reach an acceptable level, the risk management is terminated or stopped, as shown in Figure 1 above. This proactive approach emphasizes the Act's commitment to robust, ongoing risk management and legal certainty in high-risk AI applications.

5.2. Risk management measures, Article 9(3)

Articles 9(3) and (4) of the EU Artificial Intelligence Act elaborate on risk management measures providers of high-risk AI systems must adopt to address and mitigate potential risks. According to Article 9(3), risk management measures should consider the effects and possible interactions of all requirements in Chapter 2 of the Act. Additionally, providers are encouraged to adopt the "state of the art" in AI risk management, even though formal harmonized standards or typical specifications are still emerging (Schuett, 2024). Paragraph 4 divides the measures into three types: design-focused measures, mitigation, and user-focused communication. First, providers are to eliminate or decrease risks as much as possible during the system's design and development phase, such as fine-tuning a language model to prevent toxic outputs. In places where elimination is not possible, controls can be deployed by providers in order to manage the remaining risks, including deploying content filters. Lastly, there should be sufficient information and training for users so that users are aware of the capabilities and limitations of the system. According to the EU Artificial Intelligence Act (2024), these measures are put together to ensure that any residual risks are minimized and the system remains safe, with compliance with fundamental rights.

5.3. Testing procedures, Article 9(5-7)

Testing procedures under Article 9(5)–(7) of the EU Artificial Intelligence Act represent the fourth step in the risk management process for high-risk AI systems. The purpose of testing is threefold: it helps providers identify appropriate risk management measures, ensures the AI system performs consistently for its intended purpose, and verifies compliance with regulatory requirements, such as transparency and accuracy [6]. Testing addresses challenges like distributional shift, where the system's performance may vary due to environmental changes from its training phase. It also assesses the system against predefined metrics and probabilistic thresholds to ensure accuracy and robustness, especially in varied real-world contexts. While providers are required to conduct testing throughout development, it must be finalized before the AI system reaches the market. Though the Act does not specify if testing must be conducted in-house or outsourced, the provider is ultimately responsible for compliance, making accountability crucial. Thus, testing is an essential iterative process to uphold safety, functionality, and regulatory alignment.

5.4. Special rules for Kids and Credit institutions, Article 9(8), (9).

Articles 9(8) and (9) of the EU Artificial Intelligence Act introduce special rules for protecting vulnerable groups, specifically children and credit institutions. Paragraph 8 mandates that providers give particular attention to risks associated with children (defined as persons under 18), requiring that risk management systems address potential

impacts on this group due to their unique vulnerability and specific rights [6]. Paragraph 9 addresses credit institutions, clarifying that AI-specific risk management requirements should integrate with existing credit risk protocols, ensuring that AI-related risks are covered without redundancy. This complementary approach allows credit institutions to align their risk management practices with AI-specific and general industry regulations.

6. Enforcement of the Act

Article 9 of the AI Act can be enforced through a combination of administrative, civil, and potential criminal measures. Non-compliance by the suppliers of high-risk AI systems may be administratively fined in quite considerable amounts. Further, compliance may be controlled by the competent national authorities, normally starting with requests to the providers to demonstrate compliance with the conditions in Article 9. The provision of false or misleading information may also lead to further administrative penalties [6]. Other civil enforcement options include contractual liability in cases where failure to comply with Article 9 on the part of the provider causes harm to a contracting party, and this could position the obligations under Article 9 as a secondary contractual duty. There is also tort liability if, through a high-risk AI system, an individual suffers harm and makes claims against the obligations for risk management [10]. In some jurisdictions, non-compliance may be deemed negligent and constitute a criminal offense, reflecting the seriousness with which AI-related risks are approached across regulatory frameworks.

7. Summary and Conclusion

Overall, the AI Act represents a pioneering step in establishing a structured and risk-oriented regulatory framework for AI, mainly focusing on high-risk AI systems that may impact health, fundamental rights, and safety. This article focused on Article 9, which described what it is, its scope, and the particular requirements it imposes. The Act obliges providers to institute adequate risk management systems, including risk identification, mitigation of that risk, and testing procedures. It is intriguing to realize that the special provisions for the protection of vulnerable groups and children were incorporated. Then, the adoption of previous regulatory standards in sectors like credit institutions for which the same approach to regulation would be crucial. Article 9 enforcement mechanisms contribute to reinforced accountability through administrative fines, possible civil liability, and, in certain cases, criminal measures so that effective compliance mechanisms are ensured. The Act's focus on harmonizing AI regulations within the EU and safeguarding fundamental rights places it at the forefront of global AI governance. Moving forward, further refinements and harmonized standards will strengthen its effectiveness, promoting safe and ethical AI deployment

Compliance with ethical standards

Disclosure of conflict of interest

I'm Md Fokrul Islam Khan, declare that I have no financial, professional, or personal conflicts that may influence my judgment in Risk Management Framework in the AI Act. I commit to maintaining impartiality and will disclose any future conflicts if they arise.

References

[1] U.S. Department of State, "Risk management profile for artificial intelligence and human rights," 2024. [Online]. Available: https://www.state.gov/risk-management-profile-for-ai-and-human-rights/ Accessed:Mar.7,2025Accessed: Mar. 7, 2025Accessed:Mar.7,2025

[2] M. Veale and F. Zuiderveen Borgesius, "Demystifying the draft EU Artificial Intelligence Act—analysing the good, the bad, and the unclear elements of the proposed approach," Comput. Law Rev. Int., vol. 22, no. 4, pp. 97–112, 2021. [Online]. Available: https://arxiv.org/pdf/2107.03721 Accessed:Mar.7,2025Accessed: Mar. 7, 2025Accessed:Mar.7,2025

[3] L. Vesnic-Alujevic, S. Nascimento, and A. Polvora, "Societal and ethical impacts of artificial intelligence: Critical notes on European policy frameworks," Telecommunications Policy, vol. 44, no. 6, p. 101961, 2020. [Online]. Available: https://doi.org/10.1016/j.telpol.2020.101961

[4] National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0), 2023. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf Accessed:Mar.7,2025Accessed: Mar. 7, 2025Accessed:Mar.7,2025

[5] J. Laux, S. Wachter, and B. Mittelstadt, "Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk," Regulation & Governance, vol. 18, no. 1, pp. 3–32, 2024. [Online]. Available: https://doi.org/10.1111/rego.12512

[6] J. Schuett, "Risk management in the Artificial Intelligence Act," Eur. J. Risk Regul., vol. 15, no. 2, pp. 367–385, 2024. [Online]. Available: https://doi.org/10.1017/err.2023.1

[7] N. A. Smuha et al., "How the EU can achieve legally trustworthy AI: A response to the European Commission's proposal for an Artificial Intelligence Act," SSRN, 2021. [Online]. Available: http://dx.doi.org/10.2139/ssrn.3899991 Accessed:Mar.7,2025Accessed: Mar. 7, 2025Accessed:Mar.7,2025

[8] S. S. Gadde and V. D. Kalli, "Artificial intelligence and its models," Int. J. for Res. Appl. Sci. Eng. Technol., vol. 9, no. 11, pp. 315–318, 2021. [Online]. Available: https://doi.org/10.22214/ijraset.2021.33007

[9] EU Artificial Intelligence Act, "Article 9: Risk management system," 2024. [Online]. Available: https://artificialintelligenceact.eu/article/9/ Accessed:Mar.7,2025Accessed: Mar. 7, 2025Accessed:Mar.7,2025

[10] K. Ramakrishnan, G. Smith, and C. Downey, "US tort liability for large-scale artificial intelligence damages," RAND Corporation, 2024. [Online]. Available: https://www.rand.org/content/dam/rand/pubs/research_reports/RRA3000/RRA3084-1/RAND_RRA3084-1.pdf Accessed:Mar.7,2025Accessed: Mar. 7, 2025Accessed:Mar.7,2025