International Journal of Interdisciplinary Innovative Research & Development (IJIIRD)
ISSN: 2456-236X
Vol. **11** Special Issue **02** | **2026**

Software Systems Compliance with the European Union Artificial Intelligence Act: A Comprehensive Review of Frameworks, Challenges, and Best Practices

Prof. Priya T. Ghute[1]
[1] *Lecturer, Computer Science & Engineering, Padm. Dr. V. B. Kolte College Of Engg., M.H, India*

DOI: 10.5281/zenodo.19254356

ABSTRACT

The European Union Artificial Intelligence Act (AI Act) represents the world's first comprehensive legal framework aimed at regulating artificial intelligence systems through a risk-based approach. Its introduction marks a paradigm shift in how AI systems are designed, deployed, and governed, with significant implications for software engineering practices, organizational processes, and ethical accountability. While a growing body of research has examined the legal foundations of the AI Act, less attention has been devoted to systematically reviewing how software systems can achieve and demonstrate compliance in practice.

This review paper provides a comprehensive analysis of AI Act compliance from a software systems perspective. It synthesizes existing literature on risk classification, conformity assessment, governance frameworks, technical standards, and Trustworthy AI methodologies. The paper categorizes compliance efforts into legal, technical, and organizational dimensions and reviews existing frameworks, standards, and tools that support operationalization of AI Act requirements. Key challenges—including uncertainty in risk classification, technical opacity of AI models, fairness and bias management, explainability, and organizational readiness—are critically examined.

Based on the review, the paper consolidates best practices and outlines future research directions for building compliance-by-design AI systems. The findings emphasize that AI Act compliance is not a one-time legal exercise but a continuous socio-technical process that must be integrated into the full software lifecycle. This review aims to support researchers, practitioners, and policymakers in understanding the current state of AI Act compliance and in developing scalable, trustworthy, and legally aligned AI systems.

Keywords:- AI Act, AI Governance, Regulatory Compliance, Trustworthy AI, Software Engineering, Review Paper

1. INTRODUCTION

Artificial Intelligence has rapidly transitioned from experimental technology to a foundational component of modern software systems. AI-driven applications are increasingly embedded in safety-critical, socially sensitive, and legally regulated domains such as healthcare, transportation, finance, employment, and public administration. This widespread adoption has amplified concerns regarding safety, fairness, accountability, transparency, and fundamental rights.

In response to these concerns, the European Union introduced the Artificial Intelligence Act, a landmark regulatory initiative designed to govern AI systems using a risk-based regulatory approach. Unlike previous technology regulations, the AI Act directly targets the lifecycle of AI systems, imposing obligations on providers, deployers, and other actors involved in AI development and use.

From a software systems perspective, the AI Act introduces unprecedented compliance challenges. Developers must translate abstract legal principles into concrete engineering practices, integrate legal requirements into system design, and ensure continuous compliance throughout deployment and operation. This review paper examines how existing research and practice address these challenges and identifies gaps that require further investigation.

2. OVERVIEW OF THE EU AI ACT

The AI Act establishes a horizontal regulatory framework applicable to a broad range of AI systems, irrespective of the underlying technology. Its central feature is a **risk-based classification** that categorizes AI systems into four levels: unacceptable risk, high risk, limited risk, and minimal or no risk.

Unacceptable-risk systems are prohibited outright due to their potential to cause significant harm to fundamental rights. High-risk systems are permitted but subject to stringent requirements, including risk management, data governance, technical documentation, human oversight, and post-market monitoring. Limited-risk systems are subject primarily to transparency obligations, while minimal-risk systems remain largely unregulated.

For software engineers, this classification fundamentally reshapes development priorities. Compliance obligations are no longer uniform but depend on system purpose, context of use, and potential impact. As a result, risk assessment becomes a critical early-stage activity in AI system design.

3. AI ACT COMPLIANCE AS A SOFTWARE ENGINEERING PROBLEM

Compliance with the European Union Artificial Intelligence Act cannot be addressed solely as a legal or policy exercise; rather, it represents a fundamental software engineering challenge. The AI Act introduces obligations that directly affect how AI-based software systems are specified, designed, implemented, deployed, and maintained. As a result, compliance must be embedded within the entire software lifecycle instead of being treated as a final verification step.

From an engineering perspective, the first major implication of the AI Act is the need to incorporate **risk assessment into requirements engineering**. Unlike traditional software regulations that apply uniformly, the AI Act assigns obligations based on the intended use, context, and potential impact of an AI system. This requires software teams to explicitly document system purpose, stakeholders, and foreseeable misuse scenarios at early design stages. Such documentation becomes a technical artifact that guides subsequent architectural and implementation decisions.

Another critical aspect is the **translation of legal requirements into technical controls**. Provisions related to data governance, robustness, accuracy, transparency, and human oversight must be operationalized through concrete engineering mechanisms. Examples include dataset versioning, model performance monitoring, logging infrastructures, explainability components, and fallback procedures enabling human intervention. These mechanisms must be measurable, verifiable, and auditable, aligning software quality attributes with legal compliance goals.

AI Act compliance also challenges conventional development workflows due to the **dynamic nature of AI systems**. Machine learning models may evolve through retraining, data drift, or context changes after deployment. Consequently, compliance is not static but requires continuous monitoring and reassessment throughout the system's operational life. This shifts compliance from a one-time certification mindset toward a **continuous engineering process**, similar to practices in safety-critical and regulated software domains.

Finally, AI Act compliance demands **interdisciplinary collaboration within software teams**. Engineers must work closely with legal experts, ethicists, and organizational stakeholders to ensure that compliance requirements are correctly interpreted and technically implemented. This reinforces the view that AI Act compliance is a socio-technical engineering problem, requiring coordinated design, governance, and operational strategies across the software lifecycle.

4. FRAMEWORKS FOR AI ACT COMPLIANCE

A growing body of research proposes frameworks to support AI Act compliance. These frameworks typically aim to translate regulatory requirements into structured assessment processes.

4.1 Conformity Assessment Frameworks

Conformity assessment frameworks provide structured procedures for evaluating whether an AI system meets applicable legal and ethical requirements. These approaches often adopt lifecycle-based models that incorporate pre-deployment assessment, deployment checks, and post-market monitoring.

4.2 Governance and Audit Frameworks

AI governance frameworks emphasize internal accountability, documentation, and auditing. They support traceability of design decisions and allocation of responsibility across organizational roles. Continuous auditing mechanisms are increasingly emphasized to align with post-market monitoring requirements.

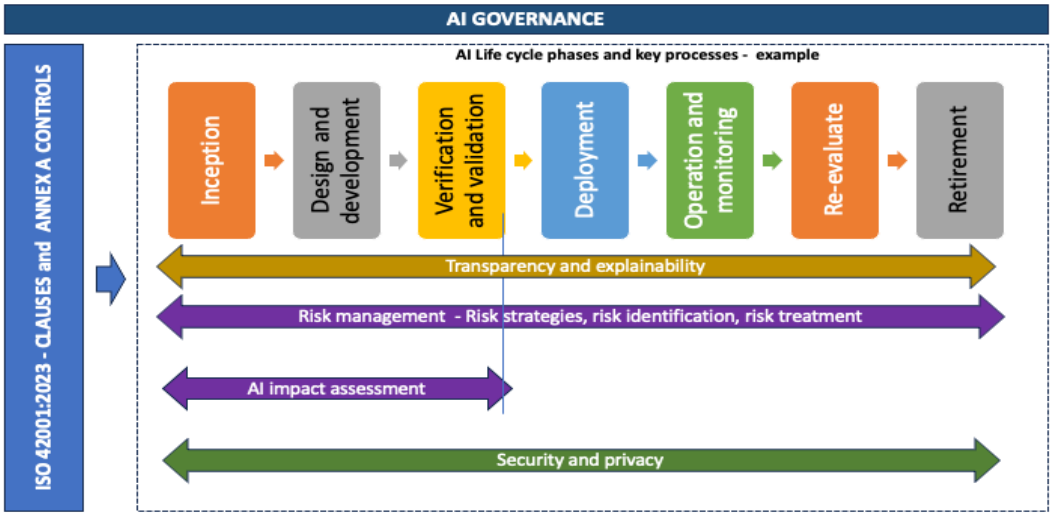
4.3 Compliance-by-Design Approaches

Compliance-by-design integrates regulatory requirements directly into system architecture and development processes. This approach mirrors privacy-by-design principles and aims to reduce retrofitting costs by embedding compliance considerations early in development.

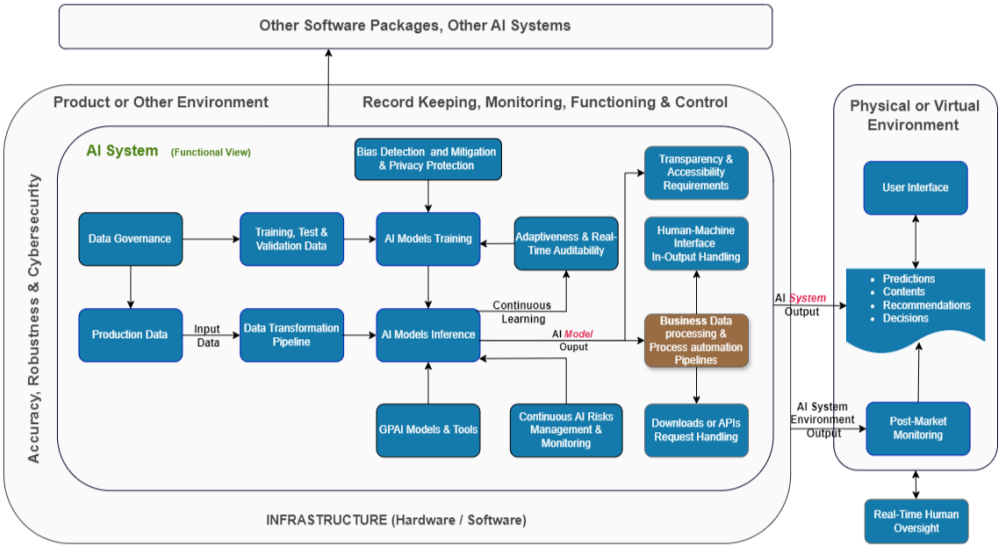
5. STANDARDS AND TECHNICAL SUPPORT FOR AI ACT COMPLIANCE

Standards play a crucial role in bridging the gap between high-level regulatory requirements and concrete software engineering practices. Although the AI Act does not currently mandate specific technical standards for

certification, it explicitly anticipates the development and adoption of harmonized standards to support compliance. In the interim, existing international standards and technical specifications can be leveraged as partial enablers of AI Act requirements.



Several standards issued by organizations such as ISO and IEC address aspects relevant to AI governance, including risk management, quality management systems, data governance, robustness evaluation, and system documentation. These standards provide structured methodologies for assessing system reliability, managing data quality, and documenting development processes, all of which align with obligations imposed on high-risk AI systems under the AI Act.



However, existing standards were largely designed for traditional software systems or generic machine learning workflows and therefore require adaptation to address the unique characteristics of AI systems, such as model opacity, probabilistic behavior, and data dependency. In particular, gaps remain in standardizing explainability, fairness assessment, and post-market monitoring procedures. Consequently, standards should be viewed as supportive instruments rather than complete solutions, requiring contextual interpretation and integration within broader compliance frameworks.

6. TRUSTWORTHY AI METHODS AND TOOLS SUPPORTING COMPLIANCE

Research on Trustworthy AI has produced a wide range of methods and tools that directly support the operationalization of AI Act requirements. These methods focus on key principles such as fairness, transparency, robustness, accountability, and human oversight, which are central to the regulation.

From a technical standpoint, fairness assessment tools enable the identification and mitigation of biases in datasets and model outputs. Explainable AI techniques provide mechanisms to interpret and communicate

system behavior to users and regulators, addressing transparency obligations. Robustness and security testing methods help evaluate system resilience against errors, adversarial inputs, and unexpected operational conditions.

While these tools are valuable, their application is highly context-dependent. Fairness metrics, for instance, may vary significantly across domains, and explainability requirements differ depending on user expertise and system criticality. Moreover, the integration of these tools into real-world software pipelines remains a challenge, as many are research prototypes rather than production-ready solutions.

As a result, Trustworthy AI methods should be incorporated as components of a broader compliance strategy, complemented by governance processes, documentation practices, and human oversight mechanisms.

7. CONCLUSION

This review paper examined software systems compliance with the European Union Artificial Intelligence Act from a comprehensive socio-technical perspective. By synthesizing regulatory provisions, compliance frameworks, technical standards, and Trustworthy AI methodologies, the paper highlighted how the AI Act fundamentally reshapes the way AI-based software systems are engineered, governed, and maintained.

The analysis demonstrated that AI Act compliance extends far beyond legal interpretation and requires systematic integration into software engineering practices across the entire AI lifecycle. Risk-based classification, conformity assessment, data governance, transparency, and human oversight must be operationalized through concrete technical and organizational mechanisms. The review further emphasized that compliance is not a one-time certification activity but a continuous process, driven by model evolution, data drift, and changing deployment contexts.

Key challenges identified in this review include regulatory uncertainty, technical opacity of AI models, difficulties in measuring fairness and explainability, and limited organizational readiness. These challenges underscore the necessity of interdisciplinary collaboration between software engineers, legal experts, ethicists, and organizational decision-makers. Existing standards and Trustworthy AI tools provide valuable support, but they remain insufficient in isolation and must be adapted and combined within broader governance frameworks.

In conclusion, achieving sustainable AI Act compliance requires a shift toward compliance-by-design and governance-by-design principles. Future research should focus on standardized compliance toolchains, automation of conformity assessment activities, domain-specific compliance frameworks, and empirical validation of compliance practices in real-world systems. Such efforts are essential to ensure that AI systems deployed in Europe are not only innovative but also lawful, trustworthy, and aligned with fundamental rights.

8. REFERENCES

[1] European Commission, *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, COM(2021) 206 final, 2021.

[2] European Parliament, *Artificial Intelligence Act – Amendments Adopted by the European Parliament*, Brussels, 2023.

[3] B. Shneiderman, "Human-centered artificial intelligence: Reliable, safe, and trustworthy," *International Journal of Human–Computer Interaction*, vol. 36, no. 6, pp. 495–504, 2020.

[4] S. Amershi et al., "Guidelines for human-AI interaction," *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI)*, pp. 1–13, 2019.

[5] T. Miller, "Explanation in artificial intelligence: Insights from the social sciences," *Artificial Intelligence*, vol. 267, pp. 1–38, 2019.

[6] A. Holzinger, "From machine learning to explainable AI," *Computer Science Review*, vol. 40, p. 100330, 2021.

[7] M. Veale and F. Zuiderveen Borgesius, "Demystifying the Draft EU Artificial Intelligence Act," *Computer Law Review International*, vol. 22, no. 4, pp. 97–112, 2021.

[8] ISO/IEC 23894:2023, *Information Technology — Artificial Intelligence — Risk Management*, International Organization for Standardization, 2023.

[9] ISO/IEC 22989:2022, *Artificial Intelligence — Artificial Intelligence Concepts and Terminology*, ISO, 2022.

[10] ISO/IEC TR 24028:2020, *Artificial Intelligence — Overview of Trustworthiness in Artificial Intelligence*, ISO, 2020.

[11] L. Floridi et al., "AI4People—An ethical framework for a good AI society," *Minds and Machines*, vol. 28, no. 4, pp. 689–707, 2018.

[12] F. Doshi-Velez and B. Kim, "Towards a rigorous science of interpretable machine learning," *arXiv preprint arXiv:1702.08608*, 2017.

[13] S. Barocas, M. Hardt, and A. Narayanan, *Fairness and Machine Learning*, fairmlbook.org, 2019.

[14] R. K. Bellamy et al., "AI Fairness 360: An extensible toolkit for detecting and mitigating algorithmic bias," *IBM Journal of Research and Development*, vol. 63, no. 4, pp. 1–15, 2019.
[15] European Union Agency for Fundamental Rights, *Getting the Future Right—Artificial Intelligence and Fundamental Rights*, Publications Office of the EU, 2020.
[16] A. Raji et al., "Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing," *Proceedings of the Conference on Fairness, Accountability, and Transparency (FAccT)*, pp. 33–44, 2020.
[17] M. Kroll, "The fallacy of inscrutability," *Philosophical Transactions of the Royal Society A*, vol. 376, no. 2133, 2018.
[18] J. W. Schmidt et al., "Regulating AI: Lessons from the EU's AI Act," *IEEE Computer*, vol. 56, no. 2, pp. 24–33, 2023.